aws

Guida per l'utente

Amazon Elastic Compute Cloud



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

Amazon Elastic Compute Cloud: Guida per l’utente

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

I marchi e l’immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità 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 cosa è Amazon EC2? ... 1
Funzionalità ... 1
Servizi correlati ... 2
Accesso a EC2 ... 4
Prezzi ... 5
Stime, fatturazione e ottimizzazione dei costi ... 6
Resources ... 7
Guida introduttiva ... 8
Fase 1: avvio di un'istanza ... 10
Fase 2. connessione all'istanza ... 12
Fase 3. pulizia di un'istanza ... 15
Fasi successive ... 16
Best practice ... 17
Amazon Machine Image ... 20
Caratteristiche di AMI ... 22
Permessi di avvio ... 22
Tipo di volume root ... 23
Individua il tipo di volume root dell'AMI ... 24
Tipi di virtualizzazione ... 26
Trovare una AMI ... 28
Parametri Systems Manager ... 31
Parametri Systems Manager pubblici ... 35
AMI a pagamento in Marketplace AWS ... 39
Vendi la tua AMI nel Marketplace AWS ... 40
Trovare un'AMI a pagamento ... 40
Acquistare un'AMI a pagamento ... 42
Recupera il codice del prodotto ... 43
Utilizzo del supporto a pagamento ... 44
Fatture per AMI a pagamento e supportate ... 45
Gestione delle sottoscrizioni ... 45
Ciclo di vita di un'AMI ... 47
Creare un'AMI ... 49
Crea un' S3-backed AMI Amazon ... 58
Creare un'AMI utilizzando Windows Sysprep ... 98

Copiare un'AMI ... 116
Archiviazione e ripristino di un'AMI ... 135
Discendenza AMI ... 145
Filigrane AMI ... 151
Tipi di istanza consentiti dall'AMI ... 157
Uso delle AMI ... 162
Dichiarazione di un'AMI come obsoleta ... 187
Disabilitazione di un'AMI ... 193
Annullare la registrazione di un'AMI ... 199
Modalità di avvio ... 206
Requisiti per la modalità di avvio UEFI ... 208
Parametro della modalità di avvio dell'AMI ... 209
Modalità di avvio del tipo di istanza ... 211
Modalità di avvio dell'istanza ... 214
Modalità di avvio del sistema operativo ... 216
Impostazione della modalità di avvio dell'AMI ... 218
Variabili UEFI ... 224
UEFI Secure Boot ... 225
Crittografia AMI ... 242
Instance-launching scenari ... 243
Image-copying scenari ... 246
AMI condivise ... 249
Fornitore verificato ... 249
Trovare AMI condivise ... 250
Preparati a usare AMI condivise per Linux ... 253
AMI consentite ... 254
Rendere pubblica l'AMI ... 276
Blocco dell'accesso pubblico per le AMI ... 280
Condivisione di un'AMI con organizzazioni e unità organizzative ... 290
Condividi un'AMI con uno specifico AWS account ... 302
Annullamento la condivisione di un'AMI con il tuo account ... 306
Consigli per creare AMI Linux condivise ... 308
Monitoraggio degli eventi ... 313
Dettagli dell'evento ... 315
disponibile eventi ... 315
Non riuscito eventi ... 316

annullata la registrazione eventi ... 317
disabled eventi ... 317
Comprendere la fatturazione AMI ... 318
Campi di fatturazione AMI ... 319
Trovare le informazioni di fatturazione AMI ... 321
Verificare gli addebiti AMI in fattura ... 323
Quote delle AMI ... 324
Richiedi un aumento della quota per AMIs ... 325
Istanze ... 327
Tipi di istanza ... 328
Tipi di istanza disponibili ... 329
Specifiche dell'hardware ... 330
Tipi di hypervisor ... 330
Tipi di virtualizzazione dell'AMI ... 331
Processori ... 331
Individuazione di un tipo di istanza ... 334
Strumento di ricerca del tipo di istanza EC2 ... 341
Suggerimenti sul Compute Optimizer ... 344
Modifiche del tipo di istanza ... 347
Istanze a prestazioni espandibili ... 356
Istanze GPU ... 410
Istanze Mac ... 424
Ottimizzazione EBS ... 480
Opzioni della CPU ... 609
AMD SEV-SNP ... 920
Controllo degli stati del processore ... 935
Istanze gestite ... 939
Fatturazione per le istanze gestite ... 940
Identificazione di istanze gestite ... 941
Impostazioni di visibilità delle risorse gestite ... 943
Iniziare a utilizzare le istanze gestite ... 947
Virtualizzazione annidata ... 948
Come funziona ... 948
Considerazioni ... 948
Avvia una nuova istanza con la virtualizzazione annidata abilitata ... 949
Configurare un'istanza esistente per utilizzare la virtualizzazione annidata ... 950

Trova i tipi di istanza che supportano la virtualizzazione annidata 951
Opzioni di fatturazione e acquisto 953
Istanze on demand 954
Istanze riservate 956
Spot Instances 1027
Host dedicati 1129
Istanze dedicate 1193
Prenotazioni della capacità 1201
Modelli di avvio 1362
Restrizioni 1363
Permissions 1364
Controllo dell'avvio delle istanze 1371
Crea 1374
Modifica (gestione delle versioni) 1390
Elimina 1394
Avvio di un'istanza 1397
Esercitazioni 1400
Riferimento ai parametri delle istanze 1424
Avvio tramite la procedura guidata di avvio dell'istanza 1438
Utilizzo di un modello di avvio 1442
Avvio da un'istanza esistente 1449
Avvio da un' Marketplace AWS AMI 1451
Connessione all'istanza 1454
Prerequisiti generali per la connessione 1456
Connessione a un'istanza Linux tramite SSH 1461
Connessione all'istanza Windows con il protocollo RDP 1478
Connessione tramite Session Manager 1488
Connettiti tramite un IP pubblico ed EC2 Instance Connect 1489
Connessione usando un IP privato e l'endpoint EC2 Instance Connect 1526
Cambio di stato istanza 1559
Fatturazione per stato dell'istanza 1560
Istanze in sospeso 1562
Istanze arrestate 1562
Istanze ibernate 1562
Riavvio delle istanze 1563
Istanze interrotte 1563

Differenze tra gli stati dell'istanza 1564
Arresto e avvio 1567
Ibernazione 1587
Riavvio 1618
Interruzione 1620
Ritiro 1637
Ripristino automatico dell'istanza 1642
Concetti chiave del ripristino automatico dell'istanza 1644
Differenze tra ripristino automatico semplificato e ripristino basato sull' CloudWatch azione 1646
Creare un sistema resiliente 1647
Verificare se è avvenuto il ripristino automatico 1647
Ripristino automatico semplificato 1649
CloudWatch ripristino basato sull'azione 1654
Metadati delle istanze 1658
Categorie di metadati dell'istanza 1660
Categorie dei dati dinamici 1674
Accesso ai metadati dell'istanza 1675
Configurazione delle opzioni IMDS 1717
Esecuzione di comandi durante l'avvio 1755
Esempio: valore dell'indice di avvio dell'AMI 1782
Individua se un host è un'istanza EC2 1786
Ispezionare l'Documenti di identità dell'istanza 1787
Ispezionare l'UUID del sistema 1787
Ispezione dell'identificatore di generazione della macchina virtuale del sistema 1789
Documenti di identità dell'istanza 1794
Recupera il documento di identità dell'istanza 1796
Verifica documento di identità dell'istanza 1798
Certificati pubblici 1809
Conformità STIG 1871
Impostazioni STIG 1873
Scarica gli script STIG 1895
Applica le impostazioni STIG con Systems Manager 1918
Sincronizzazione dell'orologio 1921
Marcatura temporale dei pacchetti hardware 1922
Secondi intercalari 1923

Utilizzo del servizio di sincronizzazione oraria di Amazon locale 1924
Utilizzo del servizio di sincronizzazione oraria di Amazon pubblico 1941
Confronto dei timestamp per le istanze Linux 1943
Modifica del fuso orario dell'istanza 1944
EC2 Capacity Manager 1947
Caratteristiche chiave 1948
Abilitazione di Capacity Manager 1948
Organizzazione dei dati 1961
Navigazione di Capacity Manager nella console 1980
Esportazione dei dati 1983
Gestione dei driver di dispositivo 1987
Driver di rete 1988
Driver grafici 1988
Driver dei dispositivi di archiviazione 1988
Altri driver di dispositivo Windows 1989
Driver AMD 1989
Driver NVIDIA 1995
Installa il driver ENA su Windows 2044
Driver Windows PV 2065
Driver NVMe 2101
Altri driver di dispositivo Windows 2113
Configurazione di istanze Windows 2114
Windows-specific impostazioni di sistema 2114
AWS driver di dispositivo per istanze Windows 2115
Agenti di avvio Windows 2117
EC2 Fast Launch per Windows 2283
Modifica della password dell'amministratore Windows 2308
Aggiunta di componenti di sistema Windows 2309
Installazione di WSL su Windows 2315
Utilità Windows 2316
Aggiornamento delle istanze Windows 2318
Esecuzione di un aggiornamento in loco 2319
Esecuzione di un aggiornamento automatico 2324
Esegui la migrazione a un tipo di istanza Nitro-based 2335
Risoluzione dei problemi relativi a un aggiornamento 2344
Tutorial: Connessione di un'istanza EC2 a un database RDS 2345

Obiettivo del tutorial ... 2345
Contesto ... 2346
Architecture ... 2346
Considerazioni ... 2348
È ora di completare il tutorial ... 2348
Costi ... 2349
Opzione 1: connessione automatica tramite la console EC2 ... 2349
Opzione 2: connessione automatica tramite la console RDS ... 2362
Opzione 3: connessione manuale ... 2374
Flotte ... 2385
Funzionalità e vantaggi ... 2385
Quale metodo per parco istanze utilizzare? ... 2386
Opzioni di configurazione ... 2388
Tipi di richieste ... 2390
Limiti di spesa ... 2419
Attribute-based selezione del tipo di istanza ... 2421
Ponderazione delle istanze ... 2458
Strategie di allocazione ... 2461
Ribilanciamento della capacità ... 2469
Prenotazioni della capacità ... 2474
Lavorare con un parco istanze EC2 ... 2476
Stati della richiesta parco istanze EC2 ... 2477
Prerequisiti di parco istanze EC2 ... 2478
Creazione di un parco istanze EC2 ... 2483
Tagging di un parco istanze EC2 ... 2493
Descrivi un parco istanze EC2 ... 2495
Come modificare un parco istanze EC2 ... 2499
Eliminazione di un parco istanze EC2 ... 2502
Lavorare con un parco istanze spot ... 2507
Stati della richiesta di parco istanze spot ... 2508
Autorizzazioni del parco istanze spot ... 2509
Creazione di un parco istanze Spot ... 2520
Assegnare tag a un parco istanze spot ... 2530
Descrivere un parco istanze spot ... 2540
Modificare una richiesta di parco istanze spot ... 2541
Annullare (eliminare) una richiesta di parco istanze spot ... 2544

Scalabilità automatica per il parco istanze spot ... 2547
Monitoraggio del parco istanze ... 2558
Monitora la tua flotta utilizzando CloudWatch ... 2559
Monitora la tua flotta utilizzando EventBridge ... 2562
Esercitazioni ... 2581
Tutorial: Configura il parco istanze EC2 per usare la ponderazione dell'istanza ... 2584
Tutorial: configura la flotta EC2 per utilizzare le On-Demand istanze come capacità principale ... 2588
Tutorial: configura la flotta EC2 per avviare On-Demand istanze utilizzando prenotazioni di capacità mirate ... 2589
Tutorial: Configura il tuo parco istanze EC2 per avviare istanze in Blocchi di capacità ... 2596
Tutorial: configura la tua flotta EC2 per avviare le istanze in prenotazioni di capacità interrompibile ... 2599
Tutorial: configura la tua flotta EC2 per avviare le istanze in più tipi di prenotazione della capacità utilizzando un gruppo di risorse per la prenotazione della capacità ... 2604
Esempi di configurazioni di CLI per parco istanze EC2 ... 2610
Esempio 1: Avviare Istanze spot come opzione di acquisto predefinita ... 2611
Esempio 2: Launch On-Demand Instances come opzione di acquisto predefinita ... 2611
Esempio 3: Launch On-Demand Instances come capacità principale ... 2612
Esempio 4: avvio di On-Demand istanze utilizzando più prenotazioni di capacità ... 2612
Esempio 5: On-Demand istanze di avvio che utilizzano le prenotazioni di capacità quando la capacità totale di destinazione supera il numero di prenotazioni di capacità non utilizzate ... 2616
Esempio 6: avvio di On-Demand istanze utilizzando prenotazioni di capacità mirate ... 2620
Esempio 7: Configurare il ribilanciamento della capacità per avviare la sostituzione delle istanze spot ... 2623
Esempio 8: Avviare le istanze spot in un parco istanze ottimizzato per la capacità ... 2625
Esempio 9: Avviare le istanze spot in un parco istanze ottimizzato per la capacità con priorità ... 2627
Esempio 10: avvio di istanze spot in un parco istanze ottimizzato per prezzo e capacità ... 2628
Esempio 11: configurazione della selezione del tipo di istanza basata su attributi ... 2630
Esempio 12: avvia le istanze in più tipi di prenotazione di capacità utilizzando un gruppo di risorse per la prenotazione di capacità ... 2631
Configurazioni CLI di esempi per parco istanze spot ... 2632
Esempio 1: Zona di disponibilità Lowest-priced ... 2633
Esempio 2: Zona di Lowest-priced disponibilità da un elenco ... 2634
Esempio 3: tipo di Lowest-priced istanza da un elenco ... 2636

Esempio 4. Sostituire il prezzo per la richiesta. 2638
Esempio 5: Utilizza la strategia di allocazione diversificata 2640
Esempio 6: Utilizza la ponderazione delle istanze 2643
Esempio 7: utilizzo On-Demand della capacità 2644
Esempio 8: Configura il ribilanciamento della capacità 2645
Esempio 9: Utilizza un parco istanze ottimizzato per la capacità 2647
Esempio 10: Utilizza un parco istanze ottimizzato per la capacità con priorità 2648
Esempio 11: Utilizza un parco istanze priceCapacityOptimized 2649
Esempio 12: configurazione della selezione del tipo di istanza basata su attributi 2651
Quote del parco istanze 2652
Richiesta di un aumento della quota per la capacità obiettivo 2653
Reti 2655
Regioni e zone 2656
Regioni 2657
Zone di disponibilità 2657
Local Zones 2659
Zone Wavelength 2660
AWS Outposts 2661
Indirizzamento IP per le istanze 2663
Indirizzi IPv4 privati 2664
Indirizzi IPv4 pubblici 2665
Ottimizzazione dell'indirizzo IPv4 pubblico 2667
Indirizzi IPv6 2669
Indirizzi IP multipli 2670
Nomi host per le istanze EC2 2671
Link-local indirizzi 2671
Indirizzi IPv4 2672
Indirizzi IPv6 2678
Indirizzi IP secondari 2684
Indirizzi IPv4 su Windows 2688
Hostname e domini delle istanze EC2 2695
Comprensione degli hostname e dei domini delle istanze EC2 2696
Tipi di hostname 2696
Utilizzo dei propri indirizzi IP 2712
Definizioni BYOIP 2713
Requisiti e quote 2713

Disponibilità regionale ... 2715
Disponibilità delle zone locali ... 2715
Prerequisiti ... 2717
Onboarding dell'intervallo di indirizzi ... 2726
Utilizzo dell'intervallo di indirizzi ... 2735
Indirizzi IP elastici ... 2737
Prezzi degli indirizzi IP elastici ... 2737
Nozioni di base sull'indirizzo IP elastico ... 2737
Quota degli indirizzi IP elastici ... 2739
Associazione di un indirizzo IP elastico ... 2739
Trasferimento di un indirizzo IP elastico ... 2745
Rilascio di un indirizzo IP elastico ... 2751
Utilizzo del DNS inverso per applicazioni e-mail ... 2752
Interfacce di rete ... 2756
Concetti di interfaccia di rete ... 2758
Schede di rete ... 2760
Indirizzi IP per interfaccia di rete ... 2764
Creazione di un'interfaccia di rete ... 2767
Allegati dell'interfaccia di rete ... 2772
Gestire gli indirizzi IP ... 2776
Modifica degli attributi dell'interfaccia di rete ... 2780
Interfacce di rete multiple ... 2784
Requester-managed interfacce di rete ... 2788
Delega prefisso ... 2790
Eliminazione di un'interfaccia di rete ... 2801
Larghezza di banda di rete ... 2801
Larghezza di banda disponibile per l'istanza ... 2803
Ponderazione della larghezza di banda ... 2805
Monitorare la larghezza di banda delle istanze ... 2845
Reti avanzate ... 2846
Adattatore elastico di rete (ENA) ... 2847
ENA Express ... 2931
Intel 82599 VF ... 2972
Monitoraggio delle prestazioni di rete ... 2985
Miglioramento della latenza di rete su Linux ... 2996
Considerazioni sulle prestazioni di Nitro ... 3000

Ottimizza le prestazioni di rete su Windows 3009
Elastic Fabric Adapter 3011
Nozioni di base su EFA 3012
Librerie e interfacce supportate 3014
Tipi di istanze supportati 3015
Sistemi operativi supportati 3032
Limitazioni di EFA 3032
Prezzi EFA 3033
Nozioni di base su EFA e MPI 3033
Nozioni di base su EFA e NCCL 3053
Inizia con EFA e NIXL 3081
Ottimizzare la larghezza di banda della rete 3102
Installa EFA in un contenitore 3118
Creare e collegare un EFA 3120
Scollegare ed eliminare un EFA 3125
Monitoraggio di un EFA 3125
Verifica del programma di installazione EFA 3133
Note di rilascio 3147
Topologia EC2 3176
Come funziona 3177
Prerequisiti 3184
Esempi 3186
Gruppi di collocamento 3201
Strategie di posizionamento 3203
Creazione di un gruppo di collocamento 3209
Modifica del collocamento dell'istanza 3212
Eliminazione di un gruppo di collocamento 3214
Gruppi di posizionamento condivisi 3215
Gruppi di collocamento attivi AWS Outposts 3218
MTU rete 3219
Frame jumbo (9001 MTU) 3220
Rilevamento della MTU del percorso 3221
Imposta la MTU per le istanze 3222
Risoluzione dei problemi 3228
Cloud privati virtuali 3228
I tuoi VPC predefiniti 3229

VPC non predefiniti ... 3230
Accesso a Internet ... 3231
Sottoreti condivise ... 3231
IPv6-only sottoreti ... 3232
Reti secondarie ... 3232
Cosa sono le reti secondarie? ... 3233
Concetti chiave ... 3233
Architecture ... 3234
Ulteriori considerazioni ... 3234
Nozioni di base ... 3234
Gestione delle risorse di rete secondarie ... 3236
Best practice per la progettazione della rete ... 3237
Risoluzione dei problemi ... 3238
Quote e limiti ... 3239
Sicurezza ... 3240
Protezione dei dati ... 3241
Sicurezza dei dati di Amazon EBS ... 3242
Crittografia dei dati a riposo ... 3242
Crittografia dei dati in transito ... 3244
Sicurezza dell'infrastruttura ... 3246
Isolamento della rete ... 3246
Isolamento su host fisici ... 3247
Controllo del traffico di rete ... 3247
Resilienza ... 3250
Convalida della conformità ... 3251
Identity and Access Management ... 3251
Identity-based politiche ... 3252
Policy di esempio per l'API ... 3264
Policy di esempio per la console ... 3309
AWS politiche gestite ... 3322
Ruoli IAM ... 3331
Gestione degli aggiornamenti ... 3344
Procedure ottimali relative alle istanze Windows ... 3344
High-level best practice in materia di sicurezza ... 3345
Gestione degli aggiornamenti ... 3346
Gestione della configurazione ... 3348

Gestione delle modifiche ... 3349
Audit e responsabilità istanze Windows Amazon EC2 ... 3350
Key pairs (Coppie di chiavi) ... 3350
Creazione di una coppia di chiavi ... 3352
Descrivere le tue coppie di chiavi ... 3360
Eliminazione della coppia di chiavi ... 3364
Aggiungi o sostituisci una chiave pubblica sull'istanza Linux ... 3366
Verifica dell'impronta digitale ... 3367
Gruppi di sicurezza ... 3370
Panoramica di ... 3371
Creare un gruppo di sicurezza ... 3372
Modifica i gruppi di sicurezza per l'istanza ... 3375
Eliminare un gruppo di sicurezza ... 3381
Monitoraggio delle connessioni ... 3382
Regole del gruppo di sicurezza per diversi casi d'uso ... 3389
NitroTPM ... 3396
Requisiti ... 3397
Abilitazione di un'AMI Linux per NitroTPM ... 3399
Verifica che un'AMI sia abilitata per NitroTPM ... 3400
Abilitazione o interruzione dell'utilizzo di NitroTPM ... 3402
Verifica che un'istanza sia abilitata per NitroTPM ... 3403
Recupero della chiave di approvazione pubblica ... 3404
Attestazione dell'istanza EC2 ... 3406
Integrazione con AWS KMS ... 3408
Attestazione di ambienti di elaborazione isolati ... 3408
AWS Modello di responsabilità condivisa ... 3409
AMI attestabili ... 3409
Preparazione AWS KMS per l'attestazione ... 3419
Ottieni il documento di attestazione NitroTPM ... 3420
Integrazione con AWS KMS ... 3428
Isola i dati dai tuoi operatori ... 3429
Credential Guard per istanze Windows ... 3430
Prerequisiti ... 3430
Avviare un'istanza supportata ... 3431
Disattivare l'integrità della memoria ... 3433
Attivare Credential Guard ... 3433

Verificare se Credential Guard è in esecuzione ... 3435
AWS PrivateLink ... 3436
Creazione di un endpoint VPC dell'interfaccia ... 3437
Creazione di una policy di endpoint ... 3437
Archiviazione ... 3439
AWS Prezzi dello archiviazione ... 3440
Amazon EBS ... 3440
Limiti di volume EBS ... 3441
Schede EBS ... 3445
Archivio dell'istanza Amazon EC2 ... 3448
Persistenza dei dati ... 3449
Limiti di volume di archivio dell'istanza ... 3451
Volumi di instance store SSD ... 3455
Aggiungere volumi di instance store ... 3460
Abilita il volume di swap per le istanze M1 e C1 ... 3468
Inizializza i volumi dell'archivio dell'istanza ... 3471
Statistiche dettagliate delle prestazioni per i volumi di archivio dell'istanza ... 3473
Volumi root ... 3477
Istanze con volume root Amazon EBS ... 3478
Istanze con un volume root di archivio dell'istanza (solo istanze Linux) ... 3479
Conservazione del volume root dopo aver terminato l'istanza ... 3480
Sostituzione di un volume root ... 3485
Nomi dei dispositivi per i volumi ... 3499
Nomi dei dispositivi disponibili ... 3499
Considerazioni sul nome dei dispositivi ... 3502
Mappatura dei dispositivi a blocchi ... 3504
Concetti relativi alla mappatura dei dispositivi a blocchi ... 3504
Aggiungi una mappatura dei dispositivi a blocchi dell'AMI ... 3508
Aggiungi una mappatura dei dispositivi a blocchi all'istanza ... 3512
Come vengono collegati e mappati i volumi per le istanze Windows ... 3521
Mappare i dischi NVMe ai volumi ... 3522
Mappare i dischi non NVMe ai volumi ... 3528
Prevenzione delle distorsioni di scrittura ... 3538
Dimensioni dei blocchi supportate ... 3539
Requisiti ... 3540
Verificare il supporto delle istanze ... 3541

Configurazione del carico di lavoro ... 3543
Snapshot EBS basati su Windows VSS ... 3544
Cos'è VSS? ... 3545
Come funziona la soluzione con snapshot Amazon EBS basati su VSS ... 3546
Prerequisiti VSS ... 3547
Creazione di snapshot VSS ... 3560
Risoluzione dei problemi relativi agli snapshot VSS ... 3571
Opzioni di ripristino per la soluzione AWS VSS ... 3575
Cronologia delle versioni ... 3577
Archiviazione di oggetti, file e memorizzazione dei file nella cache ... 3582
Simple Storage Service (Amazon S3) ... 3582
Amazon EFS ... 3588
Amazon FSx ... 3592
Amazon File Cache ... 3598
Gestione delle risorse ... 3599
Selezione di una regione per le risorse ... 3599
Trova le tue risorse ... 3601
Passaggi della console ... 3601
Esempi della riga di comando ... 3610
Global View (in più regioni) ... 3614
AWS Vista globale ... 3614
Tagging delle risorse. ... 3618
Nozioni di base sui tag ... 3619
Assegnazione di tag alle risorse ... 3620
Limitazioni applicate ai tag ... 3621
Tag e gestione degli accessi ... 3622
Tagging delle risorse per la fatturazione ... 3622
Autorizzazioni dei tag delle risorse ... 3623
Aggiungi e rimuovi i tag. ... 3626
Filtra le risorse per tag ... 3631
Visualizza i tag utilizzando i metadati delle istanze ... 3633
Service Quotas ... 3639
Visualizzazione delle quote correnti ... 3639
Richiesta di un aumento ... 3640
Restrizione sull'e-mail inviata tramite la porta 25 ... 3640
Monitoraggio delle risorse ... 3642

Monitoraggio dello stato delle istanze ... 3643
Verifiche di stato ... 3644
Controlli dello stato delle applicazioni ... 3654
Eventi di modifica dello stato ... 3676
Eventi pianificati ... 3678
Monitora le tue istanze utilizzando CloudWatch ... 3717
Allarmi delle istanze ... 3718
Gestione del monitoraggio dettagliato ... 3719
CloudWatch metriche ... 3722
Installa e configura l'agente CloudWatch ... 3743
Statistiche sui parametri dei ... 3747
Visualizzare i grafici di monitoraggio ... 3757
Creazione di un allarme ... 3758
Creazione di allarmi che arrestano, terminano, riavviano o recuperano un'istanza ... 3759
Automatizza utilizzando EventBridge ... 3773
Tipi di EC2 eventi Amazon ... 3773
Registra le chiamate API utilizzando CloudTrail ... 3774
Eventi di gestione delle API di Amazon EC2 in CloudTrail ... 3776
Esempi di eventi dell'API Amazon EC2 ... 3776
Connessioni di audit effettuate tramite EC2 Instance Connect ... 3777
Monitorare le applicazioni .NET e SQL Server ... 3779
Monitoraggio dell'utilizzo del piano gratuito ... 3780
Vantaggi del piano gratuito prima e dopo il 15 luglio 2025 ... 3780
Tracciamento dell'utilizzo del piano gratuito per gli account creati prima del 15 luglio 2025 3782
Report di fatturazione e utilizzo ... 3784
Istanze ... 3785
Istanze Bare Metal ... 3786
Host dedicati ... 3786
Istanze dedicate ... 3786
Ottimizzazione EBS ... 3787
Prenotazioni della capacità ... 3787
Inventario delle istanze EC2 ... 3787
Posizione geografica ... 3789
Specifiche dell'hardware ... 3790
Immagini ... 3791
Indirizzi IP e nomi host DNS ... 3793

Regole del gruppo di sicurezza ... 3794
Dati utente ... 3796
Risorse correlate ... 3797
Risoluzione dei problemi ... 3798
Problemi di avvio dell'istanza ... 3798
Nome del dispositivo non valido ... 3799
Superamento del limite di istanze ... 3800
Capacità insufficiente dell'istanza ... 3800
La configurazione richiesta attualmente non è supportata. Controlla la documentazione per verificare le configurazioni supportate. ... 3801
Terminazione immediata dell'istanza ... 3802
Autorizzazioni insufficienti ... 3803
Utilizzo elevato della CPU poco dopo l'avvio di Windows (solo istanze Windows) ... 3804
L'avvio di un' IMDSv1-enabled istanza non riesce ... 3805
Problemi di arresto dell'istanza ... 3806
Arresto forzato di un'istanza ... 3807
(Facoltativo) Creare un'istanza sostitutiva ... 3809
Problemi di terminazione istanza ... 3812
Terminazione immediata dell'istanza ... 3812
Ritardo della terminazione dell'istanza ... 3812
L'istanza terminata rimane visualizzata ... 3814
Errore: l'istanza non può essere terminata. Modifica il relativo attributo di istanza «disable» ApiTermination ... 3815
Istanze avviate o terminate automaticamente ... 3815
Istanze irraggiungibili ... 3815
Riavvio dell'istanza ... 3816
Output della console delle istanze ... 3816
Acquisizione di uno screenshot di un'istanza irraggiungibile ... 3817
Screenshot comuni per le istanze di Windows ... 3819
Ripristino delle istanze in caso di errori del computer host ... 3828
L'istanza è apparsa offline ed è stata inaspettatamente riavviata ... 3828
Problemi SSH dell'istanza Linux ... 3829
Cause comuni dei problemi di connessione ... 3830
Errore di connessione all'istanza: Connection timed out ... 3832
Errore: impossibile caricare la chiave... Valore previsto: QUALSIASI CHIAVE PRIVATA ... 3835
Errore: User key not recognized by server ... 3836

Errore: autorizzazione negata o connessione chiusa dalla porta 22 [istanza] 3838
Errore: Unprotected Private Key File (File della chiave privata non protetto) 3840
Errore: la chiave privata deve iniziare con "-----BEGIN RSA PRIVATE KEY-----" e finire con "-----END RSA PRIVATE KEY-----" 3842
Errore: verifica della chiave host non riuscita 3843
Errore: il server ha rifiutato la nostra chiave or Nessun metodo di autenticazione supportato disponibile 3843
Cannot Ping Instance (Impossibile eseguire il ping dell'istanza) 3844
Errore: il server ha chiuso inaspettatamente la connessione di rete 3845
Errore: convalida della chiave host non riuscita per EC2 Instance Connect 3845
Impossibile connettersi all'istanza Ubuntu tramite EC2 Instance Connect 3847
Ho perso la mia chiave privata. Come posso connettermi alla mia istanza? 3847
Istanza Linux con esito negativo delle verifiche dello stato 3854
Esame delle informazioni di verifica dello stato 3855
Recupero dei log di sistema 3856
Risoluzione degli errori del log di sistema per le istanze Linux 3857
Out of memory: kill process 3858
ERROR: mmu_update failed (aggiornamento della gestione della memoria non riuscito) ... 3859
I/O errore (errore del dispositivo di blocco) 3860
I/O ERRORE: né disco locale né remoto (dispositivo a blocchi distribuiti danneggiato) 3862
request_module: runaway loop modprobe (looping del modprobe del kernel legacy sulle versioni precedenti di Linux) 3863
"FATAL: kernel too old" e "fsck: No such file or directory while trying to open /dev" (mancata corrispondenza di kernel e AMI) 3864
«IRREVERSIBILE: impossibile caricare/lib/modules" o BusyBox "(moduli del kernel mancanti) 3865
ERROR Invalid kernel (kernel non compatibile con EC2) 3867
fsck: No such file or directory while trying to open... file system non trovato 3868
General error mounting filesystems (errore di montaggio) 3870
VFS: Unable to mount root fs on unknown-block (mancata corrispondenza del file system root) 3873
Errore: impossibile determinare il major/minor numero di dispositivo root... (Mancata system/device corrispondenza del file principale) 3874
XENBUS: Device with no driver... 3876
... days without being checked, check forced (verifica del file system richiesta) 3877
fsck died with exit status... (dispositivo mancante) 3877

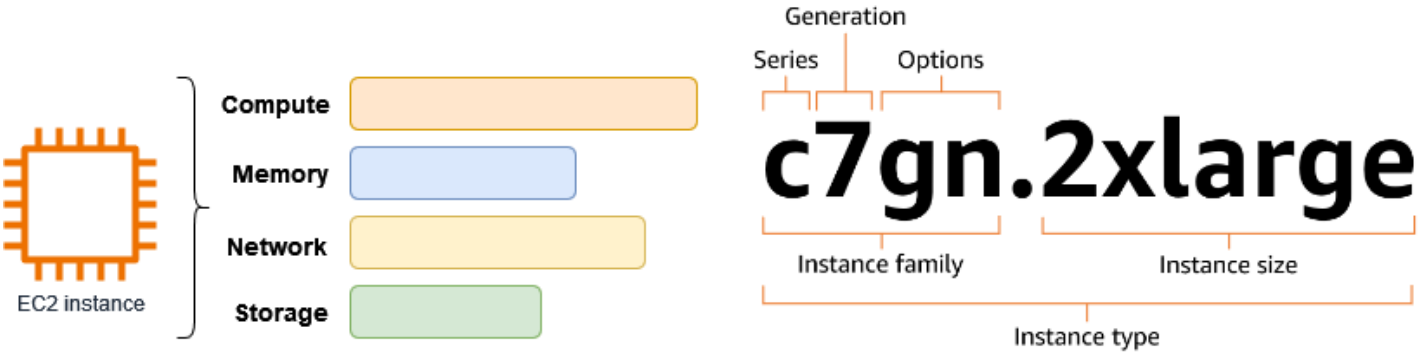
Prompt di GRUB (grubdom>) ... 3879
Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (indirizzo MAC) Hard-coded ... 3882
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (configurazione SELinux errata) ... 3884
XENBUS: Timeout connecting to devices (timeout di Xenbus) ... 3885
Avvio dell'istanza Linux dal volume sbagliato ... 3886
Problematiche RDP relative all'istanza Windows ... 3888
Il desktop remoto non può connettersi al computer remoto ... 3888
Errore durante l'uso del client macOS RDP ... 3890
RDP mostra una schermata nera invece del desktop ... 3890
Impossibile accedere da remoto a un'istanza con un utente che non è un amministratore ... 3891
Risoluzione dei problemi di Remote Desktop utilizzando AWS Systems Manager ... 3891
Abilitazione di Desktop remoto in un'istanza EC2 con il Registro di sistema remoto ... 3895
Ho perso la mia chiave privata. Come posso connettermi alla mia istanza Windows? ... 3897
Problemi di avvio delle istanze Windows ... 3897
"La password non è disponibile" ... 3898
"Password non ancora disponibile" ... 3899
"Impossibile recuperare la password di Windows" ... 3899
"In attesa del servizio di metadati" ... 3899
"Impossibile attivare Windows" ... 3904
"Windows non è originale (0x80070005)" ... 3906
"Nessun server Terminal Server License disponibile per fornire una licenza" ... 3906
"Alcune impostazioni sono gestite dalla tua organizzazione" ... 3907
Problemi relativi all'istanza Windows ... 3907
Impossibile connettersi AWS Systems Manager Sessions Manager su un'istanza di Windows Server 2025 ... 3908
I volumi EBS non vengono inizializzati su Windows Server 2016 e 2019 ... 3908
Avvio di un'istanza EC2 Windows in Directory Services Restore Mode (DSRM) ... 3909
L'istanza perde la connettività di rete oppure le attività programmate non vengono eseguite quando previsto ... 3912
Impossibile ottenere l'output della console ... 3913
Windows Server 2012 R2 non disponibile sulla rete ... 3914
Collisione della firma del disco ... 3914
Debug del kernel delle istanze Windows sulla rete ... 3915
Prerequisiti ... 3916

Passaggio 1: installare gli strumenti di debug di Windows sull'host di debug 3917
Fase 2: Impostare l'obiettivo di debug 3918
Passaggio 3: avviare la sessione di debug sull'host di debug 3920
Passaggio 4: riavviare la destinazione di debug 3921
Pulisci le impostazioni di debug dopo il debug 3921
Limitazioni 3922
Note aggiuntive 3922
Reimposta password dell'amministratore Windows. 3922
Reimpostazione password tramite EC2Launch v2 3924
Reimpostazione password tramite EC2Launch 3929
Reimpostazione password tramite EC2Config 3935
Risoluzione dei problemi relativi a Sysprep 3942
EC2Rescue for istanze Linux 3943
Installazione di EC2Rescue 3944
Esegui comandi EC2Rescue 3948
Sviluppo dei moduli EC2Rescue 3950
EC2Rescue per istanze Windows 3958
Risoluzione dei problemi con la GUI EC2Rescue 3959
Risoluzione dei problemi con la CLI EC2Rescue 3965
Risoluzione dei problemi con EC2Rescue e Systems Manager 3974
Console seriale EC2 3978
Prerequisiti 3979
Configurazione dell'accesso alla console seriale EC2 3987
Connessione alla console seriale EC2 3998
Disconnettiti dalla console seriale EC2 4008
Risoluzione dei problemi relativi all'istanza utilizzando la console seriale EC2 4009
Invio di interruzioni della diagnostica 4018
Tipi di istanze supportati 4019
Prerequisiti 4019
Invio di un'interruzione della diagnostica 4022
Cronologia dei documenti 4023
Cronologia per il 2018 e anni precedenti 4067
..... mmmmxciii

Che cosa è Amazon EC2?

Amazon Elastic Compute Cloud (Amazon EC2) fornisce capacità di calcolo scalabile on demand nel cloud Amazon Web Services (AWS). L'utilizzo di Amazon EC2 riduce i costi hardware in modo da poter sviluppare e implementare applicazioni più velocemente. Puoi utilizzare Amazon EC2 per avviare il numero di server virtuali necessari, configurare la sicurezza e i servizi di rete, nonché gestire l'archiviazione. Puoi aggiungere capacità (aumento) per gestire attività a uso intensivo di calcolo, come processi mensili o annuali o picchi nel traffico del sito Web. Quando l'utilizzo diminuisce, puoi ridurre nuovamente la capacità (riduzione).

Un'istanza EC2 è un server virtuale nel cloud. AWS Quando si avvia un'istanza EC2, il tipo di istanza specificato determina l'hardware disponibile per tale istanza. Ogni tipo di istanza mette a disposizione diverse risorse di calcolo, memoria, rete e archiviazione. Per maggiori informazioni, consulta la Guida ai tipi di istanza Amazon EC2.



Caratteristiche di Amazon EC2

Amazon EC2 offre le seguenti funzionalità di alto livello:

Istanze

- Server virtuali.

Amazon Machine Images (AMI)

- Modelli preconfigurati per le istanze contenenti i pacchetti di bit necessari per il server (compresi il sistema operativo e il software aggiuntivo).

Tipi di istanza

Varie configurazioni di CPU, memoria, archiviazione, capacità di rete e hardware grafico per le istanze.

Volumi Amazon EBS

Volumi di archiviazione persistente per i dati tramite Amazon Elastic Block Store (Amazon EBS).

Volumi di archivio dell'istanza

Volumi di archiviazione per i dati temporanei che verranno eliminati quando l'istanza viene arrestata, ibernata o terminata.

Key pairs (Coppie di chiavi)

Informazioni di accesso sicure per le tue istanze. AWS archivia la chiave pubblica e l'utente archivia la chiave privata in un luogo sicuro.

Gruppi di sicurezza

Un firewall virtuale che consente di specificare i protocolli, le porte e gli intervalli IP di origine che possono raggiungere le istanze e gli intervalli IP di destinazione a cui le istanze possono connettersi.

Amazon EC2 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.

Servizi correlati

Servizi da usare con Amazon EC2

Puoi usarne altre Servizi AWS con le istanze che distribuisci utilizzando Amazon EC2.

Amazon EC2 Auto Scaling

Assicura di disporre del numero corretto di istanze Amazon EC2 disponibili per gestire il carico dell'applicazione.

AWS Backup

Automatizza il backup delle istanze Amazon EC2 e dei volumi Amazon EBS ad esse collegati.

Amazon CloudWatch

Monitora le istanze e i volumi Amazon EBS.

Elastic Load Balancing

Distribuisci automaticamente il traffico delle applicazioni in ingresso tra più istanze.

Amazon GuardDuty

Rileva l'uso potenzialmente non autorizzato o dannoso delle istanze EC2.

EC2 Image Builder

Automatizza la creazione, la gestione e l'implementazione di immagini server personalizzate, sicure e aggiornate.

AWS Launch Wizard

Dimensiona, configura e distribuisci AWS risorse per applicazioni di terze parti senza dover identificare e fornire manualmente le singole risorse. AWS

AWS Systems Manager

Esegui operazioni su larga scala sulle istanze EC2 con questa soluzione di gestione end-to-end sicura.

Servizi di calcolo aggiuntivi

Puoi avviare istanze utilizzando un altro servizio di AWS elaborazione anziché Amazon EC2.

Amazon Lightsail

Crea siti Web o applicazioni Web utilizzando Amazon Lightsail, una piattaforma cloud che fornisce le risorse necessarie per implementare rapidamente il tuo progetto a un prezzo mensile basso e prevedibile. Per confrontare Amazon EC2 e Lightsail, consulta Amazon Lightsail o Amazon EC2.

Amazon Elastic Container Service (Amazon ECS)

Implementa, gestisci e dimensiona le applicazioni containerizzate su un cluster di istanze EC2. Per ulteriori informazioni, consulta Scelta di un servizio container. AWS

Amazon Elastic Kubernetes Service (Amazon EKS)

Esegui le tue applicazioni Kubernetes su AWS. Per ulteriori informazioni, vedere Scelta di un servizio AWS container.

Accesso a Amazon EC2

È possibile creare e gestire le istanze Amazon EC2 utilizzando le seguenti interfacce:

Console Amazon EC2

Una semplice interfaccia Web per creare e gestire istanze e risorse Amazon EC2. Se hai registrato un AWS account, puoi accedere alla console Amazon EC2 accedendo Console di gestione AWS e selezionando EC2 dalla home page della console.

AWS Command Line Interface

Consente di interagire con i AWS servizi utilizzando i comandi nella shell della riga di comando. È supportata su Windows, Mac e Linux. Per ulteriori informazioni sulla AWS CLI , consulta la Guida per l'utente di AWS Command Line Interface. Puoi trovare i comandi di Amazon EC2 nella Documentazione di riferimento ai comandi di AWS CLI.

CloudFormation

Amazon EC2 supporta la creazione di risorse utilizzando CloudFormation. Crei un modello, in formato JSON o YAML, che descrive AWS le tue risorse e fornisce e configura CloudFormation tali risorse per te. Puoi riutilizzare i CloudFormation modelli per fornire le stesse risorse più volte, nella stessa regione e account o in più aree e account. Per ulteriori informazioni sui tipi di risorse supportati e sulle proprietà di Amazon EC2, consulta la sezione Riferimento al tipo di risorsa EC2 nella Guida per l'utente di AWS CloudFormation .

AWS SDK

Se preferisci creare applicazioni utilizzando API specifiche per una lingua anziché inviare una richiesta tramite HTTP o HTTPS, AWS fornisce librerie, codice di esempio, tutorial e altre risorse per gli sviluppatori di software. Le librerie offrono funzioni di base per automatizzare attività quali la firma crittografica delle richieste, la ripetizione delle richieste e la gestione delle risposte agli errori, semplificando le attività iniziali. Per ulteriori informazioni, consulta Strumenti per creare su AWS.

AWS Strumenti per PowerShell

Un insieme di PowerShell moduli che si basano sulle funzionalità esposte da. SDK per .NET Gli strumenti PowerShell consentono di eseguire operazioni di script sulle AWS risorse dalla PowerShell riga di comando. Per iniziare, consulta la AWS Strumenti per PowerShell Guida per l'utente di . Puoi trovare i cmdlet per Amazon EC2 nella Documentazione di riferimento di AWS Strumenti per PowerShell Cmdlet.

API della query

Amazon EC2 fornisce un'API di query. Queste richieste sono richieste HTTP o HTTPS che utilizzano i verbi HTTP GET o POST e un parametro di query denominato `Action`. Per ulteriori informazioni sulle operazioni dell'API per Amazon EC2, consulta la sezione relativa alle operazioni della Amazon EC2 API Reference.

Prezzi delle Amazon EC2

Amazon EC2 offre le seguenti opzioni di prezzo:

Piano gratuito

È possibile iniziare a utilizzare Amazon EC2 gratuitamente. Per esplorare le opzioni del piano gratuito, consulta Piano gratuito di AWS.

On-Demand Istanze

Pagamenti per le istanze utilizzate al secondo, con un minimo di 60 secondi, senza impegni a lungo termine o pagamenti anticipati.

Savings Plans

Puoi ridurre i costi di Amazon EC2 e svolgere una serie di attività, in USD per ora, per un periodo di uno o tre anni.

Reserved Instances

Puoi ridurre i costi Amazon EC2 utilizzando un'istanza specifica per una configurazione di istanza specifica, incluso il tipo di istanza e la regione, per un periodo di uno o tre anni.

Spot Instances

Consente di richiedere istanze EC2 inutilizzate, in grado di ridurre i costi di Amazon EC2 in modo significativo.

Host dedicati

Riduci i costi utilizzando un server EC2 fisico completamente dedicato al tuo utilizzo, On-Demand o come parte di un Savings Plan. Puoi utilizzare le licenze software esistenti legate al server e ottenere assistenza per soddisfare i requisiti di conformità.

On-Demand Prenotazioni di capacità

Prenota capacità di calcolo per le istanze EC2 per qualsiasi durata in una determinata zona di disponibilità.

Per-second fatturazione

Rimuove dalla fattura il costo dei minuti e dei secondi inutilizzati.

Per un elenco completo delle tariffe e dei prezzi specifici per Amazon EC2 e per ulteriori informazioni sui modelli di acquisto, consulta la sezione Prezzi di Amazon EC2.

Stime, fatturazione e ottimizzazione dei costi

Per creare stime per i tuoi casi AWS d'uso, usa il Calcolatore dei prezzi AWS.

Per stimare il costo della trasformazione dei carichi di lavoro Microsoft in un'architettura moderna che utilizza servizi open source e nativi del cloud distribuiti su AWS, usa il Modernization AWS Calculator for Microsoft Workloads.

Per vedere la tua fattura, vai sul Pannello di controllo di gestione dei costi e della fatturazione nella console Gestione costi e fatturazione AWS. La fattura contiene collegamenti per passare ai report di utilizzo, che consentono di visualizzare i dettagli della fattura. Per ulteriori informazioni sulla fatturazione AWS dell'account, consulta la Guida per l'utente di AWS Billing and Cost Management.

In caso di domande relative alla AWS fatturazione, agli account e agli eventi, contatta l' AWS assistenza.

Per calcolare il costo di un ambiente con provisioning di esempio, consultare Cloud Economics Center. Quando si calcola il costo di un ambiente con provisioning, ricordare di includere costi accidentali come l'archiviazione snapshot per i volumi EBS.

È possibile ottimizzare i costi, la sicurezza e le prestazioni del proprio AWS ambiente utilizzando AWS Trusted Advisor.

Puoi utilizzarlo AWS Cost Explorer per analizzare il costo e l'utilizzo delle tue istanze EC2. Puoi visualizzare i dati fino agli ultimi 13 mesi e prevedere le tue spese nei prossimi 12 mesi. Per ulteriori informazioni, consulta Analyzing your costs and usage with AWS Cost Explorer nella Guida per l'utente di AWS Cost Management .

Resources

- Caratteristiche di Amazon EC2
- AWS Re: post
- AWS Skill Builder
- AWS Support
- Hands-on Tutorial
- Web hosting
- Windows attivo AWS

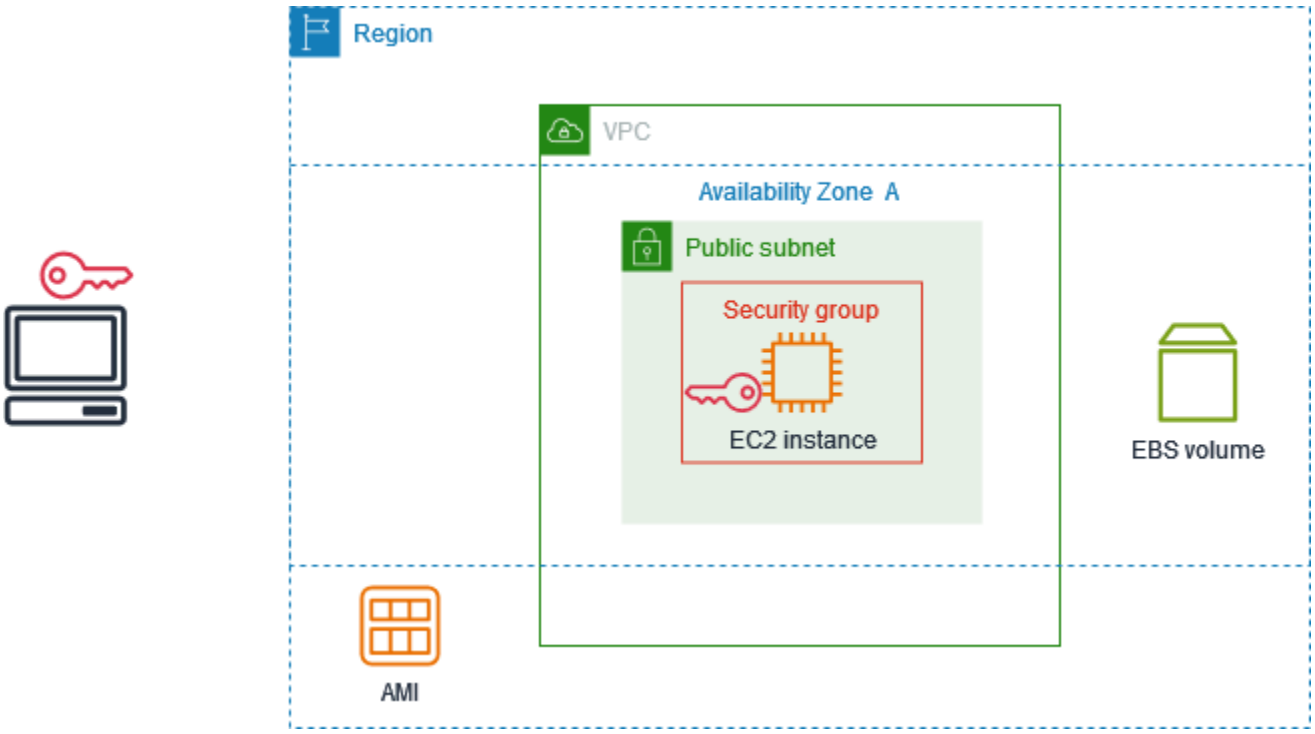
Nozioni di base su Amazon EC2

Utilizza questo tutorial per iniziare a usare Amazon Elastic Compute Cloud (Amazon EC2). Scoprirai come avviare e connettere un'istanza EC2. Un'istanza è un server virtuale nel AWS cloud. Con Amazon EC2, puoi installare e configurare il sistema operativo e le applicazioni eseguiti sull'istanza.

Panoramica di

Il seguente diagramma illustra i componenti principali che verranno utilizzati in questo tutorial:

- Un'immagine: – Un modello che contiene il software da eseguire sull'istanza, come il sistema operativo.
- Una coppia di chiavi – Un set di credenziali di sicurezza che puoi utilizzare per dimostrare la tua identità quando ti colleghi alla tua istanza. La chiave pubblica è nella tua istanza e la chiave privata è nel tuo computer.
- Una rete – Un cloud privato virtuale (VPC) è una rete virtuale dedicata nel tuo Account AWS. Per aiutarti a iniziare rapidamente, il tuo account include un VPC predefinito in ogni VPC predefinito e ogni Regione AWS VPC predefinito ha una sottorete predefinita in ciascuna zona di disponibilità.
- Un gruppo di sicurezza – Agisce da firewall virtuale per controllare il traffico in entrata e in uscita.
- Un volume EBS: per l'immagine è necessario un volume principale. Facoltativamente, è possibile anche aggiungere volumi di dati.



Costo di questo tutorial

Quando crei il tuo Account AWS, puoi iniziare a usare Amazon EC2 gratuitamente utilizzando. Piano gratuito di AWS

Se hai creato il tuo Account AWS prima del 15 luglio 2025, ha meno di 12 mesi e non hai ancora superato i vantaggi del piano gratuito per Amazon EC2, completare questo tutorial non ti costerà nulla, perché questo tutorial ti aiuta a selezionare le opzioni che rientrano nei vantaggi del piano gratuito. In caso contrario, ti verranno addebitati i costi di utilizzo standard di Amazon EC2 dal momento in cui avvii l'istanza (anche se rimane inattiva) fino alla sua interruzione.

Se hai creato il tuo Account AWS account il 15 luglio 2025 o dopo, ha meno di 6 mesi e non hai esaurito tutti i tuoi crediti, completare questo tutorial non ti costerà nulla, perché questo tutorial ti aiuta a selezionare le opzioni che rientrano nei vantaggi del livello gratuito.

Per istruzioni su come determinare se disponi dell'idoneità al Piano gratuito, consulta the section called "Monitoraggio dell'utilizzo del piano gratuito".

Processi

- Fase 1: avvio di un'istanza
- Fase 2. connessione all'istanza
- Fase 3. pulizia di un'istanza

- Fasi successive

Fase 1: avvio di un'istanza

Puoi avviare un'istanza EC2 utilizzando la procedura Console di gestione AWS descritta nella seguente procedura. La finalità di questo tutorial è aiutarti ad avviare in modo semplice e rapido la prima istanza. Pertanto, non verranno descritte tutte le possibili opzioni.

Per avviare un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore dello schermo, Regione AWS viene visualizzata la corrente, ad esempio Ohio. Puoi utilizzare la regione selezionata o, facoltativamente, selezionare una regione più vicina a te.
3. Nel pannello di controllo della console EC2, nel riquadro Avvia istanza, scegli Avvia istanza.
4. In Name and tags (Nome e tag), per Name (Nome), inserisci un nome descrittivo per l'istanza.
5. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), esegui la seguente operazione:

   a. Scegli Avvio rapido, poi seleziona il sistema operativo (SO) per la tua istanza. Per la tua prima istanza Linux, ti consigliamo di scegliere Amazon Linux.

   b. Da Amazon Machine Image (AMI), seleziona un'AMI contrassegnata come Idonea al piano gratuito.
6. In Tipo di istanza, per Tipo di istanza, seleziona un tipo di istanza contrassegnato come Idoneo per il Piano gratuito.
7. In Coppia di chiavi (accesso), per Nome coppia di chiavi, scegli una coppia di chiavi esistente oppure scegli Crea nuova coppia di chiavi per creare la tua prima coppia di chiavi.

   > **Warning**
   >
   > Se scegli Procedi senza una coppia di chiavi (Non consigliato), non potrai connetterti all'istanza utilizzando i metodi descritti in questo tutorial.
8. In Impostazioni di rete, notate che è selezionato il VPC predefinito, l'opzione per utilizzare la sottorete predefinita in una zona di disponibilità scelta per voi e un gruppo di sicurezza con una regola che consente le connessioni all'istanza da qualsiasi luogo (). `0.0.0.0/0`

> **Warning**
>
> Se specifichi `0.0.0.0/0`, abiliti il traffico da qualsiasi indirizzo IP nel mondo. Per i protocolli SSH e RDP, potresti considerarlo accettabile per un breve periodo di tempo in un ambiente di test, ma non è sicuro per gli ambienti di produzione. In produzione, assicurati di autorizzare l'accesso solo dall'indirizzo IP individuale o dall'intervallo di indirizzi appropriato.

Per la tua prima istanza, consigliamo di mantenere le impostazioni predefinite. In caso contrario, puoi aggiornare le impostazioni di rete come indicato di seguito:

- (Facoltativo) Per utilizzare una sottorete predefinita specifica, scegli Modifica, poi scegli una sottorete.
- (Facoltativo) Per utilizzare un VPC diverso, scegli Modifica, poi scegli un VPC esistente. Se il VPC non è configurato per l'accesso pubblico a Internet, non potrai connetterti alla tua istanza.
- (Facoltativo) Per limitare il traffico di connessione in entrata a una rete specifica, scegli Personalizzato anziché Ovunque e inserisci il blocco CIDR per la rete.
- (Facoltativo) Per utilizzare un gruppo di sicurezza esistente, scegli Seleziona un gruppo di sicurezza esistente, e scegli un gruppo di sicurezza esistente. Se il gruppo di sicurezza non dispone di una regola che consenta il traffico di connessione dalla rete, non potrai connetterti alla tua istanza. Per un'istanza Linux, devi consentire il traffico SSH. Per un'istanza Windows, devi consentire il traffico RDP.

9. In Configura archiviazione, notate che è configurato un volume principale ma non un volume di dati. Questo è sufficiente per scopi di prova.
10. Analizza un riepilogo della configurazione dell'istanza nel pannello Summary (Riepilogo) e, quando è tutto pronto, scegli Launch instance (Avvia istanza).
11. Se il lancio ha esito positivo, scegli l'ID dell'istanza dalla notifica di successo per aprire la pagina Istanze e monitorare lo stato dell'avvio.
12. Seleziona la casella di controllo relativa all'istanza. Lo stato iniziale dell'istanza è `pending`. Dopo l'avvio di dell'istanza, il suo stato diventa `running`. Scegli la scheda Stato e allarmi. Dopo aver superato le verifiche dello stato, l'istanza è pronta a ricevere le richieste di connessione.

Fase 2. connessione all'istanza

La procedura utilizzata dipende dal sistema operativo dell'istanza. Se non riesci a collegarti all'istanza, consulta Risoluzione dei problemi di connessione all'istanza Linux di Amazon EC2 per ricevere assistenza.

Istanze Linux

Puoi connetterti all'istanza Linux tramite qualsiasi client SSH. Se utilizzi Windows sul tuo computer, apri un terminale ed esegui il comando `ssh` per verificare che sia installato un client SSH. Se il comando non viene trovato, installa OpenSSH per Windows.

Per connettersi all'istanza tramite SSH

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza quindi scegli Connect (Connetti).
4. Nella pagina Connettiti all'istanza, scegli la scheda Client SSH.
5. (Facoltativo) Se hai creato una coppia di chiavi all'avvio dell'istanza e hai scaricato la chiave privata (file.pem) su un computer che utilizza Linux o macOS, esegui il comando di esempio chmod per impostare le autorizzazioni per la tua chiave privata.
6. Copia il comando di esempio SSH. Di seguito è riportato un esempio, dove *key-pair-name* .pem è il nome del file della chiave privata, *ec2-user* è il nome utente associato all'immagine e la stringa dopo il simbolo @ è il nome DNS pubblico dell'istanza.

   ```
   ssh -i key-pair-name.pem ec2-user@ec2-198-51-100-1.us-east-2.compute.amazonaws.com
   ```

7. In una finestra del terminale del computer, esegui il comando ssh da te salvato nella fase precedente. Se il file della chiave privata non è presente nella directory attuale, devi specificare il percorso completo per il file della chiave in questo comando.

   Di seguito è riportata una risposta di esempio:

   ```
   The authenticity of host 'ec2-198-51-100-1.us-east-2.compute.amazonaws.com
    (198-51-100-1)' can't be established.
   ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
   Are you sure you want to continue connecting (yes/no)?
   ```

8. (Facoltativo) Verifica che l'impronta nell'avviso di sicurezza corrisponda all'impronta dell'istanza nell'output della console al momento del primo avvio di un'istanza. Per ottenere l'output della console, scegli Operazioni, Monitoraggio e risoluzione dei problemi, Ottieni log di sistema. Se le impronte digitali non corrispondono, qualcuno potrebbe tentare un attacco man-in-the-middle. Se invece corrispondono, passare alla fase successiva.
9. Specificare (sì **`yes`**.

   Di seguito è riportata una risposta di esempio:

```
Warning: Permanently added 'ec2-198-51-100-1.us-
east-2.compute.amazonaws.com' (ECDSA) to the list of known hosts.
```

Istanze Windows

Per connettersi a un'istanza di Windows usando RDP, è necessario recuperare la password iniziale dell'amministratore e immetterla quando ci si connette all'istanza. Dopo l'avvio dell'istanza, dovrai attendere alcuni minuti prima che la password sia disponibile. Il tuo account deve disporre dell'autorizzazione per richiamare l'azione. GetPasswordData Per ulteriori informazioni, consulta Policy di esempio da utilizzare all'API Amazon EC2.

Il nome utente predefinito per l'account amministratore dipende dalla lingua del sistema operativo (OS) contenuto nell'AMI. Per verificare il nome utente corretto, identifica la lingua del sistema operativo, poi scegli il nome utente corrispondente. Ad esempio, per un sistema operativo in inglese, il nome utente è `Administrator`, per un sistema operativo in francese è `Administrateur` e per un sistema operativo portoghese è `Administrador`. Se una versione di lingua del sistema operativo non ha un nome utente nella stessa lingua, scegli il nome utente `Administrator (Other)`. Per ulteriori informazioni, consulta Nomi localizzati dell'account amministratore in Windows nel sito Web di Microsoft.

Per recuperare la password dell'amministratore iniziale

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza quindi scegli Connect (Connetti).
4. Nella pagina Connettiti all'istanza, scegli la scheda Client RDP.
5. Per Nome utente, scegli il nome utente predefinito per l'account amministratore. Il nome utente scelto deve corrispondere alla lingua del sistema operativo (OS) contenuto nell'AMI utilizzata per

avviare l'istanza. Se non esiste un nome utente nella stessa lingua del sistema operativo, scegli Amministratore (Altro).

6. Scegliere Ottieni password.
7. Nella pagina Ottieni password di Windows, procedi nel modo seguente:

   a. Scegli Carica file della chiave privata e individua il file della chiave privata (`.pem`) da te specificato al momento dell'avvio dell'istanza. Selezionare il file e scegliere Open (Apri) per copiare l'intero contenuto del file in questa finestra.

   b. Selezionare Decifra password. La pagina Ottieni password Windows si chiude e la password di amministratore predefinita per l'istanza viene visualizzata in Password, sostituendo il link Ottieni password mostrato in precedenza.

   c. Copia la password e salvala in un luogo sicuro. Questa password ti servirà per connetterti all'istanza.

La procedura seguente utilizza il client Remote Desktop Connection per Windows (MSTSC). Se utilizzi un client RDP diverso, scarica il file RDP e consulta la documentazione per il client RDP per i passaggi necessari per stabilire la connessione RDP.

Per connetterti a un'istanza Windows utilizzando un client RDP

1. Nella pagina Connettiti all'istanza, scegli Scarica file desktop remoto. Al termine del download del file, scegli Annulla per tornare alla pagina Istanze. Il file RDP viene scaricato nella tua cartella `Downloads`.
2. Esegui `mstsc.exe` per aprire il client RDP.
3. Espandi Mostra opzioni, scegli Apri e seleziona il file.rdp dalla cartella `Downloads`.
4. Per impostazione predefinita, Computer è il nome DNS IPv4 pubblico dell'istanza e Nome utente è l'account amministratore. Per connetterti all'istanza utilizzando invece IPv6, sostituisci il nome DNS IPv4 pubblico dell'istanza con il relativo indirizzo IPv6. Rivedi le impostazioni predefinite e modificale come necessario.
5. Scegli Connetti. Se ricevi un avviso che il publisher della connessione remota non è noto, scegli Connetti per continuare.
6. Inserisci la password salvata in precedenza, poi scegli OK.
7. Data la natura dei certificati autofirmati, è possibile che venga visualizzato un avviso relativo all'impossibilità di autenticare il certificato di sicurezza. Esegui una delle seguenti operazioni:
   - Se consideri attendibile il certificato, scegli Sì per connetterti all'istanza.

- [Windows] Prima di procedere, confronta l'impronta digitale del certificato con il valore nel log di sistema per confermare l'identità del computer remoto. Scegli Visualizza certificato e poi seleziona Identificazione personale dalla scheda Dettagli. Confronta questo valore con il valore di `RDPCERTIFICATE-THUMBPRINT` in Operazioni, Monitoraggio e risoluzione dei problemi, Ottieni log di sistema.
- [Mac OS X] Prima di procedere, confronta l'impronta del certificato con il valore nel log di sistema per confermare l'identità del computer remoto. Scegli Mostra certificato, espandi Dettagli e seleziona Impronte digitali SHA1. Confronta questo valore con il valore di `RDPCERTIFICATE-THUMBPRINT` in Operazioni, Monitoraggio e risoluzione dei problemi, Ottieni log di sistema.

8. Se la connessione RDP ha esito positivo, il client RDP visualizza la schermata di accesso di Windows e poi il desktop di Windows. Se invece ricevi un messaggio di errore, consulta the section called "Il desktop remoto non può connettersi al computer remoto". Quando hai completato la connessione RDP, puoi chiudere il client RDP.

Fase 3. pulizia di un'istanza

> **Warning**
>
> La terminazione di un'istanza è permanente e irreversibile.
> Dopo aver terminato un'istanza, non puoi più connetterti a essa e non puoi ripristinarla. Inoltre, tutti i volumi Amazon EBS collegati e configurati per essere eliminati in caso di terminazione vengono eliminati in modo definitivo e non possono essere recuperati. Tutti i dati archiviati nei volumi di archivio dell'istanza vengono persi in modo definitivo. Per ulteriori informazioni, consulta Come funziona la terminazione delle istanze.
> Prima di terminare un'istanza, assicurati di aver eseguito il backup di tutti i dati che devi mantenere dopo la terminazione sull'archivio persistente.

Dopo aver creato l'istanza per questo tutorial, è consigliabile eseguire la pulizia mediante l'interruzione dell'istanza. Per eseguire altre operazioni con questa istanza prima di eseguire la pulizia, consulta Fasi successive.

Non incorrerai in altri costi per quell'istanza o l'utilizzo che rientra nei limiti del piano gratuito non appena lo stato dell'istanza diventa `shutting down` o `terminated`. Per mantenere l'istanza per un secondo momento, ma non sostenerne i costi o l'utilizzo entro i limiti del piano gratuito, puoi arrestare

ora l'istanza e poi riavviarla più tardi. Per ulteriori informazioni, consulta Avvio e arresto di un'istanza Amazon EC2.

Per terminare l'istanza

1. Nel riquadro di navigazione, seleziona Instances (Istanze). Nell'elenco delle istanze, selezionare l'istanza.
2. Scegli Stato dell'istanza, Termina (elimina) istanza.
3. Quando viene richiesta la conferma, scegli Termina (elimina).

   Amazon EC2 arresta e termina l'istanza. Dopo averla terminata, l'istanza rimane visibile sulla console per un breve periodo di tempo, quindi la voce verrà eliminata automaticamente. L'utente non può rimuovere l'istanza terminata dal display della console.

Fasi successive

Dopo aver avviato l'istanza, potresti provare ad analizzare le seguenti fasi successive:

- Esplora i concetti fondamentali di Amazon EC2 con i tutorial introduttivi. Per ulteriori informazioni, consulta Tutorial per avviare istanze EC2.
- Scopri come tenere traccia dell'utilizzo del piano gratuito di Amazon EC2 tramite la console. Per ulteriori informazioni, consulta the section called “Monitoraggio dell'utilizzo del piano gratuito”.
- Configura un CloudWatch allarme per avvisarti se il tuo utilizzo supera il livello gratuito (per gli account creati prima del 15 luglio 2025). Per ulteriori informazioni, consulta Monitoraggio dell'utilizzo di Piano gratuito di AWS nella Guida per l'utente AWS Billing .
- Installa un volume EBS. Per ulteriori informazioni, consulta Creare un volume di Amazon EBS nella Guida per l'utente di Amazon EBS.
- Scopri come gestire in remoto l'istanza EC2 utilizzando il comando Run. Per ulteriori informazioni, consulta Run Command AWS Systems Manager nella Guida per l'utente AWS Systems Manager .
- Scopri le opzioni di acquisto delle istanze. Per ulteriori informazioni, consulta Opzioni di fatturazione e acquisto di Amazon EC2.
- Ottieni i dati sui tipi di istanze. Per ulteriori informazioni, consulta Ottieni consigli dallo strumento di ricerca del tipo di istanza EC2.

Best practice per Amazon EC2

Per ottenere il massimo vantaggio da Amazon EC2, ti consigliamo di eseguire le best practice seguenti.

Sicurezza

- Gestisci l'accesso alle AWS risorse e APIs utilizza la federazione delle identità con un provider di identità e ruoli IAM quando possibile. Per ulteriori informazioni, consulta Provider di identità e federazione nella Guida per l'utente IAM.
- Implementa regole meno permissive per il gruppo di sicurezza.
- Applica patch, aggiorna e proteggi con regolarità il sistema e le applicazioni nell'istanza. Per ulteriori informazioni, consulta Gestione degli aggiornamenti. Per linee guida specifiche per i sistemi operativi Windows, consulta Procedure ottimali relative alla sicurezza delle istanze Windows.
- Utilizza Amazon Inspector per individuare e scansionare automaticamente le istanze Amazon EC2 alla ricerca di vulnerabilità software ed esposizione alla rete non intenzionale. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon Inspector.
- Usa AWS Security Hub CSPM i controlli per monitorare le tue risorse Amazon EC2 rispetto alle best practice e agli standard di sicurezza. Per ulteriori informazioni sull'uso di Security Hub CSPM, consulta i controlli di Amazon Elastic Compute Cloud nella Guida per l'AWS Security Hub CSPM utente.

Archiviazione

- Valuta le implicazioni del tipo di volume root per quanto riguarda la persistenza, il backup e il ripristino dei dati. Per ulteriori informazioni, consulta Tipo di volume root.
- Utilizza volumi Amazon EBS distinti per il sistema operativo e per i dati. Assicurati che il volume contenente i dati sia persistente dopo l'interruzione dell'istanza. Per ulteriori informazioni, consulta Conservare i dati quando un'istanza viene terminata.
- Utilizza l'instance store disponibile per l'istanza per archiviare i dati temporanei. Ricorda che i dati archiviati nell'instance store vengono eliminati quando arresti o interrompi l'istanza. Se utilizzi un instance store per lo storage dei database, assicurati di disporre di un cluster con un fattore di replica che garantisca la tolleranza ai guasti.

- Crittografare volumi e snapshot EBS. Per ulteriori informazioni, consulta Crittografia Amazon EBS nella Guida per l'utente di Amazon EBS.

Gestione delle risorse

- Utilizza i metadati dell'istanza e i tag di risorsa personalizzati per monitorare e identificare le risorse AWS . Per ulteriori informazioni, consulta Utilizzo dei metadati dell'istanza per gestire l'istanza EC2 e Tagging delle risorse Amazon EC2..
- Visualizza le restrizioni correnti valide per Amazon EC2. Pianifica le richieste di incremento dei limiti con un certo anticipo rispetto a quando ne avrai effettivamente bisogno. Per ulteriori informazioni, consulta Service Quotas di Amazon EC2.
- Utilizzali AWS Trusted Advisor per ispezionare il tuo AWS ambiente e poi formulare consigli quando esistono opportunità per risparmiare denaro, migliorare la disponibilità e le prestazioni del sistema o contribuire a colmare le lacune di sicurezza. Per ulteriori informazioni, consulta AWS Trusted Advisor nella Guida per l'utente di Supporto AWS .

Backup e ripristino

- Esegui regolarmente il backup dei volumi EBS utilizzando gli snapshot Amazon EBS e crea un' Amazon Machine Image (AMI) dall'istanza per salvare la configurazione come modello per l'avvio delle istanze future. Per ulteriori informazioni sui AWS servizi che aiutano a raggiungere questo caso d'uso, consulta AWS BackupAmazon Data Lifecycle Manager.
- Distribuisci i componenti di importanza critica dell'applicazione in più zone di disponibilità e replica i dati di conseguenza.
- Progetta le applicazioni in modo che siano in grado di gestire l'indirizzamento IP dinamico quando l'istanza viene riavviata. Per ulteriori informazioni, consulta Indirizzamento IP per le istanze Amazon EC2.
- Esegui il monitoraggio degli eventi e rispondi agli eventi. Per ulteriori informazioni, consulta Monitoraggio delle risorse Amazon EC2.
- Assicurati di essere preparato a gestire situazioni di failover. Come soluzione di base puoi collegare manualmente un'interfaccia di rete o un indirizzo IP elastico a un'istanza di sostituzione. Per ulteriori informazioni, consulta Interfacce di rete elastiche. Per una soluzione automatizzata, puoi utilizzare Amazon EC2 Auto Scaling. Per ulteriori informazioni, consulta Guida per l'utente di Amazon EC2 Auto Scaling.

- Esegui regolarmente dei test del processo di recupero di istanze e volumi Amazon EBS per garantire che i dati e i servizi vengano ripristinati correttamente.

Reti

- Imposta il valore time-to-live (TTL) per le tue applicazioni su 255, per e. IPv4 IPv6 Se si utilizza un valore inferiore, esiste il rischio che il TTL scada mentre il traffico dell'applicazione è in transito, causando problemi di raggiungibilità per le istanze.

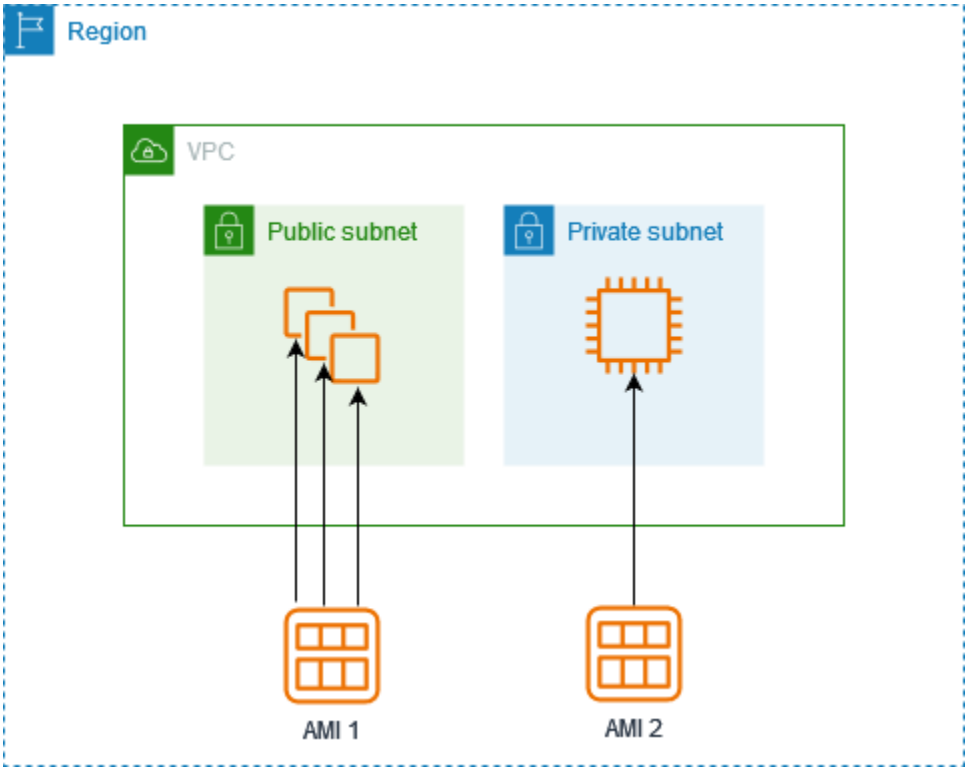
Amazon Machine Image in Amazon EC2

Un'Amazon Machine Image (AMI) è un'immagine che fornisce il software richiesto per impostare e avviare un'istanza Amazon EC2. Ogni AMI contiene anche una mappatura dei dispositivi a blocchi che specifica i dispositivi a blocchi da collegare alle istanze che vengono lanciate. Devi specificare un'AMI quando avvii un'istanza. Il tipo di istanza deve essere compatibile con il tipo di istanza scelto per la tua istanza. Puoi utilizzare un'AMI fornita da AWS, un'AMI pubblica, un'AMI che qualcun altro ha condiviso con te o un'AMI che hai acquistato da Marketplace AWS.

Un'AMI è specifica per quanto segue:

- Region
- Sistema operativo
- Architettura del processore
- Tipo di volume root
- Tipo di virtualizzazione

Puoi avviare più istanze da un'unica AMI quando devi disporre di più istanze con la stessa configurazione. Puoi utilizzare AMI diverse per avviare istanze quando devi disporre di istanze con configurazioni diverse, come mostrato nel seguente diagramma.



Puoi creare un'AMI dalle tue istanze Amazon EC2 e poi usarla per avviare istanze con la stessa configurazione. Puoi copiare un'AMI in un'altra AWS regione e quindi utilizzarla per avviare istanze in quella regione. Puoi anche condividere un'AMI che hai creato con altri account in modo tale che possano avviare istanze con la stessa configurazione. Puoi vendere la tua AMI utilizzando il Marketplace AWS.

Indice

- Tipi di AMI e caratteristiche in Amazon EC2
- Trova una AMI che soddisfi i requisiti per l'istanza EC2
- AMI a pagamento in Marketplace AWS per istanze Amazon EC2
- Ciclo di vita dell'AMI di Amazon EC2
- Comportamento di avvio delle istanze con le modalità di avvio di Amazon EC2
- Usa la crittografia con le EBS-backed AMI
- Informazioni sull'utilizzo delle AMI condivise in Amazon EC2
- Monitora gli eventi AMI utilizzando Amazon EventBridge
- Comprendere le informazioni di fatturazione AMI
- Quote AMI in Amazon EC2

Tipi di AMI e caratteristiche in Amazon EC2

Quando si avvia un'istanza, l'AMI scelta deve essere compatibile con il tipo di istanza scelta. Puoi selezionare un'AMI da utilizzare in base alle seguenti caratteristiche:

- Region
- Sistema operativo
- Architettura del processore
- Permessi di avvio
- Tipo di volume root
- Tipi di virtualizzazione

Permessi di avvio

Le autorizzazioni di avvio determinano chi può utilizzare un'AMI per avviare le istanze. Puoi considerare le autorizzazioni di avvio come la condivisione di un'AMI: quando concedi le autorizzazioni di avvio, condividi l'AMI con altri utenti. Solo il proprietario di un'AMI può determinarne la disponibilità specificando le autorizzazioni di avvio. I permessi di avvio sono suddivisi nelle seguenti categorie.

Permesso di avvio	Descrizione
pubblico	Il proprietario concede le autorizzazioni di avvio a tutti gli AWS account.
esplicito	Il proprietario concede le autorizzazioni di avvio a specifici AWS account, organizzazioni o unità organizzative (OU).
implicito	Il proprietario concede permessi di avvio impliciti per un'AMI.

Amazon e la community Amazon EC2 mettono a disposizione un'ampia selezione di AMI pubbliche. Per ulteriori informazioni, consulta Informazioni sull'utilizzo delle AMI condivise in Amazon EC2. Gli sviluppatori possono richiedere un pagamento per le proprie AMI. Per ulteriori informazioni, consulta AMI a pagamento in Marketplace AWS per istanze Amazon EC2.

Tipo di volume root

Tutte le AMI sono suddivise tra AMI supportate da Amazon EBS e AMI supportate da Amazon S3.

- Amazon EBS-backed AMI: il volume principale di un'istanza avviata dall'AMI è un volume Amazon Elastic Block Store (Amazon EBS) creato da un'istantanea di Amazon EBS. Supportato per le AMI di Linux e Windows.
- Amazon S3-backed AMI: il volume principale di un'istanza avviata dall'AMI è un volume di archivio di istanze creato da un modello archiviato in Amazon S3. Supportato solo per le AMI di Linux. Le AMI di Windows non supportano l'archivio istanza per il volume root.

Per ulteriori informazioni, consulta Volumi root per le tue istanze Amazon EC2.

> **Note**
>
> Le S3-backed AMI Amazon sono considerate fuori uso e non sono consigliate per un nuovo utilizzo. Sono supportate solo sui seguenti tipi di istanze meno recenti: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

La tabella seguente offre un riepilogo delle principali differenze relative all'utilizzo dei due tipi di AMI.

Caratteristica	AMI Amazon EBS-backed	S3-backed AMI Amazon
Volume root	Volume EBS	Volume di instance store
Tempo di avvio di un'istanza	In genere meno di 1 minuto	In genere meno di 5 minuti
Persistenza dei dati	Per impostazione predefinita, il volume root viene eliminato quando viene terminata l'istanza .* I dati su qualsiasi altro volume EBS sono persistenti dopo l'interruzione dell'istanza per impostazione predefinita.	I dati in qualsiasi volume instance store sono persistenti solo durante il ciclo di vita dell'istanza.

Caratteristica	AMI Amazon EBS-backed	S3-backed AMI Amazon
Stato arrestato	Può essere in uno stato di arresto. Anche quando l'istanza viene arrestata e non in è esecuzione, il volume root viene mantenuto in Amazon EBS.	Non possono essere in stato arrestate; le istanze sono in esecuzione o terminate.
Modifiche	Il tipo di istanza, il kernel, il disco RAM e i dati utente possono essere modificati mentre l'istanza è arrestata.	Gli attributi di istanza sono fissi per la durata di un'istanza.
Costi	Ti vengono addebitati i costi per l'utilizzo dell'istanza, l'utilizzo del volume EBS e l'archiviazione dell'AMI come snapshot EBS.	Ti vengono addebitati i costi per l'utilizzo dell'istanza e l'archivi azione dell'AMI in Amazon S3.
AMI creation/bundling	Utilizza un singolo command/call	Richiede l'installazione e l'utilizzo degli strumenti AMI

* Per impostazione predefinita, i volumi root EBS hanno il flag `DeleteOnTermination` impostato su `true`. Per informazioni su come modificare questo flag in modo che il volume sia persistente dopo l'interruzione, consulta Conservazione di un volume root Amazon EBS dopo aver terminato un'istanza Amazon EC2.

** Supportato solo con `io2` EBS Block Express. Per ulteriori informazioni, consulta i volumi SSD Block Express con capacità di IOPS allocata nella Guida per l'utente di Amazon EBS.

Individua il tipo di volume root determinato dalla tua AMI

L'AMI utilizzata per avviare l'istanza EC2 determina il tipo di volume root. Il volume root di un'istanza EC2 è un volume EBS o un volume di archivio dell'istanza.

Nitro-based le istanze supportano solo i volumi root EBS. I seguenti tipi di istanza della generazione precedente sono gli unici tipi che supportano i volumi root dell'archivio dell'istanza: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

Console

Per individuare il tipo di volume principale determinato da un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli AMI, quindi seleziona l'AMI.
3. Nella scheda Details (Dettagli), controllare il valore di Root device type (Tipo di dispositivo root) come riportato di seguito:
   - `ebs`: le istanze avviate da questa AMI riceveranno un volume root EBS
   - `instance store`: le istanze avviate da questa AMI riceveranno un volume root dell'archivio dell'istanza.

AWS CLI

Per individuare il tipo di volume principale determinato da un'AMI

Utilizzare il comando describe-images .

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[].RootDeviceType
```

Di seguito è riportato un output di esempio.

```
ebs
```

PowerShell

Per individuare il tipo di volume principale determinato da un'AMI

Utilizza il cmdlet Get-EC2Image.

```
(Get-EC2Image `
```

```
    -ImageId ami-0abcdef1234567890).RootDeviceType.Value
```

Di seguito è riportato un output di esempio.

```
ebs
```

Tipi di virtualizzazione

Le Amazon Machine Image utilizzano uno dei due tipi di virtualizzazione disponibili: paravirtuale (PV) o hardware virtual machine (HVM). Le principali differenze tra le AMI PV e HVM risiedono nel modo in cui vengono avviate e nella loro capacità di sfruttare i vantaggi delle estensioni hardware speciali (CPU, rete e archiviazione) per l'ottimizzazione delle prestazioni. Le AMI Windows sono AMI HVM.

Nella tabella seguente vengono confrontate le AMI HVM e PV.

Caratteristica	HVM	PV
Descrizione	Le AMI HVM sono caratteri zzate da un set completam ente virtualizzato di hardware e configurazione di avvio mediante l'esecuzione della partizione Master Boot Record (MBR) del dispositivo a blocchi root dell'immagine. Questo tipo di virtualizzazione ti permette di eseguire un sistema operativo direttame nte su una macchina virtuale senza la necessità di alcuna modifica, come se venisse eseguito su hardware Bare Metal. Il sistema host Amazon EC2 emula parte o tutto l'hardware sottostante presentato al sistema guest.	Le AMI PV si avviano con uno speciale boot loader chiamato PV-GRUB, che avvia il ciclo di avvio e quindi carica a catena il kernel specificato nel file sull'immagine. `menu.lst` I guest paravirtuali possono essere eseguiti su hardware host che non dispone di supporto esplicito per la virtualizzazione. Per ulteriori informazioni PV-GRUB e sul suo utilizzo in Amazon EC2, consulta Kernel forniti dall'utente. https://docs.aws.amazon.com/linux/al2/ug/UserProvidedKernels.html

Caratteristica	HVM	PV
Tipi di istanze supportati	Tutti i tipi di istanza della generazione corrente supportano le AMI HVM.	I seguenti tipi di istanza di generazioni precedenti supportano le AMI PV: C1, C3, M1, M3, M2 e T1. I tipi di istanza di generazioni precedenti non supportano le AMI PV.
Supporto per estensioni hardware	I sistemi guest HVM possono sfruttare le estensioni hardware che forniscono un accesso rapido all'hardware sottostante sul sistema host. Sono tenuti a utilizzare le reti avanzate e l'elaborazione della GPU. Per garantire il passaggio delle istruzioni ai dispositivi di rete specializzati e ai dispositivi GPU, il sistema operativo deve accedere alla piattaforma hardware nativa e ciò è garantito dalla virtualizzazione HVM. Per ulteriori informazioni, consulta Rete migliorata per le istanze Amazon EC2.	No, non possono usufruire di estensioni hardware speciali come reti avanzate o elaborazione GPU.
Come trovare	Verifica che il tipo di virtualizzazione dell'AMI sia impostato su `hvm`, utilizzando la console o il comando describe-images.	Verifica che il tipo di virtualizzazione dell'AMI sia impostato su `paravirtual` , utilizzando la console o il comando describe-images.

PV su HVM

I guest paravirtual tradizionalmente hanno ottenuto risultati migliori con le operazioni di storage e rete rispetto ai guest HVM perché potevano sfruttare driver speciali per I/O evitare il sovraccarico dell'emulazione dell'hardware di rete e del disco, mentre i guest HVM dovevano tradurre queste istruzioni in hardware emulato. Ora i driver PV sono disponibili per i guest HVM, quindi i sistemi operativi che non possono essere portati per l'esecuzione in un ambiente paravirtualizzato possono comunque ottenere vantaggi prestazionali nello storage e nella rete utilizzandoli. I/O Grazie a questi driver PV su HVM, i sistemi guest HVM possono essere caratterizzati dallo stesso livello di prestazioni dei sistemi guest PV.

Trova una AMI che soddisfi i requisiti per l'istanza EC2

Una AMI include i componenti e le applicazioni, come il sistema operativo e il tipo di volume root, necessari per avviare un'istanza. Per avviare un'istanza, devi trovare un'AMI che soddisfi le tue esigenze.

Quando selezioni un'AMI, tieni in considerazione i requisiti seguenti per le istanze da avviare:

- La AWS regione dell'AMI come ID AMI è unica per ogni regione.
- Il sistema operativo (ad esempio Linux o Windows).
- L'architettura (ad esempio, 32-bit, 64-bit, o 64-bit ARM).
- Il tipo di volume root (ad esempio, Amazon EBS o archivio dell'istanza).
- Il fornitore (ad esempio Amazon Web Services).
- Software aggiuntivo (ad esempio SQL Server).

Console

Puoi scegliere dall'elenco delle AMI quando utilizzi la procedura guidata di avvio dell'istanza, oppure puoi eseguire ricerche tra tutte le AMI disponibili utilizzando la pagina Immagini.

Per individuare un'AMI di avvio rapido tramite la procedura guidata di avvio dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dalla barra di navigazione selezionare la regione in cui avviare le istanze. È possibile selezionare qualsiasi regione disponibile, indipendentemente dalla posizione. Gli ID AMI sono unici per ogni AWS regione.
3. Dal pannello di controllo della console, scegliere Launch Instance (Avvia istanza).

4. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo (Amazon Machine Image), scegliere Quick Start (Avvio rapido), scegliere il sistema operativo per l'istanza, quindi da Amazon Machine Image (AMI), selezionare nell'elenco una delle AMI comunemente utilizzate. Se l'AMI che si desidera utilizzare non è visualizzata, è scegliere Browse more AMIs (Sfoglia altre AMI) per sfogliare il catalogo completo di AMI. Per ulteriori informazioni, consulta Immagini di applicazioni e sistema operativo (Amazon Machine Image).

Come trovare un'AMI dalla pagina delle AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dalla barra di navigazione selezionare la regione in cui avviare le istanze. È possibile selezionare qualsiasi regione disponibile, indipendentemente dalla posizione. Gli ID AMI sono univoci per ogni AWS regione.
3. Nel riquadro di navigazione scegliere AMIs (AMI).
4. (Opzionale) Utilizza le opzioni di filtro e ricerca per definire l'ambito dell'elenco delle AMI visualizzate e visualizzare solo le AMI corrispondenti ai criteri.

   Ad esempio, per elencare tutte le AMI fornite da AWS, scegli Immagini pubbliche. Quindi utilizza le opzioni di ricerca per definire ulteriormente l'ambito delle AMI visualizzate. Scegli la barra Search (Ricerca) e scegli Owner alias (Alias proprietario) dal menu, quindi seleziona l'operatore = e infine il valore amazon. Per trovare le AMI che corrispondono a una piattaforma specifica, ad esempio Linux o Windows, scegli nuovamente la barra di ricerca per scegliere la Piattaforma, quindi l'operatore = e infine il sistema operativo dall'elenco fornito.
5. (Facoltativo) Scegli l'icona Mostra/Nascondi colonne per selezionare gli attributi immagine da visualizzare, come il tipo di volume root. In alternativa, selezione un'AMI dall'elenco e visualizzarne le proprietà nella scheda Details (Dettagli).
6. Prima di selezionare un'AMI, è necessario controllare se è supportata da instance store o da Amazon EBS e conoscere gli effetti di questa differenza. Per ulteriori informazioni, consulta Tipo di volume root.
7. Per avviare un'istanza da questa AMI, selezionala e scegli Avvia istanza. Per informazioni sull'utilizzo della console per avviare un'istanza, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console. Se non si è ancora pronti per avviare l'istanza, annotare l'ID dell'AMI per un utilizzo successivo.

AWS CLI

Utilizza il comando describe-images per trovare un'AMI che soddisfi i tuoi requisiti. Per impostazione predefinita, questo comando restituisce tutte le AMI pubbliche, di cui sei proprietario e che sono condivise con te.

Per individuare un'AMI di proprietà di Amazon

Utilizza il comando describe-images con l'opzione `--owners`.

```
aws ec2 describe-images --owners amazon
```

Per individuare un'AMI Windows

Aggiungi il filtro seguente per visualizzare solo le AMI Windows.

```
--filters "Name=platform,Values=windows"
```

Per trovare un'AMI EBS-backed

Aggiungi il filtro seguente per visualizzare solo le AMI supportate da Amazon EBS.

```
--filters "Name=root-device-type,Values=ebs"
```

PowerShell

Usa il Get-EC2Image cmdlet per trovare un'AMI che soddisfi i tuoi requisiti. Per impostazione predefinita, questo cmdlet restituisce tutte le AMI pubbliche, di cui sei proprietario o che sono condivise con te.

Per individuare un'AMI di proprietà di Amazon

Usa il comando Get-EC2Image con il parametro `-Owner`.

```
Get-EC2Image -Owner amazon
```

Per individuare un'AMI Windows

Aggiungi il filtro seguente per visualizzare solo le AMI Windows.

```
-Filter @{Name="platform"; Values="windows"}
```

Per ulteriori esempi, consulta Find an Amazon Machine Image Using Windows PowerShell nella Guida per l'AWS Strumenti per PowerShell utente.

Risorse correlate

Per ulteriori informazioni sulle AMI per un sistema operativo specifico, consulta le seguenti risorse:

- Amazon Linux 2023 – AL2023 su Amazon EC2 nella Guida per l'utente di Amazon Linux 2023
- Ubuntu – Amazon EC2 AMI Locator sul sito web Canonical Ubuntu
- RHEL – Immagini Red Hat Enterprise Linux (AMI) disponibili su Amazon Web Services (AWS) sul sito web di Red Hat
- Windows Server: Riferimento di AWS Windows AMI

Per informazioni sulle AMI a cui puoi abbonarti, Marketplace AWS AMI a pagamento in Marketplace AWS per istanze Amazon EC2 consulta.

Per informazioni sull'utilizzo di Systems Manager per aiutare gli utenti a trovare l'AMI più recente da utilizzare all'avvio di un'istanza, consulta le risorse seguenti:

- Fai riferimento alle AMI usando i parametri Systems Manager
- Fai riferimento alle AMI più recenti usando i parametri Systems Manager pubblici

Fai riferimento alle AMI usando i parametri Systems Manager

Quando avvii un'istanza utilizzando la procedura guidata di avvio dell'istanza EC2 nella console Amazon EC2, puoi selezionare un'AMI dall'elenco oppure selezionare un AWS Systems Manager parametro che punti a un ID AMI (descritto in questa sezione). Se utilizzi codice di automazione per avviare le istanze, puoi specificare il parametro Systems Manager anziché l'ID AMI.

Un parametro Systems Manager è una coppia chiave-valore definita dal cliente che puoi creare nell'archivio parametri Systems Manager. Archivio parametri fornisce uno store centralizzato per esternalizzare i valori di configurazione dell'applicazione. Per ulteriori informazioni, consulta Archivio parametri AWS Systems Manager nella Guida per l'utente di AWS Systems Manager Systems Manager.

Quando crei un parametro che punta ad un ID AMI, assicurati di specificare il tipo di dati come `aws:ec2:image`. Specificare questo tipo di dati garantisce che quando il parametro viene creato

o modificato, il valore del parametro viene convalidato come un ID AMI. Per ulteriori informazioni, consulta Supporto dei parametri nativi per gli ID di Amazon Machine Image (AMI) nella Guida per l'utente di AWS Systems Manager .

Indice

- Casi d'uso
- Permissions
- Limitazioni
- Avviare un'istanza utilizzando un parametro Systems Manager

Casi d'uso

Quando si utilizzano i parametri di Systems Manager per puntare agli ID AMI, è più facile selezionare l'AMI corretta durante l'avvio delle istanze. I parametri di Systems Manager possono inoltre semplificare la manutenzione del codice di automazione.

Più facile per gli utenti

Se è richiesto che le istanze vengano avviate utilizzando un'AMI specifica e se tale AMI viene aggiornata regolarmente, si consiglia di richiedere agli utenti di selezionare un parametro Systems Manager per trovare l'AMI. Richiedendo agli utenti di selezionare un parametro Systems Manager, puoi assicurarti che l'AMI più recente venga utilizzata per avviare le istanze.

Ad esempio, ogni mese nell'organizzazione è possibile creare una nuova versione dell'AMI con le patch del sistema operativo e delle applicazioni più recenti. Puoi inoltre richiedere che gli utenti avviino istanze utilizzando l'ultima versione dell'AMI. Per assicurarti che gli utenti utilizzino la versione più recente, puoi creare un parametro Systems Manager (ad esempio, `golden-ami`) che punta all'ID AMI corretto. Ogni volta che viene creata una nuova versione dell'AMI, il valore dell'ID AMI nel parametro viene aggiornato in modo che punti sempre all'AMI più recente. Non occorre che gli utenti conoscano gli aggiornamenti periodici all'AMI, perché continuano ogni volta a selezionare lo stesso parametro Systems Manager. Utilizzando un parametro Systems Manager per l'AMI facilita la selezione dell'AMI corretta per l'avvio di un'istanza agli utenti.

Semplificazione della manutenzione del codice di automazione

Se utilizzi codice di automazione per avviare le istanze, puoi specificare il parametro Systems Manager anziché l'ID AMI. Se viene creata una nuova versione dell'AMI, è possibile modificare il valore dell'ID AMI nel parametro in modo che punti all'AMI più recente. Il codice di automazione

che fa riferimento al parametro non deve essere modificato ogni volta che viene creata una nuova versione dell'AMI. Ciò semplifica la manutenzione dell'automazione e contribuisce a ridurre i costi di implementazione.

> **Note**
>
> Le istanze in esecuzione non sono interessate quando si modifica l'ID AMI a cui punta il parametro Systems Manager.

Permissions

Se utilizzi parametri Systems Manager che puntano a ID dell'AMI nella procedura guidata di avvio dell'istanza, devi aggiungere le autorizzazioni seguenti alla policy IAM:

- `ssm:DescribeParameters` – Concede l'autorizzazione per visualizzare e selezionare i parametri Systems Manager.
- `ssm:GetParameters` – Concede l'autorizzazione per recuperare i valori dei parametri di Systems Manager.

Puoi inoltre limitare l'accesso a parametri Systems Manager specifici. Per ulteriori informazioni e policy IAM di esempio, consulta Esempio: utilizzo della procedura guidata per l'avvio dell'istanza EC2.

Limitazioni

AMI e parametri Systems Manager sono specifici della regione. Per utilizzare lo stesso nome di parametro Systems Manager tra regioni, crea un parametro Systems Manager in ogni ragione con lo stesso nome (ad esempio, `golden-ami`). In ogni regione, il parametro Systems Manager deve puntare a un'AMI in tale regione.

I nomi dei parametri fanno distinzione tra maiuscole e minuscole. Le barre rovesciate per il nome del parametro sono necessarie solo quando il parametro fa parte di una gerarchia, ad esempi, `/amis/production/golden-ami`. È possibile omettere la barra rovesciata se il parametro non fa parte di una gerarchia.

Avviare un'istanza utilizzando un parametro Systems Manager

Quando avvii un'istanza, anziché specificare un ID AMI, puoi specificare un parametro Systems Manager che punta a un ID AMI.

Per specificare il parametro in modo programmatico, utilizza la sintassi seguente, dove `resolve:ssm` è il prefisso standard e `parameter-name` è il nome del parametro univoco.

```
resolve:ssm:parameter-name
```

I parametri Systems Manager dispongono del supporto della versione. A ogni iterazione di un parametro viene assegnato un numero di versione univoco. Puoi fare riferimento alla versione del parametro come indicato di seguito, in cui `version` è il numero di versione univoco. Per impostazione predefinita, la versione più recente del parametro viene utilizzata quando non è specificata alcuna versione.

```
resolve:ssm:parameter-name:version
```

Per avviare un'istanza utilizzando un parametro pubblico fornito da AWS, consulta. Fai riferimento alle AMI più recenti usando i parametri Systems Manager pubblici

Console

Per individuare un'AMI mediante un parametro Systems Manager

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dalla barra di navigazione selezionare la regione in cui avviare le istanze. È possibile selezionare qualsiasi regione disponibile, indipendentemente dalla posizione.
3. Dal pannello di controllo della console, scegliere Launch Instance (Avvia istanza).
4. In Applicazioni e immagini SO (Amazon Machine Image), scegli Sfoglia altre AMI.
5. Scegli il pulsante freccia a destra della barra delle ricerche, quindi scegli Cerca per parametro Systems Manager.
6. Per Systems Manager parameter (Parametro Systems Manager), selezionare un parametro. L'ID AMI corrispondente viene visualizzato sotto Attualmente si risolve in.
7. Selezionare Search (Cerca). Le AMI che corrispondono all'ID AMI vengono visualizzate nell'elenco.
8. Selezionare l'AMI dall'elenco e scegliere Select (Seleziona).

Per ulteriori informazioni sull'avvio di un'istanza tramite la procedura guidata di avvio dell'istanza, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

AWS CLI

Per avviare un'istanza utilizzando un parametro Systems Manager

Utilizza il comando run-instances con l'opzione `--image-id`. Questo esempio utilizza un parametro Systems Manager denominato **`golden-ami`**, che specifica un ID AMI.

```
--image-id resolve:ssm:/golden-ami
```

Puoi creare versioni di un parametro Systems Manager. L'esempio seguente specifica la versione 2 del parametro **`golden-ami`**.

```
--image-id resolve:ssm:/golden-ami:2
```

PowerShell

Per avviare un'istanza utilizzando un parametro Systems Manager

Utilizzare il New-EC2Instance cmdlet con il `-ImageId` parametro. Questo esempio utilizza un parametro Systems Manager denominato **`golden-ami`**, che specifica un ID AMI.

```
-ImageId "resolve:ssm:/golden-ami"
```

Puoi creare versioni di un parametro Systems Manager. L'esempio seguente specifica la versione 2 del parametro **`golden-ami`**.

```
-ImageId "resolve:ssm:/golden-ami:2"
```

Fai riferimento alle AMI più recenti usando i parametri Systems Manager pubblici

AWS Systems Manager fornisce parametri pubblici per le AMI pubbliche gestite da. AWS Puoi utilizzare i parametri pubblici all'avvio delle istanze per assicurarti di utilizzare le AMI più recenti. Ad esempio, il parametro pubblico `/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-arm64` è disponibile in tutte le regioni e punta sempre alla versione più recente dell'AMI Amazon Linux 2023 per l'architettura arm64 in una determinata regione.

I parametri pubblici sono disponibili nei percorsi seguenti:

- Linux – `/aws/service/ami-amazon-linux-latest`
- Windows – `/aws/service/ami-windows-latest`

Per ulteriori informazioni, consulta la pagina Utilizzo dei parametri pubblici nella Guida per l'utente di AWS Systems Manager .

Trova il parametro SSM per un'AMI pubblica

Quando descrivi un'AMI pubblica, la risposta include il parametro associato AWS Systems Manager (SSM) nel `PublicSsmParameterName` campo. Usa questo parametro per identificare il parametro SSM che punta sempre alla versione più recente di quell'AMI.

Console

Per trovare il parametro SSM per un'AMI pubblica

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona un'AMI pubblica.
4. Nella scheda Dettagli, trova il nome del parametro SSM pubblico.

AWS CLI

Per trovare il parametro SSM per un'AMI pubblica

Utilizzare il comando describe-images . La risposta include il `PublicSsmParameterName` campo per le AMI pubbliche a cui è associato un parametro SSM.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890
```

L'output di esempio seguente mostra il campo. `PublicSsmParameterName` Alcuni campi vengono omessi per brevità.

```
{
    "Images": [
        {
            "ImageId": "ami-0abcdef1234567890",
            "Name": "al2023-ami-2023.7.20260601.0-kernel-6.1-x86_64",
```

```
            ...
            "PublicSsmParameterName": "aws/service/ami-amazon-linux-latest/al2023-
ami-kernel-default-x86_64"
        }
    ]
}
```

PowerShell

Per trovare il parametro SSM per un'AMI pubblica

Utilizza il cmdlet Get-EC2Image. La risposta include il `PublicSsmParameterName` campo per le AMI pubbliche a cui è associato un parametro SSM.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

L'output di esempio seguente mostra il campo. `PublicSsmParameterName` Alcuni campi vengono omessi per brevità.

```
ImageId               : ami-0abcdef1234567890
Name                  : al2023-ami-2023.7.20260601.0-kernel-6.1-x86_64
...
PublicSsmParameterName : aws/service/ami-amazon-linux-latest/al2023-ami-kernel-
default-x86_64
```

Elenca le AMI di Amazon Linux

AWS CLI

Per elencare le AMI Linux nella versione corrente AWS Region

Utilizza il seguente comando get-parameters-by-path. Il valore del parametro `--path` è specifico delle AMI di Linux.

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-amazon-linux-latest \
    --query "Parameters[].Name"
```

PowerShell

Per elencare le AMI Linux nella versione attuale AWS Region

Utilizza il cmdlet Get-SSMParametersByPath.

```
Get-SSMParametersByPath `
    -Path "/aws/service/ami-amazon-linux-latest" | `
    Sort-Object Name | Format-Table Name
```

Elenca le AMI di Windows

AWS CLI

Per elencare le AMI di Windows nella versione corrente AWS Region

Utilizza il seguente comando get-parameters-by-path. Il valore del parametro `--path` è specifico delle AMI di Windows.

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-windows-latest \
    --query "Parameters[].Name"
```

PowerShell

Per elencare le AMI di Windows nella versione corrente AWS Region

Utilizza il cmdlet Get-SSMParametersByPath.

```
Get-SSMParametersByPath `
    -Path "/aws/service/ami-windows-latest" | `
    Sort-Object Name | Format-Table Name
```

Avvia un'istanza mediante un parametro pubblico

Per specificare il parametro pubblico quando si lancia un'istanza, utilizza la sintassi seguente: `resolve:ssm:`*`public-parameter`*, dove `resolve:ssm` è il prefisso standard e *`public-parameter`* è il percorso e il nome del parametro pubblico.

AWS CLI

Per avviare un'istanza mediante un parametro pubblico

Utilizza il comando run-instances con l'opzione `--image-id`. Questo esempio specifica il parametro pubblico Systems Manager per l'ID dell'immagine per avviare un'istanza mediante l'AMI Amazon Linux 2023 più recente

```
--image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64
```

PowerShell

Per avviare un'istanza mediante un parametro pubblico

Utilizzare il New-EC2Instance cmdlet con il parametro. `-ImageId` Questo esempio specifica il parametro pubblico Systems Manager per l'ID dell'immagine per avviare un'istanza mediante l'AMI più recente per Windows Server 2022.

```
-ImageId "resolve:ssm:/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base"
```

Per altri esempi che utilizzano i parametri di Systems Manager, consulta Query for the latest Amazon Linux AMI ID Using AWS Systems Manager Parameter Store e Query for the Latest Windows AMI Using AWS Systems Manager Parameter Store.

AMI a pagamento in Marketplace AWS per istanze Amazon EC2

Un'AMI a pagamento è un'AMI elencata in vendita in Marketplace AWS. Marketplace AWS È un negozio online in cui è possibile acquistare software che funziona su AWS, comprese le AMI che è possibile utilizzare per avviare l'istanza EC2. Le Marketplace AWS AMI sono organizzate in categorie, come Developer Tools, per consentirti di trovare prodotti adatti alle tue esigenze. Per ulteriori informazioni in merito Marketplace AWS, consulta il Marketplace AWS sito Web.

È possibile acquistare AMI Marketplace AWS da terze parti, incluse le AMI fornite con contratti di servizio di organizzazioni come Red Hat. Puoi anche creare un'AMI e venderla Marketplace AWS ad altri utenti di Amazon EC2. La creazione di un'AMI sicura, protetta e utilizzabile per l'uso pubblico è un processo molto semplice se segui alcune semplici linee guida. Per ulteriori informazioni su come creare e utilizzare le AMI condivise, consulta Informazioni sull'utilizzo delle AMI condivise in Amazon EC2.

L'avvio di un'istanza da un'AMI a pagamento è analogo all'avvio di un'istanza da qualsiasi altra AMI. Non sono necessari altri parametri. Per l'istanza vengono addebitate le tariffe impostate dal

proprietario dell'AMI, assieme ai costi di utilizzo standard per i servizi Web correlati, ad esempio la tariffa oraria per l'esecuzione di un tipo di istanza m5.small in Amazon EC2. Potrebbero essere applicate anche tasse aggiuntive. Il proprietario dell'AMI a pagamento può confermare se un'istanza specifica è stata avviata utilizzato l'AMI a pagamento indicata.

> **Important**
>
> Amazon DevPay non accetta più nuovi venditori o prodotti. Marketplace AWS è ora l'unica piattaforma di e-commerce unificata per la vendita di software e servizi tramite AWS. Per informazioni su come distribuire e vendere software da Marketplace AWS, consulta Selling in AWS Marketplace. Marketplace AWS supporta le AMI supportate da Amazon EBS.

Indice

- Vendi la tua AMI nel Marketplace AWS
- Trovare un'AMI a pagamento
- Acquista un'AMI a pagamento nel Marketplace AWS
- Recupera il Marketplace AWS codice prodotto dalla tua istanza
- Utilizza l'assistenza a pagamento per i servizi supportati Marketplace AWS offerte
- Fatture per AMI a pagamento e supportate
- Gestisci il tuo Marketplace AWS sottoscrizioni

Vendi la tua AMI nel Marketplace AWS

Puoi vendere la tua AMI utilizzando. Marketplace AWS Marketplace AWS offre un'esperienza di acquisto organizzata. Inoltre, supporta Marketplace AWS anche AWS funzionalità come EBS-backed AMI Amazon, istanze riservate e istanze Spot.

Per informazioni su come vendere la tua AMI su Marketplace AWS, consulta Selling in Marketplace. AWS

Trovare un'AMI a pagamento

Un'AMI a pagamento è un'Amazon Machine Image (AMI) che è disponibile per l'acquisto. Le AMI a pagamento hanno anche un codice prodotto. Puoi trovare le AMI disponibili per l'acquisto nel Marketplace AWS.

Console

Per trovare un'AMI a pagamento

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Nel primo filtro scegliere Public images (Immagini pubbliche).
4. Esegui una delle seguenti operazioni:
   - Se conosci il codice prodotto, seleziona Product code (codice prodotto), = e digita il codice.
   - Se non conosci il codice del prodotto, nella barra di ricerca specifica questo filtro: Owner alias=aws-marketplace. Specifica filtri aggiuntivi in base alle esigenze.
5. Salva l'ID dell'AMI.

AWS CLI

Per trovare un'AMI a pagamento

Usa il seguente comando describe-images.

```
aws ec2 describe-images --owners aws-marketplace
```

L'output include un numero elevato di immagini. Puoi specificare dei filtri per determinare meglio l'AMI di cui hai bisogno. Dopo aver trovato un'AMI, specifica il suo ID nel seguente comando per ottenere il codice prodotto.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[*].ProductCodes[].ProductCodeId
```

Di seguito è riportato un output di esempio.

```
[
    "cdef1234abc567def8EXAMPLE"
]
```

Se si conosce il codice prodotto, è possibile filtrare i risultati in base a quel codice. L'esempio seguente restituisce l'AMI più recente con il codice prodotto specificato.

```
aws ec2 describe-images \
    --filters "Name=product-code,Values=cdef1234abc567def8EXAMPLE" \
    --query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

PowerShell

Per trovare un'AMI a pagamento

Utilizza il cmdlet Get-EC2Image.

```
Get-EC2Image -Owner aws-marketplace
```

L'output include un numero elevato di immagini. Puoi specificare dei filtri per determinare meglio l'AMI di cui hai bisogno. Dopo aver trovato un'AMI, specifica il suo ID nel seguente comando per ottenere il codice prodotto.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).ProductCodes
```

Di seguito è riportato un output di esempio.

```
ProductCodeId             ProductCodeType
-------------             ---------------
cdef1234abc567def8EXAMPLE marketplace
```

Se si conosce il codice prodotto, è possibile filtrare i risultati in base a quel codice. L'esempio seguente restituisce l'AMI più recente con il codice prodotto specificato.

```
(Get-EC2Image -Owner aws-marketplace -Filter @{"Name"="product-
code";"Value"="cdef1234abc567def8EXAMPLE"} | sort CreationDate -Descending | Select-
Object -First 1).ImageId
```

Acquista un'AMI a pagamento nel Marketplace AWS

Devi registrarti per acquistare un'AMI a pagamento prima di poter avviare un'istanza Amazon EC2 utilizzando l'AMI.

In genere, il rivenditore di un'AMI a pagamento ti invia le informazioni sull'AMI, compresi il relativo prezzo e un collegamento associato alla pagina in cui puoi effettuare l'acquisto. Quando scegli il link, ti viene prima chiesto di accedere AWS, quindi puoi acquistare l'AMI.

Acquistare un'AMI a pagamento con la console

Puoi acquistare un'AMI a pagamento utilizzando la procedura guidata di avvio di Amazon EC2. Per ulteriori informazioni, consulta Avvia un'istanza Amazon EC2 da un'AMI Marketplace AWS.

Abbonati a un prodotto utilizzando Marketplace AWS

Per utilizzare il Marketplace AWS, è necessario disporre di un Account AWS. Per avviare istanze dai Marketplace AWS prodotti, devi essere registrato per utilizzare il servizio Amazon EC2 e devi essere abbonato al prodotto da cui avviare l'istanza. Puoi utilizzare uno dei seguenti metodi per la sottoscrizione ai prodotti in Marketplace AWS:

- Marketplace AWS sito Web: puoi avviare rapidamente il software preconfigurato con la funzione di distribuzione con un clic. Per ulteriori informazioni, consulta AMI-based i prodotti in. Marketplace AWS
- Procedura guidata di avvio di Amazon EC2: puoi cercare un'AMI e avviare un'istanza direttamente dalla procedura guidata. Per ulteriori informazioni, consulta Avvia un'istanza Amazon EC2 da un'AMI Marketplace AWS.

Recupera il Marketplace AWS codice prodotto dalla tua istanza

Puoi recuperare il codice Marketplace AWS prodotto per la tua istanza utilizzando i metadati dell'istanza. Se l'istanza dispone di un codice prodotto, Amazon EC2 restituisce tale valore. Per ulteriori informazioni sul recupero dei metadati, consulta Accesso ai metadati dell'istanza per un'istanza EC2.

IMDSv2

Linux

Esegui il seguente comando dall'istanza Linux.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/product-codes
```

Windows

Esegui i seguenti cmdlet dall'istanza Windows.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/product-codes
```

IMDSv1

Linux

Esegui il seguente comando dall'istanza Linux.

```
curl http://169.254.169.254/latest/meta-data/product-codes
```

Windows

Esegui il seguente comando dall'istanza Windows.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/product-codes
```

Utilizza l'assistenza a pagamento per i servizi supportati Marketplace AWS offerte

Amazon EC2 consente inoltre agli sviluppatori di offrire supporto per il software (AMI derivate). Gli sviluppatori possono creare prodotti di supporto per il cui utilizzo è prevista la registrazione. Durante il processo di registrazione per un prodotto di supporto, lo sviluppatore ti invia un codice prodotto, che dovrai quindi associare all'AMI in tuo possesso. Ciò consente allo sviluppatore di verificare che la tua istanza ha diritto al supporto. Garantisce inoltre che quando esegui le istanze del prodotto ti vengano addebitati i costi corretti in base alle condizioni specificate per il prodotto dallo sviluppatore.

Limitazioni

- Dopo aver impostato l'attributo relativo al codice prodotto, non puoi più modificarlo o rimuoverlo.
- Non puoi utilizzare un prodotto di supporto con le Istanze riservate. Ti verrà sempre addebitato il prezzo specificato dal rivenditore del prodotto di supporto.

AWS CLI

Per associare un codice prodotto alla tua AMI

Usa il comando modify-image-attribute.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --product-codes "cdef1234abc567def8EXAMPLE"
```

PowerShell

Per associare un codice prodotto alla tua AMI

Utilizza il cmdlet Edit-EC2ImageAttribute.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -ProductCode "cdef1234abc567def8EXAMPLE"
```

Fatture per AMI a pagamento e supportate

Alla fine di ogni mese riceverai un messaggio e-mail contenente l'importo addebitato sulla tua carta di credito per l'utilizzo di qualsiasi AMI a pagamento o supportata durante il mese appena trascorso. Questa fattura è distinta rispetto alla normale fattura di Amazon EC2. Per ulteriori informazioni, consulta Pagamento dei prodotti nella Marketplace AWS Guida per gli acquirenti .

Gestisci il tuo Marketplace AWS sottoscrizioni

Sul Marketplace AWS sito Web, puoi controllare i dettagli dell'abbonamento, visualizzare le istruzioni di utilizzo del fornitore, gestire gli abbonamenti e altro ancora.

Controlla i dettagli della sottoscrizione a

Per controllare i dettagli della sottoscrizione

1. Accedi al Marketplace AWS.
2. Scegliere Your Marketplace Account (Account Marketplace personale).
3. Scegliere Manage your software subscriptions (Gestisci sottoscrizioni software).

4. Vengono elencate tutte le sottoscrizioni correnti. Scegliere Istruzioni di utilizzo per visualizzare istruzioni specifiche relative all'utilizzo del prodotto, ad esempio un nome utente per la connessione all'istanza in esecuzione.

Annulla abbonamento

> **Note**
>
> - Annullare un abbonamento non comporta la terminazione delle istanze avviate con quell'AMI. Continueremo ad addebitarti le istanze in esecuzione fino alla loro terminazione. Devi terminare tutte le istanze avviate con l'AMI per interrompere la fatturazione dell'abbonamento.
> - Dopo aver annullato la sottoscrizione, non sara più in possibile avviare istanze dall'AMI specifica. Per utilizzare nuovamente quell'AMI, devi abbonarti nuovamente, sul Marketplace AWS sito Web o tramite la procedura guidata di avvio nella console Amazon EC2.

Per annullare un Marketplace AWS sottoscrizione

1. Per interrompere la fatturazione dell'abbonamento, assicurati di aver terminato tutte le istanze in esecuzione dall'abbonamento.

   > **Warning**
   >
   > La terminazione di un'istanza è permanente e irreversibile.
   > Dopo aver terminato un'istanza, non puoi più connetterti a essa e non puoi ripristinarla. Inoltre, tutti i volumi Amazon EBS collegati e configurati per essere eliminati in caso di terminazione vengono eliminati in modo definitivo e non possono essere recuperati. Tutti i dati archiviati nei volumi di archivio dell'istanza vengono persi in modo definitivo. Per ulteriori informazioni, consulta Come funziona la terminazione delle istanze.
   > Prima di terminare un'istanza, assicurati di aver eseguito il backup di tutti i dati che devi mantenere dopo la terminazione sull'archivio persistente.

   a. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

b. Nel riquadro di navigazione, scegliere Instances (Istanze).

c. Seleziona l'istanza e scegli Stato istanza, Termina (elimina) istanza.

d. Quando viene richiesta la conferma, scegli Termina (elimina).

2. Accedere al Marketplace AWS e scegliere Account Marketplace personale, quindi Gestisci sottoscrizioni software.

3. Scegliere Cancel subscription (Annulla sottoscrizione). Verrà richiesto di confermare l'annullamento.

Ciclo di vita dell'AMI di Amazon EC2

Un'immagine Amazon Machine Image (AMI) contiene la configurazione software necessaria per impostare e avviare un'istanza. Devi specificare un'AMI quando avvii un'istanza. Puoi utilizzare le AMI fornite da Amazon oppure creare le tue AMI. L'AMI deve trovarsi nella posizione Regione AWS in cui si desidera avviare l'istanza.

Il ciclo di vita di un'AMI comprende la creazione, la copia, l'obsolescenza, la disabilitazione e l'eliminazione (annullamento della registrazione) dell'AMI.

Crea le AMI. Amazon fornisce AMI che puoi utilizzare per avviare le istanze, ma puoi anche creare AMI personalizzate in base alle tue esigenze. Per creare un'AMI personalizzata, avvia un'istanza da un'AMI esistente, personalizzala (ad esempio, installando il software e configurando le impostazioni del sistema operativo) e poi crea un'AMI dall'istanza. Tutte le personalizzazioni delle istanze vengono salvate nella nuova AMI, in modo che le istanze avviate dalla nuova AMI includano tali personalizzazioni.

AMI attestabili. Per creare un'AMI che supporti l'attestazione delle istanze EC2, consulta AMI attestabili.

Copia le AMI. È possibile utilizzare un'AMI per avviare un'istanza solo Regione AWS nella quale si trova l'AMI. Se hai bisogno di avviare istanze con la stessa configurazione in più regioni, copia l'AMI nelle altre regioni.

Contrassegna le AMI come obsolete. Per contrassegnare un'AMI come sostituita o come obsoleta, puoi impostare una data di obsolescenza immediata o futura. Le AMI obsolete sono nascoste negli elenchi delle AMI, ma gli utenti e i servizi possono continuare a utilizzare le AMI obsolete se conoscono l'ID dell'AMI.

Disabilita le AMI. Per impedire temporaneamente l'uso di un'AMI, puoi disabilitarla. Quando un'AMI è disabilitata, non può essere utilizzata per avviare nuove istanze. Se però l'AMI viene riattivata, puoi utilizzarla per avviare nuovamente le istanze. Nota che la disabilitazione di un'AMI non influisce sulle istanze esistenti che sono già state avviate da essa.

Annulla la registrazione delle AMI (elimina le AMI). Quando un'AMI non è più necessaria, puoi annullarne la registrazione, impedendo che venga utilizzata per avviare nuove istanze. Se l'AMI soddisfa una regola di conservazione, viene spostata nel Cestino, dove può essere ripristinata prima della scadenza del periodo di conservazione, dopo il quale viene eliminata definitivamente. Se non soddisfa una regola di conservazione, viene subito eliminata definitivamente. Nota che l'annullamento della registrazione di un'AMI non influisce sulle istanze esistenti che erano state avviate dall'AMI.

Automatizza i cicli di vita dell'AMI. Puoi utilizzare Amazon Data Lifecycle Manager per automatizzare la creazione, la conservazione, la copia, la deprecazione e l'annullamento della registrazione delle AMI Amazon e delle relative istantanee di supporto. EBS-backed Puoi anche utilizzare EC2 Image Builder per automatizzare la creazione, la gestione e l'implementazione di AMI personalizzate. Per ulteriori informazioni, consulta Automate backups with Amazon Data Lifecycle Manager nella Guida per l'utente di Amazon EBS e nella Guida per l'utente di EC2 Image Builder.

Indice

- Crea un' EBS-backed AMI Amazon
- Crea un' S3-backed AMI Amazon
- Creare un'AMI Amazon EC2 utilizzando Windows Sysprep
- Copiare un'AMI Amazon EC2
- Archiviazione e ripristino di un'AMI utilizzando S3
- Usa l'ascendenza AMI per tracciare l'origine di un'AMI
- Usa le filigrane AMI per tracciare e identificare le AMI
- Tipi di istanza AMI consentiti
- Gestisci e monitora l'uso delle AMI
- Dichiarare un'AMI Amazon EC2 come obsoleta
- Disattivare un'AMI Amazon EC2
- Annullare la registrazione di un'AMI Amazon EC2

Crea un' EBS-backed AMI Amazon

Puoi creare la tua Amazon EBS-backed AMI da un'istanza Amazon EC2 o da un'istantanea del volume principale di un'istanza Amazon EC2.

Per creare un'Amazon EBS-backed AMI da un'istanza, inizia avviando un'istanza utilizzando un'AMI Amazon esistente. EBS-backed Questa AMI può essere ottenuta da te Marketplace AWS, creata tramite VM Import/Export, o qualsiasi altra AMI a cui puoi accedere. Dopo aver personalizzato l'istanza per soddisfare i tuoi requisiti specifici, crea e registra una nuova AMI. Poi, puoi usare la nuova AMI per avviare nuove istanze con le tue personalizzazioni.

> **Note**
>
> Per creare un'AMI che supporti l'attestazione delle istanze EC2, consulta AMI attestabili.

Le procedure descritte di seguito sono valide per le istanze di Amazon EC2 supportate dai volumi Amazon Elastic Block Store (Amazon EBS) (incluso il volume root) e per i volumi non crittografati.

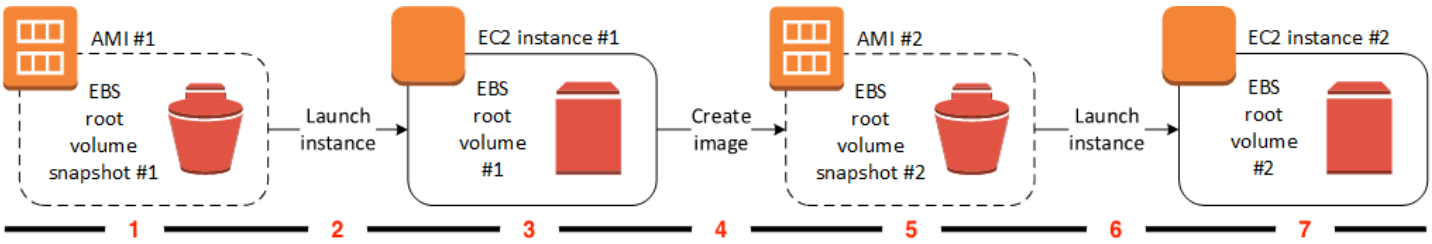
Il processo di creazione delle AMI è diverso per le AMI di S3-backed Amazon. Per ulteriori informazioni, consulta Crea un' S3-backed AMI Amazon.

Indice

- Panoramica della creazione di AMI da un'istanza
- Creare un'AMI da un'istanza
- Creazione di un'AMI da uno snapshot

Panoramica della creazione di AMI da un'istanza

Il diagramma seguente riassume il processo di creazione di un'Amazon EBS-backed AMI da un'istanza EC2 in esecuzione: inizia con un'AMI esistente, avvia un'istanza, personalizzala, crea una nuova AMI da essa e infine avvia un'istanza della tua nuova AMI. I numeri nel diagramma corrispondono ai numeri nella descrizione che segue.



1 — AMI #1: si inizia con un'AMI esistente

Individua un'AMI esistente simile all'AMI che si desidera creare. Può essere un'AMI che hai ottenuto da Marketplace AWS, un'AMI che hai creato utilizzando una VM Import/Export o qualsiasi altra AMI a cui puoi accedere. Si personalizzerà questa AMI in base alle proprie esigenze.

Nel diagramma, lo snapshot #1 del volume root EBS indica che l'AMI è un' EBS-backed AMI Amazon e che le informazioni sul volume root sono archiviate in questa istantanea.

2 — Si avvia l'istanza dall'AMI esistente

Il modo per configurare un'AMI consiste nel lanciare un'istanza dall'AMI su cui si desidera basare la nuova AMI, quindi personalizzare l'istanza (indicata all'indirizzo 3 nel diagramma). Quindi si creerà una nuova AMI che include le personalizzazioni (indicate all'indirizzo 4 nel diagramma).

3 — Istanza EC2 #1: si personalizza l'istanza

Connettersi all'istanza e personalizzarla in base alla proprie esigenze. La nuova AMI includerà queste personalizzazioni.

È possibile effettuare una delle operazioni seguenti sull'istanza per personalizzarla in base alle proprie esigenze:

- Installazione di software e applicazioni
- Copia dei dati
- Riduzione del tempo di avvio tramite l'eliminazione dei file temporanei e la deframmentazione del disco rigido
- Collegamento di volumi EBS aggiuntivi

4 — Si crea un'immagine

Quando un'AMI viene creata da un'istanza, Amazon EC2 spegne l'istanza prima di creare l'AMI per garantire che tutto ciò che è presente sull'istanza sia arrestato e mantenuto in uno stato

coerente durante la procedura di creazione. Se sei sicuro che l'istanza sia in uno stato coerente, appropriato per la creazione dell'AMI, puoi indicare ad Amazon EC2 di non spegnere e riavviare l'istanza. Alcuni file system, come XFS, possono bloccare e sbloccare l'attività, consentendo la creazione sicura dell'immagine senza il riavvio dell'istanza.

Durante il AMI-creation processo, Amazon EC2 crea istantanee del volume principale dell'istanza e di qualsiasi altro volume EBS collegato all'istanza. Ti verrà addebitato il costo degli snapshot finché non annullerai la registrazione dell'AMI e non eliminerai gli snapshot. Se i volumi collegati all'istanza sono crittografati, la nuova AMI viene avviata correttamente solo sulle istanze che supportano la crittografia Amazon EBS.

A seconda delle dimensioni dei volumi, il completamento del AMI-creation processo può richiedere diversi minuti (a volte fino a 24 ore). Si potrebbe ritenere più efficiente creare snapshot dei volumi prima della creazione dell'AMI. In questo modo, in seguito alla creazione dell'AMI, dovrai creare soltanto snapshot incrementali e di piccole dimensioni, e il processo verrà completato più rapidamente (il tempo totale per la creazione della snapshot rimane invariato).

5 — AMI #2: Una nuova AMI

Al termine del processo, si disporrà di una nuova AMI e di uno snapshot (snapshot #2) creati dal volume root dell'istanza. Se hai aggiunto volumi di archivio dell'istanza o volumi EBS all'istanza, oltre al volume root, la mappatura dei dispositivi a blocchi per la nuova AMI conterrà informazioni su tali volumi.

Amazon EC2 registra automaticamente l'AMI

6 — Si avvia un'istanza da una nuova AMI.

È possibile utilizzare la nuova AMI per avviare un'istanza.

7 — Istanza EC2 #2: una nuova istanza

Quando si avvia un'istanza con la nuova AMI, Amazon EC2 crea un nuovo volume EBS per il relativo volume root tramite lo snapshot. Se hai aggiunto volumi di archivio dell'istanza o volumi EBS quando hai personalizzato l'istanza, la mappatura dei dispositivi a blocchi per la nuova AMI conterrà informazioni su tali volumi e le mappature dei dispositivi a blocchi per le istanze avviate dalla nuova AMI includeranno automaticamente le informazioni relative a tali volumi. I volumi instance store specificati nella mappatura dei dispositivi a blocchi per la nuova istanza sono nuovi e non contengono nessun dato sui volumi instance store dell'istanza utilizzata per creare l'AMI. I dati sui volumi EBS vengono conservati. Per ulteriori informazioni, consulta Mappature dei dispositivi a blocchi per i volumi sulle istanze Amazon EC2.

Quando si crea una nuova istanza da un' EBS-backed AMI, è necessario inizializzarne il volume principale e l'eventuale storage EBS aggiuntivo prima di metterla in produzione. Per ulteriori informazioni, consulta Inizializzazione dei volumi Amazon EBS nella Guida per l'utente di Amazon EBS.

Creare un'AMI da un'istanza

Se disponi di un'istanza esistente, puoi creare un'AMI da questa istanza.

Console

Per creare un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza dalla quale creare l'AMI, quindi scegli Actions (Operazioni), Image and templates (Immagine e modelli), Create image (Crea immagine).

   > **Tip**
   >
   > Se questa opzione è disattivata, la tua istanza non è un'istanza Amazon EBS-backed .

4. Nella pagina Create image (Crea immagine), specifica le seguenti informazioni:

   a. In Image name (Nome immagine), inserisci un nome univoco per l'immagine lungo al massimo 127 caratteri.

   b. In Image description (Descrizione immagine), inserisci una descrizione facoltativa dell'immagine lunga al massimo 255 caratteri.

   c. Per Riavvia istanza, lascia selezionata la casella di spunta Abilita, che è l'impostazione predefinita, oppure deselezionala.

      - Se è selezionata l'istanza Reboot, quando Amazon EC2 crea la nuova AMI, riavvia l'istanza in modo da poter scattare istantanee dei volumi collegati mentre i dati sono inattivi, per garantire uno stato coerente.
      - Se l'opzione Riavvia istanza non è selezionata, quando Amazon EC2 crea la nuova AMI, non chiude e non riavvia l'istanza.

> **Warning**
>
> Se si deseleziona l'opzione Riavvia istanza, non possiamo garantire l'integrità del file system dell'immagine creata.

d. Volumi istanza: puoi modificare il volume root e aggiungere altri volumi Amazon EBS e di archivio dell'istanza, come segue:

   i. Il volume root è definito nella prima riga.

      - Per modificare la dimensione del volume root, in Dimensione immetti il valore richiesto.
      - Se selezioni Delete on Termination (Elimina al termine), quando termini l'istanza creata da questa AMI, il volume EBS viene eliminato. Se deselezioni Delete on Termination (Elimina al termine), quando termini l'istanza, il volume EBS non viene eliminato. Per ulteriori informazioni, consulta Conservare i dati quando un'istanza viene terminata.

   ii. Per aggiungere un volume EBS, seleziona Add New Volume (Aggiungi nuovo volume), che comporta l'aggiunta di una nuova riga. Per Tipo di archiviazione, scegli EBSe compilai campi nella riga. Quando avvii un'istanza dalla nuova AMI, questi volumi aggiuntivi vengono collegati automaticamente all'istanza. È necessario formattare e montare i volumi vuoti. È necessario montare i volumi basati su snapshot.

   iii. Per aggiungere un volume instance store, consulta Aggiunta di volumi di archivio dell'istanza a un'AMI Amazon EC2. Quando avvii un'istanza dalla nuova AMI, i volumi aggiuntivi vengono inizializzati e installati automaticamente. Questi volumi non contengono i dati dai volumi instance store dell'istanza in esecuzione sulla quale hai basato l'AMI.

e. Destinazione degli snapshot: se i volumi delle istanze si trovano in una zona locale che supporta gli snapshot locali EBS, scegli dove creare gli snapshot dell'AMI:

   - Regione AWS: crea snapshot nella regione principale della zona locale dei tuoi volumi.
   - AWS Zona locale: crea istantanee nella stessa zona locale dei tuoi volumi.

> **Note**
>
> Questa opzione è disponibile solo nelle zone locali che supportano gli snapshot locali EBS e solo se l'istanza è stata creata in una Zona locale. Se il volume si trova in un'area, questa opzione non viene visualizzata e lo snapshot viene creato automaticamente nella stessa regione del volume. Per ulteriori informazioni, consulta Local snapshots in Local Zones nella Guida per l'utente di Amazon EBS.

> **Important**
>
> Tutti gli snapshot dei volumi dell'istanza devono trovarsi nella stessa posizione. Verifica la posizione degli snapshot esistenti. Se gli snapshot esistenti si trovano in una posizione diversa dalla destinazione selezionata, la creazione dell'AMI avrà esito negativo.

f. Tags (Tag) - È possibile contrassegnare l'AMI e gli snapshot con gli stessi tag, oppure contrassegnarli con tag diversi.

- Per taggare l'AMI e gli snapshot con gli stessi tag, scegli Tag image and snapshots together. All'AMI e a ogni snapshot creato vengono applicati gli stessi tag.
- Per contrassegnare l'AMI e gli snapshot con tag diversi, scegli Tag image and snapshots separately. All'AMI e a ogni snapshot creato vengono applicati tag diversi. Tuttavia, tutti gli snapshot ricevono gli stessi tag; non è possibile contrassegnare ogni snapshot con un tag diverso.

Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore per il tag. Ripetere per ogni tag.

g. Quando è tutto pronto per creare l'AMI, scegli Create image (Crea immagine).

5. Per visualizzare lo stato dell'AMI durante la creazione:

a. Nel riquadro di navigazione scegliere AMIs (AMI).

b. Imposta il filtro su Owned by me (Di mia proprietà) e seleziona l'AMI dall'elenco.

Inizialmente lo stato è `pending`, ma dovrebbe cambiare in `available` dopo pochi minuti.

6. (Facoltativo) Per visualizzare lo snapshot creato per la nuova AMI:

   a. Annota l'ID dell'AMI individuata nel passaggio precedente.
   b. Nel pannello di navigazione, selezionare Snapshots (Snapshot).
   c. Imposta il filtro su Owned by me (Di mia proprietà), quindi trova lo snapshot con il nuovo ID AMI nella colonna Description (Descrizione).

      Quando avvii un'istanza da questa AMI, Amazon EC2 utilizza questo snapshot per creare il volume root dell'istanza.

AWS CLI

Per creare un'AMI

Utilizza il comando create-image.

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "my-web-server" \
    --description "My web server image" \
    --no-reboot
```

PowerShell

Per creare un'AMI

Utilizza il cmdlet New-EC2Image.

```
New-EC2Image `
    -InstanceId i-1234567890abcdef0 `
    -Name "my-web-server" `
    -Description "My web server image" `
    -NoReboot $true
```

Creazione di un'AMI da uno snapshot

Se disponi di uno snapshot del volume root di un'istanza, puoi creare un'AMI da tale snapshot.

> **Note**
>
> Nella maggior parte dei casi, le AMI per Windows, Red Hat, SUSE e SQL Server richiedono la presenza delle informazioni di licenza corrette sull'AMI. Per ulteriori informazioni, consulta Comprendere le informazioni di fatturazione AMI. Quando si crea un'AMI da uno snapshot, l'operazione `RegisterImage` ricava le informazioni di fatturazione corrette dai metadati dello snapshot, ma ciò richiede la presenza dei metadati appropriati. Per verificare se sono state applicate le informazioni di fatturazione corrette, controlla il campo Dettagli della piattaforma sulla nuova AMI. Se il campo è vuoto o non corrisponde al codice del sistema operativo previsto (ad esempio, Windows, Red Hat, SUSE o SQL), la creazione dell'AMI ha avuto esito negativo e dovresti eliminare l'AMI e seguire le istruzioni in Creare un'AMI da un'istanza.

Console

Per creare un'AMI da uno snapshot

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, selezionare Snapshots (Snapshot).
3. Seleziona lo snapshot dal quale creare l'AMI e scegli Actions (Operazioni), Create image from snapshot (Crea un'immagine dallo snapshot).
4. Nella pagina Crea immagine da uno snapshot, specifica le seguenti informazioni:
   a. In Image name (Nome immagine), inserire un nome descrittivo per l'immagine.
   b. In Description (Descrizione) inserire una breve descrizione dell'immagine.
   c. In Architecture (Architettura), scegliere l'architettura dell'immagine. Scegli i386 per sistemi a 32 bit, x86_64 per sistemi a 64 bit, arm64 per ARM a 64 bit o x86_64 per macOS a 64 bit.
   d. In Nome dispositivo root, inserisci il nome del dispositivo da utilizzare per il volume root. Per ulteriori informazioni, consulta Nomi dei dispositivi per i volumi sulle EC2 istanze Amazon.
   e. Per Virtualization type (Tipo di virtualizzazione), scegliere il tipo di virtualizzazione da utilizzare dalle istanze avviate da questa AMI. Per ulteriori informazioni, consulta Tipi di virtualizzazione.
   f. (Solo per la virtualizzazione paravirtuale) Per Kernel ID (ID kernel), selezionare il kernel del sistema operativo per l'immagine. Se si utilizza uno snapshot del volume root di

un'istanza, selezionare lo stesso ID kernel dell'istanza originale. Se non si è sicuri, utilizzare il kernel di default.

g. (Solo per la virtualizzazione paravirtuale) Per RAM disk ID (ID disco RAM), selezionare il disco RAM per l'immagine. Se è stato selezionato un kernel specifico, potrebbe essere necessario selezionare un disco RAM specifico con i driver che lo supportano.

h. Per la Modalità di avvio, scegli la modalità di avvio per l'immagine o scegli Usa default in modo tale che quando un'istanza viene avviata con questa AMI, venga avviata con la modalità di avvio supportata dal tipo di istanza. Per ulteriori informazioni, consulta Impostare la modalità di avvio di un'AMI Amazon EC2.

i. (Facoltativo) Nella sezione Mappatura dei dispositivi a blocchi, personalizza il volume root e aggiungi volumi di dati aggiuntivi.

   Per ogni volume, si possono specificare le dimensioni, il tipo, le caratteristiche delle prestazioni, il comportamento dell'eliminazione alla terminazione e lo stato di crittografia. Per il volume root, la dimensione non può essere inferiore alla dimensione dello snapshot. Per il tipo di volume, SSD a uso generale `gp3` è la selezione predefinita.

j. (Facoltativo) Nella sezione Tag, puoi aggiungere uno o più tag alla nuova AMI. Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore per il tag. Ripetere per ogni tag.

k. Quando è tutto pronto per creare l'AMI, scegli Create image (Crea immagine).

5. (Solo Windows, Red Hat, SUSE e SQL Server) Per verificare se sono state applicate le informazioni di fatturazione corrette, controlla il campo Dettagli della piattaforma sulla nuova AMI. Se il campo è vuoto o non corrisponde al codice del sistema operativo previsto (ad esempio, Windows o Red Hat), la creazione dell'AMI ha avuto esito negativo e dovresti eliminare l'AMI e seguire le istruzioni in Creare un'AMI da un'istanza.

AWS CLI

Per creare un'AMI da un'istantanea utilizzando AWS CLI

Utilizza il comando register-image.

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0db2cf683925d191f}
```

PowerShell

Per creare un'AMI da un'istantanea utilizzando PowerShell

Utilizza il cmdlet Register-EC2Image.

```
$block = @{SnapshotId=snap-0db2cf683925d191f}
Register-EC2Image `
    -Name my-image `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block}
```

Crea un' S3-backed AMI Amazon

L'AMI specificata quando avvii l'istanza determina il tipo di volume root.

Per creare un'AMI Amazon S3-backed Linux, inizia da un'istanza lanciata da un'AMI Amazon S3-backed Linux esistente. Dopo avere personalizzato l'istanza in base alle tue esigenze, è necessario creare un bundle del volume e registrare una nuova AMI, che puoi utilizzare per avviare nuove istanze con queste personalizzazioni.

Non puoi creare un'AMI Amazon S3-backed Windows perché le AMI Windows non supportano l'Instance Store per il volume root.

> **Important**
>
> Solo i seguenti tipi di istanza supportano un volume di archiviazione delle istanze come volume principale e richiedono un' S3-backed AMI Amazon: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

Il processo di creazione delle AMI è diverso per le AMI di Amazon. EBS-backed Per ulteriori informazioni, consulta Crea un' EBS-backed AMI Amazon.

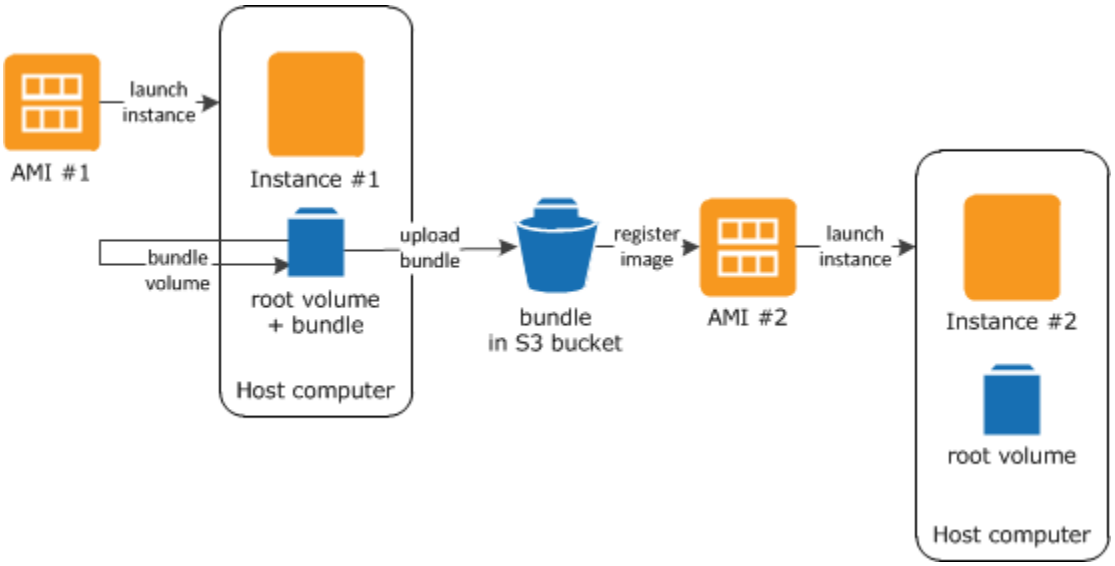
Indice

- Panoramica della creazione delle AMI
- Prerequisiti
- Creare un'AMI da un'istanza Amazon Linux

- Configurazione degli strumenti dell'AMI Amazon EC2
- Riferimento strumenti AMI Amazon EC2
- Converti la tua Amazon AMI in un'AMI S3-backed EBS-backed

Panoramica della creazione delle AMI

Il diagramma seguente riepiloga le operazioni necessarie per la creazione di un'AMI a partire da un'istanza con un volume root di archivio dell'istanza.



Innanzitutto, avvia un'istanza da un'AMI che sia simile all'AMI che desideri creare. Puoi connetterti alla tua istanza e personalizzarla. Una volta che è configurata come desideri puoi creare un bundle dell'istanza. Per il completamento di questo processo sono richiesti vari minuti. Al termine del processo avrai un bundle, composto da un manifest delle immagini (`image.manifest.xml`) e da file (`image.part.xx`) contenenti un modello per il volume root. Successivamente, carica il bundle nel bucket Amazon S3 e registra l'AMI.

> **Note**
>
> Per caricare oggetti in un bucket S3 per la tua AMI Amazon S3-backed Linux, gli ACL devono essere abilitati per il bucket. In caso contrario, Amazon EC2 non sarà in grado di impostare le ACL sugli oggetti da caricare. Se il bucket di destinazione utilizza l'impostazione applicata dal proprietario del bucket per S3 Object Ownership, ciò non funzionerà perché le ACL sono disabilitate. Per ulteriori informazioni, consulta Controllo della proprietà degli oggetti e disabilitazione delle ACL per il bucket.

Quando avvii un'istanza con la nuova AMI, viene creato il volume root dell'istanza usando il bundle che hai caricato in Amazon S3. Finché non lo elimini, lo spazio di archiviazione utilizzato dal bundle in Amazon S3 comporta dei costi che vengono addebitati sul tuo account. Per ulteriori informazioni, consulta Annullare la registrazione di un'AMI Amazon EC2.

Se aggiungi dei volumi archivio dell'istanza all'istanza, oltre al volume root, la mappatura dei dispositivi a blocchi per la nuova AMI conterrà informazioni su tali volumi e le mappature dei dispositivi a blocchi per le istanze che avvii dalla nuova AMI conterranno automaticamente le informazioni relative a tali volumi. Per ulteriori informazioni, consulta Mappature dei dispositivi a blocchi per i volumi sulle istanze Amazon EC2.

Prerequisiti

Prima di poter creare un AMI, devi completare le attività seguenti:

- Installazione degli strumenti AMI. Per ulteriori informazioni, consulta Configurazione degli strumenti dell'AMI Amazon EC2.
- AWS CLI Installa il. Per ulteriori informazioni, consulta Nozioni di base di AWS CLI.
- Verificare di disporre di un bucket S3 per il bundle e che il bucket abbia le ACL abilitate. Per ulteriori informazioni sulla configurazione delle ACL, consulta la pagina Configurazione delle ACL.
  - Per creare un bucket S3 utilizzando il Console di gestione AWS, apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/ e scegli Create Bucket.
  - Per creare un bucket S3 con AWS CLI, puoi usare il comando mb. https://docs.aws.amazon.com/cli/latest/reference/s3/mb.html Se la versione installata degli strumenti AMI è la 1.5.18 o successiva, per creare il bucket S3 puoi anche usare il comando `ec2-upload-bundle`. Per ulteriori informazioni, consulta ec2-upload-bundle.
- Assicurati che i file del tuo bundle non siano crittografati nel bucket S3. Se hai bisogno della crittografia per la tua AMI, puoi invece utilizzare un' EBS-backed AMI. Per ulteriori informazioni, consulta Usa la crittografia con le EBS-backed AMI.
- Assicurati di avere l'ID AWS del tuo account. Per ulteriori informazioni, consulta Visualizzare Account AWS gli identificatori nella Guida di riferimento per la gestione degli AWS account.
- Assicurati di disporre delle credenziali per utilizzare la AWS CLI. Per ulteriori informazioni, consulta Authentication and access credentials for the AWS CLI nella Guida per l'utente di AWS Command Line Interface .
- Assicurati di disporre di un X.509 certificato e della chiave privata corrispondente.

- Se devi creare un X.509 certificato, consultaGestione dei certificati di firma. Il X.509 certificato e la chiave privata vengono utilizzati per crittografare e decrittografare l'AMI.
- [Cina (Pechino)] Utilizza il certificato `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem`.
- [AWS GovCloud (US-West)] Usa il certificato. `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem`

- Connessione all'istanza e relativa personalizzazione. Ad esempio, è possibile installare software e applicazioni, copiare i dati, eliminare i file temporanei e modificare la configurazione Linux.

Creare un'AMI da un'istanza Amazon Linux

Le seguenti procedure descrivono come creare un'AMI da un'istanza con un volume root di archivio dell'istanza che esegue Amazon Linux 1. Potrebbero non funzionare per le istanze in esecuzione su altre distribuzioni Linux.

Per prepararsi a utilizzare gli strumenti AMI (solo istanze HVM)

1. Per essere avviati correttamente, gli strumenti AMI necessitano di GRUB Legacy. Utilizzare il comando seguente per installare GRUB:

   ```
   [ec2-user ~]$ sudo yum install -y grub
   ```

2. Installare i pacchetti di gestione delle partizioni usando il seguente comando:

   ```
   [ec2-user ~]$ sudo yum install -y gdisk kpartx parted
   ```

Per creare un'AMI da un'istanza Amazon Linux con un volume root di archivio dell'istanza

Questa procedura presuppone che i prerequisiti indicati in Prerequisiti siano stati soddisfatti.

Nei comandi seguenti, sostituisci ciascuno *`user input placeholder`* con le tue informazioni.

1. Caricare le credenziali nell'istanza. Le credenziali servono a garantire l'accesso all'AMI solo da parte dell'utente e da Amazon EC2.

   a. Creare una directory temporanea sull'istanza per le credenziali, come segue:

```
[ec2-user ~]$ mkdir /tmp/cert
```

In questo modo è possibile escludere le proprie credenziali dall'immagine creata.

b. Copia il X.509 certificato e la chiave privata corrispondente dal computer alla `/tmp/cert` directory dell'istanza utilizzando uno strumento di copia sicuro come scp. L'`-i` *my-private-key*`.pem`opzione nel scp comando seguente è la chiave privata che usi per connetterti alla tua istanza con SSH, non la chiave X.509 privata. Ad esempio:

```
you@your_computer:~ $ scp -i my-private-key.pem /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
```

In alternativa, poiché questi sono file di testo normale, è possibile aprire il certificato e la chiave in un editor di testo e copiarne il contenuto in nuovi file in `/tmp/cert`.

2. Preparare il bundle da caricare in Amazon S3 eseguendo il comando ec2-bundle-vol dall'istanza. Accertarsi di specificare l'opzione `-e` per escludere la directory in cui sono archiviate le proprie credenziali. Per impostazione predefinita, il processo di creazione di bundle esclude i file che possono contenere informazioni sensibili. Tali file includono `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` e `*/.bash_history`. Per includere tutti questi file, utilizzare l'opzione `--no-filter`. Per includere alcuni di questi file, utilizzare l'opzione `--include`.

> **Important**
>
> Per impostazione predefinita, il processo di raggruppamento dell'AMI crea una raccolta codificata di file nella directory `/tmp` che rappresenta il volume root. Se non è disponibile sufficiente spazio libero sul disco in `/tmp` per archiviare il bundle, occorre specificare una posizione diversa per il bundle da archiviare con l'opzione `-d` *`/path/to/bundle/storage`*. Alcune istanze dispongono di storage temporaneo montato su `/mnt` o `/media/ephemeral0` che è possibile utilizzare; in alternativa, è anche possibile creare, collegare e montare un nuovo volume Amazon EBS per l'archiviazione del bundle. Per

ulteriori informazioni, consulta Creare un volume di Amazon EBS nella Guida per l'utente di Amazon EBS.

a. Il ec2-bundle-vol comando deve essere eseguito come root. Per la maggior parte dei comandi, è possibile utilizzare sudo per ottenere autorizzazioni elevate, ma in questo caso occorre eseguire sudo -E su per mantenere le variabili di ambiente.

```
[ec2-user ~]$ sudo -E su
```

Si noti che il prompt bash ora identifica l'utente come utente root e il simbolo del dollaro è stato sostituito da un tag hash, a segnalare che ci si trova in una shell root:

```
[root ec2-user]#
```

b. Per creare il bundle dell'AMI, eseguire il comando ec2-bundle-vol come segue:

```
[root ec2-user]# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 123456789012 -r x86_64 -e /tmp/cert --
partition gpt
```

> **Note**
>
> Per le regioni Cina (Pechino) e AWS GovCloud (US-West), utilizza il `--ec2cert` parametro e specifica i certificati in base ai ??? prerequisiti.

Possono essere necessari alcuni minuti per creare l'immagine. Al termine di questo comando, la tua directory `/tmp` (o non predefinita) contiene il pacchetto (`image.manifest.xml`più diversi file). `image.part.` *xx*

c. Uscire dalla shell root.

```
[root ec2-user]# exit
```

3. (Facoltativo) Per aggiungere altri volumi instance store, modificare le mappature dei dispositivi a blocchi nel file `image.manifest.xml` dell'AMI. Per ulteriori informazioni, consulta Mappature dei dispositivi a blocchi per i volumi sulle istanze Amazon EC2.

a. Creare un backup del file `image.manifest.xml`.

```
[ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

b. Riformattare il file `image.manifest.xml` per renderne più semplice la lettura e la modifica.

```
[ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
image.manifest.xml
```

c. Modificare le mappature dei dispositivi a blocchi in `image.manifest.xml` con un editor di testo. Il seguente esempio mostra una nuova voce del volume instance store `ephemeral1`.

> **Note**
>
> Per un elenco dei file esclusi, consulta ec2-bundle-vol.

```
    <block_device_mapping>
      <mapping>
        <virtual>ami</virtual>
        <device>sda</device>
      </mapping>
      <mapping>
        <virtual>ephemeral0</virtual>
        <device>sdb</device>
      </mapping>
      <mapping>
        <virtual>ephemeral1</virtual>
        <device>sdc</device>
      </mapping>
      <mapping>
        <virtual>root</virtual>
        <device>/dev/sda1</device>
      </mapping>
    </block_device_mapping>
```

d. Salvare il file `image.manifest.xml` e uscire dall'editor di testo.

4. Per caricare il bundle su Amazon S3, eseguire il comando ec2-upload-bundle come segue.

```
[ec2-user ~]$ ec2-upload-bundle -b amzn-s3-demo-bucket/bundle_folder/bundle_name -
m /tmp/image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Per registrare l'AMI in una regione diversa da US East (N. Virginia), occorre specificare sia la regione di destinazione con l'opzione `--region` che un percorso del bucket esistente nella regione di destinazione oppure un percorso univoco del bucket che è possibile creare nella regione di destinazione.

5. (Facoltativo) Una volta caricato il bundle su Amazon S3, è possibile rimuoverlo dalla directory `/tmp` sull'istanza utilizzando il seguente comando rm:

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

> **Important**
>
> Se si è specificato un percorso con l'opzione `-d /path/to/bundle/storage` in Step 2, utilizzare quel percorso invece di `/tmp`.

6. Per registrare l'AMI, eseguire il comando register-image come segue.

```
[ec2-user ~]$ aws ec2 register-image --image-location amzn-s3-demo-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --
virtualization-type hvm
```

> **Important**
>
> Se precedentemente si è specificata una regione per il comando ec2-upload-bundle, specificarla nuovamente per questo comando.

Configurazione degli strumenti dell'AMI Amazon EC2

Puoi utilizzare gli strumenti AMI per creare e gestire le AMI di Amazon S3-backed Linux. Per usare gli strumenti, è necessario installarli sulla propria istanza Linux. Gli strumenti AMI sono disponibili sia come file RPM che come file .zip per le distribuzioni Linux che non supportano il formato RPM.

Per configurare gli strumenti AMI tramite il file RPM

1. Installare Ruby utilizzando il programma di gestione dei pacchetti per la distribuzione Linux in uso, come yum. Ad esempio:

```
[ec2-user ~]$ sudo yum install -y ruby
```

2. Scaricare il file RPM utilizzando uno strumento come wget o curl. Ad esempio:

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
```

3. Verificare la firma del file RPM tramite il seguente comando:

```
[ec2-user ~]$ rpm -K ec2-ami-tools.noarch.rpm
```

   Questo comando deve indicare che gli hash SHA1 e MD5 del file sono nello stato `OK`. Se il comando indica che gli hash sono nello stato `NOT OK`, utilizzare il seguente comando per visualizzare gli hash Header SHA1 e MD5 del file:

```
[ec2-user ~]$ rpm -Kv ec2-ami-tools.noarch.rpm
```

   Quindi, confrontare tali hash con i seguenti hash degli strumenti AMI verificati per confermare l'autenticità del file:

   - Header SHA1: a1f662d6f25f69871104e6a62187fa4df508f880
   - MD5: 9faff05258064e2f7909b66142de6782

   Se gli hash Header SHA1 e MD5 del file corrispondono agli hash degli strumenti AMI verificati, continuare con la fase successiva.

4. Installare il file RPM utilizzando il seguente comando:

```
[ec2-user ~]$ sudo yum install ec2-ami-tools.noarch.rpm
```

5. Verificare l'installazione degli strumenti AMI tramite il comando ec2-ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

> **Note**
>
> Se ricevi un errore di caricamento del tipo «impossibile caricare tale file -- ec2/amitools / version (LoadError)», completa il passaggio successivo per aggiungere la posizione di installazione degli strumenti AMI al tuo RUBYLIB percorso.

6. (Facoltativo) Se nella fase precedente si è ricevuto un errore, aggiungere la posizione dell'installazione degli strumenti AMI al percorso RUBYLIB.

   a. Eseguire il seguente comando per determinare i percorsi da aggiungere.

   ```
   [ec2-user ~]$ rpm -qil ec2-ami-tools | grep ec2/amitools/version
   /usr/lib/ruby/site_ruby/ec2/amitools/version.rb
   /usr/lib64/ruby/site_ruby/ec2/amitools/version.rb
   ```

   Nell'esempio di cui sopra, il file mancante indicato nel precedente errore di caricamento si trova in /usr/lib/ruby/site_ruby e /usr/lib64/ruby/site_ruby.

   b. Aggiungere le posizioni indicate nella fase precedente al percorso RUBYLIB.

   ```
   [ec2-user ~]$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/
   site_ruby
   ```

   c. Verificare l'installazione degli strumenti AMI tramite il comando ec2-ami-tools-version.

   ```
   [ec2-user ~]$ ec2-ami-tools-version
   ```

Per configurare gli strumenti AMI tramite il file .zip

1. Installare Ruby e decomprimerlo utilizzando il programma di gestione dei pacchetti per la distribuzione Linux in uso, come apt-get. Ad esempio:

   ```
   [ec2-user ~]$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
   ```

2. Scaricare il file .zip utilizzando uno strumento come wget o curl. Ad esempio:

   ```
   [ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
   ```

3. Decomprimere i file in una directory di installazione adatta, come /usr/local/ec2.

```
[ec2-user ~]$ sudo mkdir -p /usr/local/ec2
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

Nota che il file .zip contiene una cartella ec2-ami-tools-*x*.*x*.*x*, dove *x*.*x*.*x* è il numero di versione degli strumenti (ad esempio, `ec2-ami-tools-1.5.7`).

4. Impostare la variabile di ambiente `EC2_AMITOOL_HOME` sulla posizione directory di installazione degli strumenti. Ad esempio:

```
[ec2-user ~]$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

5. Aggiungere gli strumenti alla variabile di ambiente `PATH`. Ad esempio:

```
[ec2-user ~]$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

6. È possibile verificare l'installazione degli strumenti AMI tramite il comando ec2-ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

Gestione dei certificati di firma

Alcuni comandi degli strumenti AMI richiedono un certificato di firma (noto anche come X.509 certificato). È necessario creare il certificato e quindi caricarlo su AWS. Ad esempio, per creare il certificato puoi utilizzare uno strumento di terza parte come OpenSSL.

Per creare un certificato di firma

1. Installare e configurare OpenSSL
2. Creare una chiave privata usando il comando `openssl genrsa` e salvare l'output in un file `.pem`. È consigliabile creare una chiave RSA a 2048 o 4096 bit.

```
openssl genrsa 2048 > private-key.pem
```

3. Generare un certificato usando il comando `openssl req`.

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform PEM -
out certificate.pem
```

Per caricare il certificato su AWS, usa il comando https://docs.aws.amazon.com/cli/latest/reference/iam/upload-signing-certificate.html upload-signing-certificate.

```
aws iam upload-signing-certificate --user-name user-name --certificate-body
 file://path/to/certificate.pem
```

Per ottenere un elenco dei certificati disponibili per un utente, utilizzare il comando list-signing-certificates:

```
aws iam list-signing-certificates --user-name user-name
```

Per disattivare o riattivare un certificato di firma per un utente, utilizzare il comando update-signing-certificate. Il seguente comando disattiva il certificato:

```
aws iam update-signing-certificate --certificate-id OFHPLP4ZULTHYPMSYEX704BEXAMPLE --
status Inactive --user-name user-name
```

Per eliminare un certificato, utilizzare il comando delete-signing-certificate:

```
aws iam delete-signing-certificate --user-name user-name --certificate-
id OFHPLP4ZULTHYPMSYEX704BEXAMPLE
```

Riferimento strumenti AMI Amazon EC2

Puoi utilizzare i comandi degli strumenti AMI per creare e gestire le AMI di Amazon S3-backed Linux. Per impostare gli strumenti, consultare Configurazione degli strumenti dell'AMI Amazon EC2.

Per informazioni sulle chiavi di accesso, consulta Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente di IAM.

Comandi

- ec2-ami-tools-version
- ec2-bundle-image
- ec2-bundle-vol
- ec2-delete-bundle
- ec2-download-bundle

- ec2-migrate-manifest
- ec2-unbundle
- ec2-upload-bundle
- Opzioni comuni per gli strumenti AMI

ec2-ami-tools-version

Description

Descrive la versione degli strumenti AMI.

Sintassi

ec2-ami-tools-version

Output

Informazioni relative alla versione.

Esempio

Questo comando di esempio mostra le informazioni relative alla versione degli strumenti AMI che si stanno utilizzando.

```
[ec2-user ~]$ ec2-ami-tools-version
1.5.2 20071010
```

ec2-bundle-image

Description

Crea un'AMI Amazon S3-backed Linux da un'immagine del sistema operativo creata in un file di loopback.

Sintassi

ec2-bundle-image -c *path* -k *path* -u *account* -i *path* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [-p *prefix*]

Opzioni

`-c, --cert` path

Il file del certificato a chiave pubblica RSA codificato PEM dell'utente.

Campo obbligatorio: sì

`-k, --privatekey` path

Il percorso di un file chiave PEM-encoded RSA. Sarà necessario specificare questa chiave per separare questo bundle, quindi conservarla in un posto sicuro. Tieni presente che la chiave non deve essere registrata nel tuo AWS account.

Obbligatorio: sì

`-u, --user` account

L'ID dell' AWS account utente, senza trattini.

Obbligatorio: sì

`-i, --image` path

Il percorso dell'immagine da aggiungere al bundle.

Campo obbligatorio: sì

`-d, --destination` path

La directory in cui creare il bundle.

Default: `/tmp`

Campo obbligatorio: no

`--ec2cert` path

Il percorso del certificato a chiave X.509 pubblica Amazon EC2 utilizzato per crittografare il manifesto dell'immagine.

Le regioni `us-gov-west-1` e `cn-north-1` utilizzano un certificato di chiave pubblico non predefinito e il percorso di tale certificato deve essere specificato con questa opzione. Il percorso del certificato varia in base al metodo di installazione degli strumenti AMI. Per Amazon Linux, i certificati si trovano in `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se gli strumenti AMI

sono stati installati dal file RPM o ZIP in Configurazione degli strumenti dell'AMI Amazon EC2, i certificati si trovano in `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obbligatorio: Solo per le regioni `us-gov-west-1` e `cn-north-1`.

`-r, --arch` architecture

Architettura dell'immagine. Se non si fornisce l'architettura sulla riga di comando, verrà richiesta durante l'avvio del raggruppamento.

Valori validi: `i386` | `x86_64`

Campo obbligatorio: no

`--productcodes` code1,code2,...

I codici prodotto da collegare all'immagine al momento della registrazione, separati da virgole.

Campo obbligatorio: no

`-B, --block-device-mapping` mapping

Definisce come i dispositivi a blocchi sono esposti a un'istanza di questa AMI se il suo tipo di istanza supporta il dispositivo specificato.

Specificare un elenco di coppie chiave-valore separato da virgole, in cui ogni chiave è un nome virtuale e ogni valore è il nome del dispositivo corrispondente. Tra i nomi virtuali sono inclusi i seguenti:

- `ami` – Il dispositivo di sistema del file radice visto dall'istanza
- `root` – Il dispositivo di sistema del file radice visto dal kernel
- `swap` – Il dispositivo di scambio visto dall'istanza
- `ephemeralN` – Il volume Nesimo dell'instance store

Campo obbligatorio: no

`-p, --prefix` prefix

Il prefisso del nome del file per i file AMI raggruppati.

Predefinito: Il nome del file immagine. Per esempio, se il percorso dell'immagine è `/var/spool/my-image/version-2/debian.img`, il prefisso predefinito è `debian.img`.

Campo obbligatorio: no

`--kernel` kernel_id

Obsoleta. Utilizzare register-image per impostare il kernel.

Campo obbligatorio: no

`--ramdisk` ramdisk_id

Obsoleta. Utilizzare register-image per impostare il disco RAM se necessario.

Obbligatorio: no

Output

Messaggi di stato che descrivono le fasi e lo stato del processo di raggruppamento.

Esempio

Questo esempio crea un'AMI raggruppata da un'immagine del sistema operativo creata in un file di loopback.

```
[ec2-user ~]$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -i image.img -d bundled/ -r x86_64
Please specify a value for arch [i386]:
Bundling image file...
Splitting bundled/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
Created image.part.04
Created image.part.05
Created image.part.06
Created image.part.07
Created image.part.08
Created image.part.09
Created image.part.10
Created image.part.11
Created image.part.12
Created image.part.13
Created image.part.14
Generating digests for each part...
Digests generated.
```

```
Creating bundle manifest...
ec2-bundle-image complete.
```

ec2-bundle-vol

Description

Crea un'AMI Amazon S3-backed Linux comprimendo, crittografando e firmando una copia del volume principale per l'istanza.

Amazon EC2 tenta di ereditare codici prodotto, impostazioni del kernel, impostazioni del disco RAM e mappature dei dispositivi a blocchi dall'istanza.

Per impostazione predefinita, il processo di raggruppamento esclude i file che possono contenere informazioni sensibili. Tali file includono `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` e `*/.bash_history`. Per includere tutti questi file, utilizzare l'opzione `--no-filter`. Per includere alcuni di questi file, utilizzare l'opzione `--include`.

Per ulteriori informazioni, consulta Crea un' S3-backed AMI Amazon.

Sintassi

ec2-bundle-vol -c *path* -k *path* -u *account* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [--all] [-e *directory1*,*directory2*,...] [-i *file1*,*file2*,...] [--no-filter] [-p *prefix*] [-s *size*] [--[no-]inherit] [-v *volume*] [-P *type*] [-S *script*] [--fstab *path*] [--generate-fstab] [--grub-config *path*]

Opzioni

`-c, --cert` path

Il file del certificato a chiave pubblica RSA codificato PEM dell'utente.

Campo obbligatorio: sì

`-k, --privatekey` path

Il percorso del file di chiave PEM-encoded RSA dell'utente.

Obbligatorio: sì

`-u, --user` account

L'ID dell' AWS account dell'utente, senza trattini.

Obbligatorio: sì

`-d, --destination` destination

La directory in cui creare il bundle.

Default: `/tmp`

Campo obbligatorio: no

`--ec2cert` path

Il percorso del certificato a chiave X.509 pubblica Amazon EC2 utilizzato per crittografare il manifesto dell'immagine.

Le regioni `us-gov-west-1` e `cn-north-1` utilizzano un certificato di chiave pubblico non predefinito e il percorso di tale certificato deve essere specificato con questa opzione. Il percorso del certificato varia in base al metodo di installazione degli strumenti AMI. Per Amazon Linux, i certificati si trovano in `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se gli strumenti AMI sono stati installati dal file RPM o ZIP in Configurazione degli strumenti dell'AMI Amazon EC2, i certificati si trovano in `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obbligatorio: Solo per le regioni `us-gov-west-1` e `cn-north-1`.

`-r, --arch` architecture

L'architettura dell'immagine. Se non la si fornisce sulla riga di comando, verrà richiesto di fornirla durante l'avvio del raggruppamento.

Valori validi: `i386` | `x86_64`

Campo obbligatorio: no

`--productcodes` code1,code2,...

I codici prodotto da collegare all'immagine al momento della registrazione, separati da virgole.

Campo obbligatorio: no

`-B, --block-device-mapping` mapping

Definisce come i dispositivi a blocchi sono esposti a un'istanza di questa AMI se il suo tipo di istanza supporta il dispositivo specificato.

Specificare un elenco di coppie chiave-valore separato da virgole, in cui ogni chiave è un nome virtuale e ogni valore è il nome del dispositivo corrispondente. Tra i nomi virtuali sono inclusi i seguenti:

- `ami` – Il dispositivo di sistema del file radice visto dall'istanza
- `root` – Il dispositivo di sistema del file radice visto dal kernel
- `swap` – Il dispositivo di scambio visto dall'istanza
- `ephemeralN` – Il volume Nesimo dell'instance store

Campo obbligatorio: no

`-a, --all`

Raggruppare tutte le directory, comprese quelle su sistemi di file montati in remoto.

Campo obbligatorio: no

`-e, --exclude` directory1,directory2,...

Un elenco di percorsi e file di directory assoluti da escludere dall'operazione di creazione di bundle. Questo parametro sostituisce l'opzione `--all` . Quando si specifica l'opzione di esclusione, le directory e sottodirectory elencate con il parametro non verranno raggruppate con il volume.

Campo obbligatorio: no

`-i, --include` file1,file2,...

Un elenco dei file da includere nell'operazione di creazione di bundle. I file specificati sarebbero altrimenti esclusi dall'AMI in quanto potrebbero contenere informazioni sensibili.

Campo obbligatorio: no

`--no-filter`

Se specificato, non verranno esclusi file dall'AMI in quanto potrebbero contenere informazioni sensibili.

Campo obbligatorio: no

`-p, --prefix` prefix

Il prefisso del nome del file per i file AMI raggruppati.

Impostazione predefinita: `image`

Campo obbligatorio: no

`-s, --size` size

La dimensione, in MB (1024 x 1024 byte), del file di immagine da creare. La dimensione massima è 10240 MB.

Impostazione predefinita: 10240

Campo obbligatorio: no

`--[no-]inherit`

Indica se l'immagine deve ereditare i metadati dell'istanza (l'impostazione predefinita è ereditare). Il raggruppamento non va a buon fine se si attiva `--inherit` ma i metadati dell'istanza non sono accessibili.

Campo obbligatorio: no

`-v, --volume` volume

Il percorso assoluto del volume montato da cui creare il bundle.

Impostazione predefinita: la directory radice (/)

Campo obbligatorio: no

`-P, --partition` type

Indica se l'immagine del disco deve utilizzare una tabella di partizione. Se non si specifica un tipo di tabella di partizione, quello predefinito è il tipo utilizzato dal principale dispositivo a blocchi del volume, se applicabile, altrimenti quello predefinito è `gpt`.

Valori validi: `mbr` | `gpt` | `none`

Campo obbligatorio: no

`-S, --script` script

Uno script di personalizzazione da eseguire appena prima del raggruppamento. Lo script deve aspettarsi un argomento singolo, il punto di montaggio del volume.

Campo obbligatorio: no

`--fstab` path

Il percorso di fstab da aggiungere in bundle all'immagine. Se questo non è specificato, Amazon EC2 raggruppa/. etc/fstab

Obbligatorio: no

`--generate-fstab`

Raggruppa il volume utilizzando Amazon fstab. EC2-provided

Obbligatorio: no

`--grub-config`

Il percorso di un file di configurazione di sgombero alternato da aggiungere in bundle all'immagine. Per impostazione predefinita, `ec2-bundle-vol` si aspetta che `/boot/grub/menu.lst` o `/boot/grub/grub.conf` esistano nell'immagine clonata. Questa opzione consente di indicare un percorso di un file di configurazione di sgombero alternato che poi verrà copiato sui predefiniti (se presenti).

Campo obbligatorio: no

`--kernel` kernel_id

Obsoleta. Utilizzare register-image per impostare il kernel.

Campo obbligatorio: no

`--ramdisk`ramdisk_id

Obsoleta. Utilizzare register-image per impostare il disco RAM se necessario.

Obbligatorio: no

Output

Messaggi di stato che descrivono le fasi e lo stato del raggruppamento.

Esempio

Questo esempio crea un'AMI raggruppata comprimendo, crittografando e firmando uno snapshot del sistema di file radice della macchina locale.

```
[ec2-user ~]$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c
 cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -r x86_64
  Copying / into the image file /mnt/image...
```

```
  Excluding:
       sys
       dev/shm
       proc
       dev/pts
       proc/sys/fs/binfmt_misc
       dev
       media
       mnt
       proc
       sys
       tmp/image
       mnt/img-mnt
  1+0 records in
  1+0 records out
  mke2fs 1.38 (30-Jun-2005)
  warning: 256 blocks unused.

  Splitting /mnt/image.gz.crypt...
  Created image.part.00
  Created image.part.01
  Created image.part.02
  Created image.part.03
  ...
  Created image.part.22
  Created image.part.23
  Generating digests for each part...
  Digests generated.
  Creating bundle manifest...
  Bundle Volume complete.
```

ec2-delete-bundle

Description

Elimina il bundle specificato dall'archiviazione Amazon S3. Dopo aver eliminato un bundle, non è possibile avviare istanze dall'AMI corrispondente.

Sintassi

ec2-delete-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* [-t *token*] [--url *url*] [--region *region*] [--sigv *version*] [-m *path*] [-p *prefix*] [--clear] [--retry] [-y]

Opzioni

`-b, --bucket` bucket

Il nome del bucket Amazon S3 che contiene l'AMI raggruppata, seguito da un prefisso facoltativo di percorso delimitato da "/"

Campo obbligatorio: sì

`-a, --access-key` access_key_id

L'ID della chiave di AWS accesso.

Obbligatorio: sì

`-s, --secret-key` secret_access_key

La chiave di accesso AWS segreta.

Obbligatorio: sì

`-t, --delegation-token` token

Il token di delega da trasmettere alla AWS richiesta. Per ulteriori informazioni, consulta Temporary security credentials nella Guida per l'utente IAM.

Obbligatorio: Solo quando si utilizzano credenziali di sicurezza temporanee.

Predefinito: Il valore della variabile ambientale `AWS_DELEGATION_TOKEN` (se impostata).

`--region`region

La regione da utilizzare nella firma di richiesta.

Impostazione predefinita: `us-east-1`

Obbligatorio: Obbligatorio se si utilizza la versione 4 di firma

`--sigv`version

La versione della firma da utilizzare durante la firma della richiesta.

Valori validi: `2 | 4`

Default: `4`

Campo obbligatorio: no

`-m, --manifestpath`

Il percorso del file manifest.

Obbligatorio: È necessario specificare `--prefix` o `--manifest`.

`-p, --prefix` prefix

Il prefisso del nome del file AMI raggruppato. Fornire il prefisso completo. Per esempio, se il prefisso è image.img, utilizzare `-p image.img` e non `-p image`.

Obbligatorio: È necessario specificare `--prefix` o `--manifest`.

`--clear`

Cancella il bucket Amazon S3 se è vuoto dopo aver eliminato il bundle specificato.

Campo obbligatorio: no

`--retry`

Ripete automaticamente i tentativi su tutti gli errori Amazon S3, fino a cinque volte per operazione.

Campo obbligatorio: no

`-y, --yes`

Suppone automaticamente che la risposta a tutte le richieste sia sì.

Obbligatorio: no

Output

Amazon EC2 visualizza i messaggi di stato che indicano gli stadi e lo stato del processo di eliminazione.

Esempio

In questo esempio viene eliminato un bundle da Amazon S3.

```
[ec2-user ~]$ ec2-delete-bundle -b amzn-s3-demo-bucket -a your_access_key_id -
s your_secret_access_key
Deleting files:
```

```
amzn-s3-demo-bucket/image.manifest.xml
amzn-s3-demo-bucket/image.part.00
amzn-s3-demo-bucket/image.part.01
amzn-s3-demo-bucket/image.part.02
amzn-s3-demo-bucket/image.part.03
amzn-s3-demo-bucket/image.part.04
amzn-s3-demo-bucket/image.part.05
amzn-s3-demo-bucket/image.part.06
Continue? [y/n]
y
Deleted amzn-s3-demo-bucket/image.manifest.xml
Deleted amzn-s3-demo-bucket/image.part.00
Deleted amzn-s3-demo-bucket/image.part.01
Deleted amzn-s3-demo-bucket/image.part.02
Deleted amzn-s3-demo-bucket/image.part.03
Deleted amzn-s3-demo-bucket/image.part.04
Deleted amzn-s3-demo-bucket/image.part.05
Deleted amzn-s3-demo-bucket/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

Description

Scarica le AMI Amazon S3-backed Linux specificate dallo storage Amazon S3.

Sintassi

ec2-download-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* -k *path* [--url *url*] [--region *region*] [--sigv *version*] [-m *file*] [-p *prefix*] [-d *directory*] [--retry]

Opzioni

`-b, --bucket` bucket

Il nome del bucket Amazon S3 dove è posizionato il bundle, seguito da un prefisso facoltativo di percorso delimitato da "/".

Campo obbligatorio: sì

`-a, --access-key` access_key_id

L'ID della chiave di AWS accesso.

Obbligatorio: sì

`-s, --secret-key` secret_access_key

La chiave di accesso AWS segreta.

Obbligatorio: sì

`-k, --privatekey` path

La chiave privata utilizzata per decrittografare il manifest.

Campo obbligatorio: sì

`--url` url

L'URL di servizio Amazon S3.

Default: `https://s3.amazonaws.com/`

Campo obbligatorio: no

`--region` region

La regione da utilizzare nella firma di richiesta.

Impostazione predefinita: `us-east-1`

Obbligatorio: Obbligatorio se si utilizza la versione 4 di firma

`--sigv` Versione

La versione della firma da utilizzare durante la firma della richiesta.

Valori validi: `2` | `4`

Default: `4`

Campo obbligatorio: no

`-m, --manifest` file

Il nome del file manifest (senza il percorso). Si consiglia di specificare il manifest (`-m`) o un prefisso (`-p`).

Campo obbligatorio: no

`-p, --prefix prefix`

Il prefisso del nome del file per i file AMI raggruppati.

Impostazione predefinita: `image`

Campo obbligatorio: no

`-d, --directory directory`

La directory dove viene salvato il bundle scaricato. La directory deve esistere.

Predefinito: La directory di lavoro corrente.

Campo obbligatorio: no

`--retry`

Ripete automaticamente i tentativi su tutti gli errori Amazon S3, fino a cinque volte per operazione.

Obbligatorio: no

Output

Vengono visualizzati i messaggi di stato che indicano le varie fasi del processo di download.

Esempio

Questo esempio crea la directory `bundled` (tramite il comando di Linux mkdir) e scarica il bundle dal bucket Amazon S3 `amzn-s3-demo-bucket`.

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b amzn-s3-demo-bucket/bundles/bundle_name
 -m image.manifest.xml -a your_access_key_id -s your_secret_access_key -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d mybundle
Downloading manifest image.manifest.xml from amzn-s3-demo-bucket to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.00 ...
Downloaded image.part.00 from amzn-s3-demo-bucket
Downloading part image.part.01 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.01 ...
Downloaded image.part.01 from amzn-s3-demo-bucket
Downloading part image.part.02 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.02 ...
```

```
Downloaded image.part.02 from amzn-s3-demo-bucket
Downloading part image.part.03 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.03 ...
Downloaded image.part.03 from amzn-s3-demo-bucket
Downloading part image.part.04 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.04 ...
Downloaded image.part.04 from amzn-s3-demo-bucket
Downloading part image.part.05 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.05 ...
Downloaded image.part.05 from amzn-s3-demo-bucket
Downloading part image.part.06 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.06 ...
Downloaded image.part.06 from amzn-s3-demo-bucket
```

ec2-migrate-manifest

Description

Modifica un'AMI Amazon S3-backed Linux (ad esempio, il certificato, il kernel e il disco RAM) in modo che supporti una regione diversa.

Sintassi

ec2-migrate-manifest -c *path* -k *path* -m *path* {(-a *access_key_id* -s *secret_access_key* --region *region*) | (--no-mapping)} [--ec2cert *ec2_cert_path*] [--kernel *kernel-id*] [--ramdisk *ramdisk_id*]

Opzioni

`-c, --cert` path

Il file del certificato a chiave pubblica RSA codificato PEM dell'utente.

Campo obbligatorio: sì

`-k, --privatekey` path

Il percorso del file di chiave PEM-encoded RSA dell'utente.

Obbligatorio: sì

`--manifest` path

Il percorso del file manifest.

Campo obbligatorio: sì

`-a, --access-key` access_key_id

L'ID della chiave di AWS accesso.

Obbligatorio: Obbligatorio se si utilizza la mappatura automatica.

`-s, --secret-key` secret_access_key

La chiave di accesso AWS segreta.

Obbligatorio: Obbligatorio se si utilizza la mappatura automatica.

`--region` region

La regione da cercare nel file di mappatura.

Obbligatorio: Obbligatorio se si utilizza la mappatura automatica.

`--no-mapping`

Disattiva la mappatura automatica dei kernel e dei dischi RAM.

Durante la migrazione, Amazon EC2 sostituisce il kernel e il disco RAM nel file manifest con un kernel e un disco RAM progettati per la regione di destinazione. A meno che non venga fornito il parametro `--no-mapping`, `ec2-migrate-bundle` deve utilizzare le operazioni `DescribeRegions` e `DescribeImages` per eseguire le mappature automatiche.

Obbligatorio: Obbligatorio se non si forniscono le opzioni `-a`, `-s` e `--region` utilizzate per la mappatura automatica.

`--ec2cert` path

Il percorso del certificato a chiave X.509 pubblica Amazon EC2 utilizzato per crittografare il manifesto dell'immagine.

Le regioni `us-gov-west-1` e `cn-north-1` utilizzano un certificato di chiave pubblico non predefinito e il percorso di tale certificato deve essere specificato con questa opzione. Il percorso del certificato varia in base al metodo di installazione degli strumenti AMI. Per Amazon Linux, i certificati si trovano in `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se gli strumenti AMI sono stati installati dal file ZIP in Configurazione degli strumenti dell'AMI Amazon EC2, i certificati si trovano in `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obbligatorio: Solo per le regioni `us-gov-west-1` e `cn-north-1`.

`--kernel` kernel_id

L'ID del kernel da selezionare.

> **Important**
>
> Ti consigliamo di utilizzare PV-GRUB al posto dei kernel e dei dischi RAM. Per ulteriori informazioni, consulta Kernel forniti dall'utente nella Guida per l'utente di Amazon Linux 2.

Obbligatorio: no

`--ramdisk` ramdisk_id

L'ID del disco RAM da selezionare.

> **Important**
>
> Si consiglia di utilizzare PV-GRUB al posto dei kernel e dei dischi RAM. Per ulteriori informazioni, consulta Kernel forniti dall'utente nella Guida per l'utente di Amazon Linux 2.

Obbligatorio: no

Output

Messaggi di stato che descrivono le fasi e lo stato del processo di raggruppamento.

Esempio

Questo esempio copia l'AMI specificata nel manifest `my-ami.manifest.xml` dagli Stati Uniti all'Unione Europea.

```
[ec2-user ~]$ ec2-migrate-manifest --manifest my-ami.manifest.xml
 --cert cert-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --privatekey pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --region eu-west-1

Backing up manifest...
Successfully migrated my-ami.manifest.xml It is now suitable for use in eu-west-1.
```

ec2-unbundle

Description

Re-creates il pacchetto di un'AMI Amazon Linux. S3-backed

Sintassi

`ec2-unbundle -k path -m path [-s source_directory] [-d destination_directory]`

Opzioni

`-k, --privatekey` path

Il percorso del tuo file chiave PEM-encoded RSA.

Obbligatorio: sì

`-m, --manifest` path

Il percorso del file manifest.

Campo obbligatorio: sì

`-s, --source` source_directory

La directory che contiene il bundle.

Predefinita: La directory attuale.

Campo obbligatorio: no

`-d, --destination` destination_directory

La directory in cui disaggregare l'AMI. La directory di destinazione deve esistere.

Predefinita: La directory attuale.

Obbligatorio: no

Esempio

Questo esempio Linux e UNIX disaggrega l'AMI specificata nel file `image.manifest.xml`.

```
[ec2-user ~]$ mkdir unbundled
$ ec2-unbundle -m mybundle/image.manifest.xml -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -s mybundle -d unbundled
$ ls -l unbundled
total 1025008
-rw-r--r-- 1 root root 1048578048 Aug 25 23:46 image.img
```

Output

Vengono visualizzati i messaggi di stato che indicano le varie fasi del processo di disaggregazione.

ec2-upload-bundle

Description

Carica il pacchetto per un'AMI Amazon S3-backed Linux su Amazon S3 e imposta gli elenchi di controllo degli accessi (ACL) appropriati sugli oggetti caricati. Per ulteriori informazioni, consulta Crea un' S3-backed AMI Amazon.

> **Note**
>
> Per caricare oggetti in un bucket S3 per la tua AMI Amazon S3-backed Linux, gli ACL devono essere abilitati per il bucket. In caso contrario, Amazon EC2 non sarà in grado di impostare le ACL sugli oggetti da caricare. Se il bucket di destinazione utilizza l'impostazione applicata dal proprietario del bucket per S3 Object Ownership, ciò non funzionerà perché le ACL sono disabilitate. Per ulteriori informazioni, consulta Controllo della proprietà degli oggetti e disabilitazione delle ACL per il bucket.

Sintassi

```
ec2-upload-bundle -b bucket -a access_key_id -s secret_access_key [-t
token] -m path [--url url] [--region region] [--sigv version] [--acl acl]
[-d directory] [--part part] [--retry] [--skipmanifest]
```

Opzioni

`-b, --bucket` bucket

Il nome del bucket Amazon S3 dove memorizzare il bundle, seguito da un prefisso facoltativo di percorso delimitato da "/". Se il bucket non esiste, viene creato se il nome del bucket è disponibile.

Inoltre, se il bucket non esiste e la versione degli strumenti AMI è 1.5.18 o successiva, questo comando imposta le ACL per il bucket.

Obbligatorio: sì

`-a, --access-key` access_key_id

L'ID della tua chiave AWS di accesso.

Obbligatorio: sì

`-s, --secret-key` secret_access_key

La tua chiave di accesso AWS segreta.

Obbligatorio: sì

`-t, --delegation-token` token

Il token di delega da trasmettere alla AWS richiesta. Per ulteriori informazioni, consulta Temporary security credentials nella Guida per l'utente IAM.

Obbligatorio: Solo quando si utilizzano credenziali di sicurezza temporanee.

Predefinito: Il valore della variabile ambientale `AWS_DELEGATION_TOKEN` (se impostata).

`-m, --manifest` path

Il percorso del file manifest. Il file manifest viene creato durante il processo di raggruppamento e si può trovare nella directory che contiene il bundle.

Campo obbligatorio: sì

`--url` url

Obsoleta. Invece, utilizzare l'opzione `--region` a meno che il bucket non sia limitato alla posizione EU (e non `eu-west-1`). Il contrassegno `--location` è l'unico modo per mirare a quella specifica limitazione di posizione.

L'URL di servizio endpoint Amazon S3.

Default: `https://s3.amazonaws.com/`

Campo obbligatorio: no

`--region` region

La regione da utilizzare nella firma di richiesta per il bucket S3 di destinazione.

- Se il bucket non esiste e non si specifica una regione, lo strumento crea il bucket senza un vincolo di posizione (in `us-east-1`).
- Se il bucket non esiste e si specifica una regione, lo strumento crea il bucket nella regione specificata.
- Se il bucket esiste e non si specifica una regione, lo strumento utilizza la posizione del bucket.
- Se il bucket esiste e si specifica `us-east-1` come regione, lo strumento utilizza la posizione reale del bucket senza alcun messaggio di errore e senza che i file corrispondenti esistenti vengano sovrascritti.
- Se il bucket esiste e si specifica una regione (diversa da `us-east-1`) che non corrisponde alla posizione reale del bucket, lo strumento dà un errore.

Se il bucket è limitato alla posizione EU (e non `eu-west-1`), utilizzare il contrassegno `--location`. Il contrassegno `--location` è l'unico modo per mirare a quella specifica limitazione di posizione.

Impostazione predefinita: `us-east-1`

Obbligatorio: Obbligatorio se si utilizza la versione 4 di firma

`--sigv` Versione

La versione della firma da utilizzare durante la firma della richiesta.

Valori validi: `2` | `4`

Default: `4`

Campo obbligatorio: no

`--acl` acl

La policy della lista di controllo accessi dell'immagine raggruppata.

Valori validi: `public-read` | `aws-exec-read`

Default: `aws-exec-read`

Campo obbligatorio: no

`-d, --directory` directory

La directory che contiene le parti dell'AMI raggruppata.

Predefinito: La directory che contiene il file manifest (consultare l'opzione `-m`).

Campo obbligatorio: no

`--part` part

Inizia a caricare la parte specificata e tutte le parti successive. Ad esempio, `--part 04`.

Campo obbligatorio: no

`--retry`

Ripete automaticamente i tentativi su tutti gli errori Amazon S3, fino a cinque volte per operazione.

Campo obbligatorio: no

`--skipmanifest`

Non carica il manifest.

Campo obbligatorio: no

`--location` location

Obsoleta. Invece, utilizzare l'opzione `--region`, a meno che il bucket non sia limitato alla posizione EU (e non `eu-west-1`). Il contrassegno `--location` è l'unico modo per mirare a quella specifica limitazione di posizione.

La limitazione di posizione del bucket Amazon S3 di destinazione. Se il bucket esiste e si specifica una posizione che non corrisponde alla posizione reale del bucket, lo strumento dà un errore. Se il bucket esiste e non si specifica una posizione, lo strumento utilizza la posizione del bucket. Se il bucket non esiste e si specifica una posizione, lo strumento crea il bucket nella posizione specificata. Se il bucket non esiste e non si specifica una posizione, lo strumento crea il bucket senza un vincolo di posizione (in `us-east-1`).

Predefinito: Se `--region` viene specificato, viene impostata la posizione per quella regione specificata. Se `--region` non viene specificata, la posizione predefinita è `us-east-1`.

Obbligatorio: no

Output

Amazon EC2 visualizza i messaggi di stato che indicano gli stadi e lo stato del processo di caricamento.

Esempio

Questo esempio carica il bundle specificato dal manifest `image.manifest.xml`.

```
[ec2-user ~]$ ec2-upload-bundle -b amzn-s3-demo-bucket/bundles/bundle_name -m
 image.manifest.xml -a your_access_key_id -s your_secret_access_key
Creating bucket...
Uploading bundled image parts to the S3 bucket amzn-s3-demo-bucket ...
Uploaded image.part.00
Uploaded image.part.01
Uploaded image.part.02
Uploaded image.part.03
Uploaded image.part.04
Uploaded image.part.05
Uploaded image.part.06
Uploaded image.part.07
Uploaded image.part.08
Uploaded image.part.09
Uploaded image.part.10
Uploaded image.part.11
Uploaded image.part.12
Uploaded image.part.13
Uploaded image.part.14
Uploading manifest ...
Uploaded manifest.
Bundle upload completed.
```

Opzioni comuni per gli strumenti AMI

La maggior parte degli strumenti AMI accettano i parametri facoltativi seguenti.

`--help, -h`

Visualizza il messaggio di aiuto.

`--version`

Visualizza la versione e l'avviso di copyright.

`--manual`

Visualizza l'immissione manuale.

`--batch`

Funziona in modalità batch, sopprimendo le richieste interattive.

`--debug`

Visualizza le informazioni che possono essere utili durante la risoluzione dei problemi.

Converti la tua Amazon AMI in un'AMI S3-backed EBS-backed

Puoi convertire un'AMI Amazon S3-backed Linux di tua proprietà in un'AMI Amazon EBS-backed Linux.

> **Important**
>
> Non puoi convertire un'AMI che non è di tua proprietà.

Per convertire un' S3-backed AMI Amazon in un' EBS-backed AMI Amazon

1. Avvia un'istanza Amazon Linux da un' EBS-backed AMI Amazon. Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console. Le istanze Amazon Linux hanno gli strumenti AWS CLI e AMI preinstallati.
2. Carica la chiave X.509 privata che hai usato per raggruppare la tua Amazon S3-backed AMI nella tua istanza. Questa chiave serve a garantire l'accesso all'AMI solo da parte dell'utente e da Amazon EC2.

   a. Crea una directory temporanea sulla tua istanza per la tua chiave X.509 privata come segue:

   ```
   [ec2-user ~]$ mkdir /tmp/cert
   ```

   b. Copia la tua chiave X.509 privata dal tuo computer nella `/tmp/cert` directory dell'istanza, usando uno strumento di copia sicuro come scp. Il *`my-private-key`* parametro nel comando seguente è la chiave privata che usi per connetterti alla tua istanza con SSH. Ad esempio:

```
you@your_computer:~ $ scp -i my-private-key.pem /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
```

3. Configura le tue variabili ambiente per usare la AWS CLI. Per ulteriori informazioni, consulta Variabili di ambiente.

   a. (Consigliato) Imposta le variabili di ambiente per la chiave di AWS accesso, la chiave segreta e il token di sessione.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   [ec2-user ~]$ export AWS_SESSION_TOKEN=your_session_token
   ```

   b. Imposta le variabili di ambiente per la tua chiave di AWS accesso e la chiave segreta.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   ```

4. Preparare un volume Amazon Elastic Block Store (Amazon EBS) per la nuova AMI.

   a. Creare un volume EBS vuoto nella stessa zona di disponibilità dell'istanza utilizzando il comando create-volume. Prendere nota dell'ID del volume nell'output del comando.

   > **Important**
   >
   > Questo volume EBS deve essere uguale o maggiore delle dimensioni del volume root instance store originale.

   ```
   aws ec2 create-volume \
       --size 10 \
       --region us-west-2 \
       --availability-zone us-west-2b
   ```

   b. Collega il volume alla tua EBS-backed istanza Amazon utilizzando il comando attach-volume.

   ```
   aws ec2 attach-volume \
   ```

```
    --volume-id vol-01234567890abcdef \
    --instance-id i-1234567890abcdef0 \
    --region us-west-2
```

5. Creare una cartella per il bundle.

```
[ec2-user ~]$ mkdir /tmp/bundle
```

6. Scaricare il bundle dell'AMI basata su instance store in `/tmp/bundle` utilizzando il comando ec2-download-bundle.

```
[ec2-user ~]$ ec2-download-bundle -b amzn-s3-demo-bucket/bundle_folder/bundle_name
 -m image.manifest.xml -a $AWS_ACCESS_KEY_ID -s $AWS_SECRET_ACCESS_KEY --
privatekey /path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

7. Ricostruire il file di immagine dal bundle utilizzando il comando ec2-unbundle.

   a. Cambiare directory nella cartella del bundle.

```
[ec2-user ~]$ cd /tmp/bundle/
```

   b. Esegui il comando ec2-unbundle.

```
[ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
```

8. Copiare i file dall'immagine disaggregata nel nuovo volume EBS.

```
[ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
```

9. Esaminare il volume cercando eventuali partizioni disaggregate.

```
[ec2-user bundle]$ sudo partprobe /dev/sdb1
```

10. Elencare i dispositivi a blocchi per individuare il nome del dispositivo da montare.

```
[ec2-user bundle]$ lsblk
NAME         MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/sda    202:0    0   8G  0 disk
##/dev/sda1 202:1    0   8G  0 part /
/dev/sdb    202:80   0  10G  0 disk
##/dev/sdb1 202:81   0  10G  0 part
```

In questo esempio, la partizione da montare è `/dev/sdb1`, ma il nome del dispositivo probabilmente sarà diverso. Se il volume non è partizionato, il dispositivo da montare sarà simile a `/dev/sdb` (senza una cifra finale della partizione del dispositivo).

11. Creare un punto di montaggio per il nuovo volume EBS e montare il volume.

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. Aprire il file `/etc/fstab` sul volume EBS con l'editor di testo preferito (ad esempio vim o nano) e rimuovere tutte le voci dei volumi instance store (temporanei). Poiché il volume EBS è montato su `/mnt/ebs`, il file `fstab` si trova in `/mnt/ebs/etc/fstab`.

```
[ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
#
LABEL=/     /           ext4    defaults,noatime  1   1
tmpfs       /dev/shm    tmpfs   defaults        0   0
devpts      /dev/pts    devpts  gid=5,mode=620  0   0
sysfs       /sys        sysfs   defaults        0   0
proc        /proc       proc    defaults        0   0
/dev/sdb        /media/ephemeral0       auto    defaults,comment=cloudconfig    0
     2
```

In questo esempio, l'ultima riga deve essere rimossa.

13. Smontare il volume e distaccarlo dall'istanza.

```
[ec2-user bundle]$ sudo umount /mnt/ebs
[ec2-user bundle]$ aws ec2 detach-volume --volume-id vol-01234567890abcdef --
region us-west-2
```

14. Creare un'AMI dal nuovo volume EBS come segue:

    a. Creare uno snapshot del nuovo volume EBS.

```
[ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description
 "your_snapshot_description" --volume-id vol-01234567890abcdef
```

    b. Controllare se la snapshot è completa.

```
[ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-
id snap-0abcdef1234567890
```

c. Identificare l'architettura del processore, il tipo di virtualizzazione e l'immagine del kernel (`aki`) utilizzati sull'AMI originale tramite il comando describe-images. Per questo passaggio è necessario l'ID AMI dell'Amazon S3-backed AMI originale.

```
[ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-
id ami-0abcdef1234567890 --output text
IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon
 available public machine aki-fc8f11cc instance-store paravirtual xen
```

In questo esempio, l'architettura è `x86_64` e l'ID dell'immagine del kernel è `aki-fc8f11cc`. Utilizzare questi valori nella fase seguente. Se l'output del comando sopra include anche un ID `ari`, prenderne nota.

d. Registrare la nuova AMI con l'ID dello snapshot del nuovo volume EBS e i valori della fase precedente. Se nell'output del comando precedente è incluso un ID `ari`, includerlo nel seguente comando con `--ramdisk-id` *ari_id*.

```
[ec2-user bundle]$ aws ec2 register-image --region us-west-2 --
name your_new_ami_name --block-device-mappings DeviceName=device-
name,Ebs={SnapshotId=snap-0abcdef1234567890} --virtualization-type paravirtual
 --architecture x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
```

15. (Facoltativo) Dopo avere verificato di poter avviare un'istanza dalla nuova AMI, è possibile eliminare il volume EBS creato per questa procedura.

```
aws ec2 delete-volume --volume-id vol-01234567890abcdef
```

Creare un'AMI Amazon EC2 utilizzando Windows Sysprep

Lo strumento Microsoft System Preparation (Windows Sysprep) crea una versione generalizzata del sistema operativo, con la configurazione di sistema specifica dell'istanza rimossa prima di acquisire una nuova immagine.

Si consiglia di utilizzare EC2 Image Builder per automatizzare la creazione, la gestione e la distribuzione di immagini server "gold" personalizzate, sicure e aggiornate preinstallate e preconfigurate con software e impostazioni.

Puoi anche utilizzare Windows Sysprep per creare un'AMI standardizzata utilizzando gli agenti di avvio di Windows: EC2Launch v2, EC2Launch e EC2Config.

> **Important**
>
> Non si deve utilizzare Windows Sysprep per creare il backup di un'istanza. Windows Sysprep rimuove le informazioni specifiche di sistema. La rimozione di tali informazioni può avere conseguenze indesiderate sul backup di un'istanza.

Per risolvere i problemi relativi a Windows Sysprep, vedere Risoluzione dei problemi di Sysprep relativi alle istanze Amazon EC2 Windows.

Indice

- Fasi di Windows Sysprep
- Prima di iniziare
- Crea un'AMI utilizzando Windows Sysprep con EC2Launch v2
- Crea un'AMI utilizzando Windows Sysprep con EC2Launch
- Crea un'AMI utilizzando Windows Sysprep con EC2Config

Fasi di Windows Sysprep

L'esecuzione di Windows Sysprep avviene nelle fasi seguenti:

- Generalizzazione: lo strumento Sysprep rimuove le informazioni e le configurazioni specifiche dell'immagine. Per esempio, Windows Sysprep rimuove l'identificatore di sicurezza (SID), il nome del computer, i log di eventi e i driver specifici, per citarne alcune. Dopo il completamento di questa fase, il sistema operativo (SO) è pronto a creare un'AMI.

> **Note**
>
> Quando esegui Windows Sysprep con gli agenti di avvio di Windows, il sistema impedisce la rimozione dei driver perché `PersistAllDeviceInstalls` è impostato su true per impostazione predefinita.

- Specialize (Specializzazione): Plug and Play esegue un'analisi del computer e installa i driver per ogni dispositivo rilevato. Lo strumento Sysprep genera i requisiti del SO, quali il nome del computer e il SID. Facoltativamente, è possibile eseguire comandi in questa fase.
- Out-of-Box Esperienza (OOBE): il sistema esegue una versione abbreviata del programma di installazione di Windows e richiede di immettere informazioni come la lingua del sistema, il fuso orario e l'organizzazione registrata. Quando esegui Windows Sysprep con gli agenti di avvio di Windows, il file di risposta automatizza questa fase.

Prima di iniziare

- Prima di eseguire Windows Sysprep, ti consigliamo di rimuovere tutti gli account utente locali e tutti i profili account diversi da un account amministratore singolo in cui Windows Sysprep verrà eseguito. Se esegui Windows Sysprep con account e profili aggiuntivi, si può verificare un comportamento imprevisto, inclusi perdita di dati del profilo o errore di completamento Windows Sysprep.
- Ulteriori informazioni sulla Panoramica di Sysprep.
- Informazioni sul Supporto Sysprep per i ruoli server.

Crea un'AMI utilizzando Windows Sysprep con EC2Launch v2

Quando crei un'immagine da un'istanza con l'agente EC2Launch v2 installato, EC2Launch v2 esegue specifiche attività durante la preparazione dell'immagine. Ciò include l'uso di Windows Sysprep. Per ulteriori informazioni, consulta the section called "Fasi di Windows Sysprep".

Indice

- Azioni di Windows Sysprep
- Dopo Sysprep
- Eseguire Windows Sysprep con EC2Launch v2

Azioni di Windows Sysprep

Windows Sysprep ed EC2Launch v2 eseguono le seguenti operazioni durante la preparazione di un'immagine.

1. Quando scegli Shutdown with Sysprep (Arresta con Sysprep) nella finestra di dialogo EC2Launch Service Properties (Proprietà servizio EC2), il sistema esegue il comando `ec2launch sysprep`.
2. EC2Launch v2 modifica il contenuto del file `unattend.xml` leggendo il valore del Registro di sistema in `HKEY_USERS\.DEFAULT\Control Panel\International\LocaleName`. Il file si trova nella directory seguente: `C:\ProgramData\Amazon\EC2Launch\sysprep`.
3. Il sistema esegue il comando `BeforeSysprep.cmd`. Tale comando crea una chiave di registro come indicato di seguito:

   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f

   La chiave di registro disattiva le connessioni RDP fino a che non vengono riattivate. La disattivazione delle connessioni RDP è una misura di sicurezza necessaria in quanto, nella prima sessione di avvio dopo l'esecuzione di Windows Sysprep, RDP consente le connessioni per un breve periodo di tempo in cui la password dell'Amministratore è vuota.
4. Il servizio EC2Launch v2 chiama Windows Sysprep attraverso l'esecuzione dei comandi seguenti:

   sysprep.exe /oobe /generalize /shutdown /unattend: "C:\ProgramData\Amazon\EC2Launch \sysprep\unattend.xml"

Fase di generalizzazione

- EC2Launch v2 rimuove le informazioni e le configurazioni specifiche dell'immagine, quali il nome del computer e l'SID. Se l'istanza è un membro di un dominio, essa viene rimossa dal dominio. Il file di risposta `unattend.xml` include le impostazioni seguenti che riguardano questa fase:
  - PersistAllDeviceInstalls: questa impostazione impedisce al programma di installazione di Windows di rimuovere e riconfigurare i dispositivi, velocizzando il processo di preparazione delle immagini perché le AMI Amazon richiedono l'esecuzione di determinati driver e il rilevamento di tali driver richiederebbe tempo.
  - DoNotCleanUpNonPresentDevices: questa impostazione conserva le informazioni Plug and Play per i dispositivi attualmente non presenti.

- Windows Sysprep arresta l'SO quando si prepara alla creazione dell'AMI. Il sistema avvia una nuova istanza o avvia l'istanza originale.

Fase di specializzazione

Il sistema genera OS-specific requisiti, ad esempio il nome del computer e un SID. Il sistema esegue anche le azioni seguenti, in base alle configurazioni specificate nel file di risposta `unattend.xml`.

- CopyProfile: Windows Sysprep può essere configurato per eliminare tutti i profili utente, incluso il profilo Administrator integrato. Questa impostazione mantiene l'account Amministratore integrato cosicché qualsiasi personalizzazione effettuata su tale account venga trasferita alla nuova immagine. Il valore predefinito è `True`.

  CopyProfilesostituisce il profilo predefinito con il profilo di amministratore locale esistente. Tutti gli account connessi dopo l'esecuzione di Windows Sysprep riceveranno una copia del profilo e del suo contenuto al primo accesso.

  Se non si dispone di personalizzazioni specifiche del profilo utente che si desidera trasferire alla nuova immagine, modificare questa impostazione in `False`. Windows Sysprep rimuoverà tutti i profili utente, risparmiando tempo e spazio su disco.
- TimeZone: il fuso orario è impostato su Coordinate Universal Time (UTC) per impostazione predefinita.
- Synchronous command with order 1 (Comando sincrono con ordine 1): il sistema esegue il comando seguente che abilita l'account amministratore e specifica il requisito della password:

  ```
  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /
  PASSWORDREQ:YES
  ```
- Synchronous command with order 2 (Comando sincrono con ordine 2): il sistema codifica la password dell'amministratore. Questa misura di sicurezza è progettata per impedire che l'istanza sia accessibile dopo il completamento di Windows Sysprep se non hai configurato l'attività `setAdminAccount`.

  Il sistema esegue il seguente comando dalla directory locale degli agenti di lancio (`C:\Program Files\Amazon\EC2Launch\`).

  ```
  EC2Launch.exe internal randomize-password --username Administrator
  ```

- Per abilitare le connessioni desktop remote, il sistema imposta la chiave di registro `fDenyTSConnections` di Terminal Server su false.

Fase Configurazione guidata

1. Il sistema specifica le seguenti configurazioni utilizzando il file di risposta di EC2Launch v2:
   - `<InputLocale>en-US</InputLocale>`
   - `<SystemLocale>en-US</SystemLocale>`
   - `<UILanguage>en-US</UILanguage>`
   - `<UserLocale>en-US</UserLocale>`
   - `<HideEULAPage>true</HideEULAPage>`
   - `<HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>`
   - `<ProtectYourPC>3</ProtectYourPC>`
   - `<BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>`
   - `<TimeZone>UTC</TimeZone>`
   - `<RegisteredOrganization>Amazon.com</RegisteredOrganization>`
   - `<RegisteredOwner>EC2</RegisteredOwner>`

   > **Note**
   >
   > Durante le fasi di generalizzazione e di specializzazione, EC2Launch v2 monitora lo stato del SO. Se EC2Launch v2 rileva che il SO si trova in una fase di Sysprep, pubblica il messaggio seguente al log di sistema:
   > Windows è in fase di configurazione. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Il sistema esegue EC2Launch v2.

Dopo Sysprep

Al termine di Windows Sysprep, EC2Launch v2 invia il seguente messaggio all'output della console:

```
Windows sysprep configuration complete.
```

Quindi EC2Launch v2 effettua le seguenti operazioni:

1. Legge il contenuto del file `agent-config.yml` ed esegue le attività configurate.
2. Esegue tutte le attività della fase `preReady`.
3. Al termine, invia un messaggio `Windows is ready` ai log di sistema dell'istanza.
4. Esegue tutte le attività della fase `PostReady`.

Per ulteriori informazioni su EC2Launch v2, consulta Utilizza l'agente EC2Launch v2 per eseguire attività durante l'avvio dell'istanza EC2 Windows.

Eseguire Windows Sysprep con EC2Launch v2

Utilizza la procedura seguente per creare un'AMI standardizzata utilizzando Windows Sysprep con EC2Launch v2.

1. Nella console Amazon EC2 individuare un'AMI che si desidera duplicare.
2. Avviare l'istanza Windows e connettersi a essa.
3. Personalizza impostazioni
    a. Dal menu Start di Windows, cerca e scegli le impostazioni di Amazon EC2Launch. Per ulteriori informazioni sulle opzioni e sulle impostazioni della finestra di dialogo Amazon EC2Launch settings (Impostazioni di Amazon EC2Launch), consulta Configurare le impostazioni di EC2Launch v2 per le istanze Windows.
    b. Se hai apportato modifiche, seleziona Salva prima di spegnere il computer.
4. Scegli Arresto con Sysprep o Arresto senza Sysprep.

Quando ti viene chiesto di confermare che desideri eseguire Windows Sysprep e chiudere l'istanza, scegli Sì. EC2Launch v2 esegue Windows Sysprep. Quindi verrai disconnesso dall'istanza e l'istanza verrà arrestata. Se si controlla la pagina Instances (Istanze) nella console Amazon EC2, lo stato dell'istanza cambia da `Running` a `Stopping` a `Stopped`. A questo punto, è opportuno creare un'AMI da questa istanza.

È possibile richiamare manualmente lo strumento Windows Sysprep dalla riga di comando con il comando seguente:

```
"%programfiles%\amazon\ec2launch\ec2launch.exe" sysprep --shutdown=true
```

Crea un'AMI utilizzando Windows Sysprep con EC2Launch

Quando crei un'immagine da un'istanza con l'agente EC2Launch installato, EC2Launch esegue specifiche attività durante la preparazione dell'immagine. Ciò include l'uso di Windows Sysprep. Per ulteriori informazioni, consulta the section called "Fasi di Windows Sysprep".

EC2Launch offre un file di risposta predefinito e dei file batch per Windows Sysprep che automatizzano e proteggono il processo di preparazione delle immagini sull'AMI. La modifica di tali file è facoltativa. Per impostazione predefinita, questi file si trovano nella directory seguente: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.

> **Important**
>
> Non si deve utilizzare Windows Sysprep per creare il backup di un'istanza. Windows Sysprep rimuove le informazioni specifiche di sistema. La rimozione di tali informazioni può avere conseguenze indesiderate sul backup di un'istanza.

Indice

- File batch e di risposta EC2Launch per Windows Sysprep
- Eseguire Windows Sysprep con EC2Launch
- Aggiorna i metadata/KMS percorsi per Server 2016 e versioni successive quando si avvia un'AMI personalizzata

File batch e di risposta EC2Launch per Windows Sysprep

Il file di risposta e i file batch di EC2Launch per Windows Sysprep includono quanto segue:

`Unattend.xml`

Si tratta del file di risposta predefinito. Se esegui `SysprepInstance.ps1` o scegli ShutdownWithSysprep nell'interfaccia utente, il sistema legge l'impostazione da questo file.

`BeforeSysprep.cmd`

Personalizzare questo file batch per eseguire i comandi prima che EC2Launch esegua Windows Sysprep.

`SysprepSpecialize.cmd`

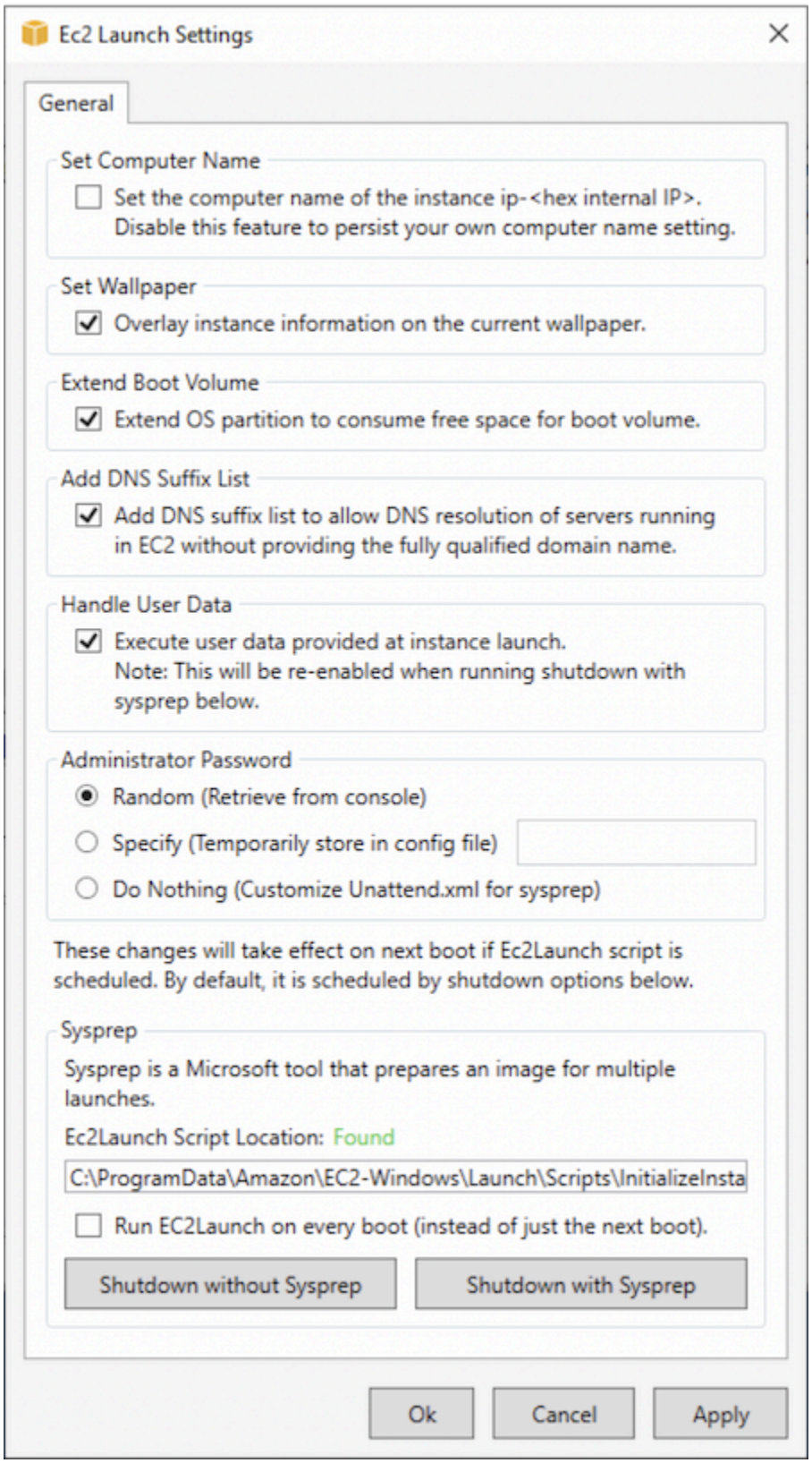
Personalizzare questo file batch per eseguire i comandi durante la fase di specializzazione di Windows Sysprep.

Eseguire Windows Sysprep con EC2Launch

Durante l'installazione completa di Windows Server 2016 o versione successiva (con un'esperienza desktop), è possibile eseguire Windows Sysprep con EC2Launch manualmente o utilizzando l'applicazione EC2 Launch Settings (Impostazioni di avvio EC2) .

Per eseguire Windows Sysprep tramite l'applicazione EC2Launch Settings

1. Nella console Amazon EC2, identificare o creare un'AMI di Windows Server 2016 o versione successiva.
2. Avviare un'istanza Windows dall'AMI.
3. Collegarsi all'istanza Windows e personalizzarla.
4. Cerca ed esegui l'EC2LaunchSettingsapplicazione. Per impostazione predefinita, si trova nella directory seguente: `C:\ProgramData\Amazon\EC2-Windows\Launch\Settings`.



5. Selezionare o deselezionare le opzioni in base alle esigenze. Tali impostazioni vengono memorizzate nel file `LaunchConfig.json`.

6. Per Administrator Password (Password amministratore), eseguire una delle seguenti operazioni:

   - Scegliere Random (Casuale). EC2Launch genera una password e la crittografa utilizzando la chiave dell'utente. Il sistema disattiva questa impostazione dopo l'avvio dell'istanza in modo che questa password rimanga se l'istanza viene riavviata o arrestata e avviata.
   - Scegliere Specify (Specifica) e digitare una password che soddisfi i requisiti di sistema. La password viene memorizzata in `LaunchConfig.json` come testo non crittografato e viene cancellata dopo che Windows Sysprep ha impostato la password amministratore. Se si esegue l'arresto in questo momento, la password viene impostata immediatamente. EC2Launch crittografa la password utilizzando la chiave dell'utente.
   - Scegli DoNothing e specifica una password nel `unattend.xml` file. Se non si indica una password in `unattend.xml`, l'account amministratore viene disattivato.
7. Selezionare Shutdown with Sysprep (Arresta con Sysprep).

Per eseguire Windows Sysprep manualmente tramite EC2Launch

1. Nella console Amazon EC2 identificare o creare un'AMI di Windows Server 2016 o versione successiva, edizione Datacenter, che si desidera duplicare.
2. Avviare l'istanza Windows e connettersi a essa.
3. Personalizzare l'istanza.
4. Specificare le impostazioni nel file `LaunchConfig.json`. Per impostazione predefinita, questo file si trova nella directory `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

   Per `adminPasswordType`, indicare uno dei valori seguenti:

   `Random`

   EC2Launch genera una password e la crittografa utilizzando la chiave dell'utente. Il sistema disattiva questa impostazione dopo l'avvio dell'istanza in modo che questa password rimanga se l'istanza viene riavviata o arrestata e avviata.

   `Specify`

   EC2Launch utilizza la password specificata in `adminPassword`. Se la password non soddisfa i requisiti di sistema, EC2Launch genera invece una password casuale. La password viene memorizzata in `LaunchConfig.json` come testo non crittografato e viene cancellata dopo che Windows Sysprep ha impostato la password amministratore. EC2Launch crittografa la password utilizzando la chiave dell'utente.

`DoNothing`

EC2Launch utilizza la password specificata nel file `unattend.xml`. Se non si indica una password in `unattend.xml`, l'account amministratore viene disattivato.

5. (Facoltativo) Specificare le impostazioni nel file `unattend.xml` e in altri file di configurazione. Se si prevede di partecipare all'installazione, non è necessario apportare modifiche a questi file. Per impostazione predefinita, i file si trovano nella directory seguente: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.
6. In Windows PowerShell, esegui `./InitializeInstance.ps1 -Schedule`. Per impostazione predefinita, lo script si trova nella directory seguente: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`. Lo script programma l'istanza da inizializzare durante l'avvio seguente. Bisogna eseguire questo script prima di eseguire lo script `SysprepInstance.ps1` durante la fase successiva.
7. In Windows PowerShell, esegui `./SysprepInstance.ps1`. Per impostazione predefinita, lo script si trova nella directory seguente: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`.

Si verrà disconnessi dall'istanza e l'istanza verrà arrestata. Se si controlla la pagina Instances (Istanze) nella console Amazon EC2, lo stato dell'istanza cambia da `Running` a `Stopping`, quindi in `Stopped`. A questo punto è sicuro creare un'AMI da questa istanza.

Aggiorna i metadata/KMS percorsi per Server 2016 e versioni successive quando si avvia un'AMI personalizzata

Per aggiornare le metadata/KMS route per Server 2016 e versioni successive all'avvio di un'AMI personalizzata, esegui una delle seguenti operazioni:

- Esegui la EC2LaunchSettings GUI (C:\\ AmazonProgramData\\ LaunchEC2-Windows\ Settings \Ec2LaunchSettings.exe) e seleziona l'opzione per chiudere con Windows Sysprep.
- Esegui EC2LaunchSettings e chiudi senza Windows Sysprep prima di creare l'AMI. Questo fa in modo che le attività di inizializzazione dell'avvio di EC2 vengano eseguite all'avvio successivo che imposta i routing in base alla sottorete per l'instanza.
- Riprogramma manualmente le attività di inizializzazione di EC2 Launch prima di creare un'AMI da. PowerShell

> **Important**
>
> Prendere nota del comportamento predefinito di reimpostazione della password prima di riprogrammare le attività.

- Per aggiornare le route su un'istanza in esecuzione in cui si verifica l'attivazione di Windows o la comunicazione con errori dei metadati dell'istanza, vedere "Impossibile attivare Windows".

Crea un'AMI utilizzando Windows Sysprep con EC2Config

Quando crei un'immagine da un'istanza con il servizio EC2Config installato, EC2Config esegue specifiche attività durante la preparazione dell'immagine. Ciò include l'uso di Windows Sysprep. Per ulteriori informazioni, consulta the section called "Fasi di Windows Sysprep".

Indice

- Azioni di Windows Sysprep
- Dopo Sysprep
- Eseguire Windows Sysprep con il servizio EC2Config

Azioni di Windows Sysprep

Durante la preparazione di un'immagine, Windows Sysprep e il servizio EC2Config eseguono le azioni seguenti.

1. Quando si sceglie Arresta con Sysprep nella finestra di dialogo Proprietà del servizio EC2, il sistema esegue il comando ec2config.exe –sysprep.
2. Il servizio EC2Config legge il contenuto del file `BundleConfig.xml`. Per impostazione predefinita, questo file si trova nella directory seguente: `C:\Program Files\Amazon \Ec2ConfigService\Settings`.

   Il file `BundleConfig.xml` include le seguenti impostazioni. È possibile modificare tali impostazioni:

   - AutoSysprep: indica se utilizzare Windows Sysprep automaticamente. Non si deve modificare tale valore se Windows Sysprep è in esecuzione dalla finestra di dialogo EC2 Service Properties (Proprietà servizio EC2). Il valore predefinito è `No`.

- SetRDPCertificate: imposta un certificato autofirmato per il server Remote Desktop. Questo consente di utilizzare il Remote Desktop Protocol (RDP) in modo sicuro per connettersi all'istanza. Modifica il valore in `Yes` se le nuove istanze devono utilizzare un certificato. Questa impostazione non si utilizza con le istanze di Windows Server 2012 in quanto tali sistemi operativi sono in grado di generare i propri certificati. Il valore predefinito è `No`.
- SetPasswordAfterSysprep: imposta una password casuale su un'istanza appena avviata, la crittografa con la chiave di avvio dell'utente e invia la password crittografata alla console. Modifica il valore in `No` se le nuove istanze non devono essere impostate su una password casuale crittografata. Il valore predefinito è `Yes`.
- PreSysprepRunCmd: la posizione del comando da eseguire. Per impostazione predefinita il comando si trova nella seguente directory: `C:\Program Files\Amazon\Ec2ConfigService\Scripts\BeforeSysprep.cmd`

3. Il sistema esegue `BeforeSysprep.cmd`. Tale comando crea una chiave di registro come indicato di seguito:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
 fDenyTSConnections /t REG_DWORD /d 1 /f
```

   La chiave di registro disattiva le connessioni RDP fino a che non vengono riattivate. La disattivazione delle connessioni RDP è una misura di sicurezza necessaria in quanto, nella prima sessione di avvio dopo l'esecuzione di Windows Sysprep, RDP consente le connessioni per un breve periodo di tempo in cui la password dell'Amministratore è vuota.

4. Il servizio EC2Config chiama Windows Sysprep attraverso l'esecuzione dei comandi seguenti:

```
sysprep.exe /unattend: "C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml" /
oobe /generalize /shutdown
```

Fase di generalizzazione

- Lo strumento rimuove le informazioni e le configurazioni specifiche dell'immagine, quali il nome del computer e l'SID. Se l'istanza è un membro di un dominio, essa viene rimossa dal dominio. Il file di risposta `sysprep2008.xml` include le impostazioni seguenti che riguardano questa fase:
  - PersistAllDeviceInstalls: questa impostazione impedisce al programma di installazione di Windows di rimuovere e riconfigurare i dispositivi, velocizzando il processo di preparazione

delle immagini perché le AMI Amazon richiedono l'esecuzione di determinati driver e il loro rilevamento richiederebbe del tempo.

- DoNotCleanUpNonPresentDevices: questa impostazione conserva le informazioni Plug and Play per i dispositivi attualmente non presenti.

- Windows Sysprep arresta l'SO quando si prepara alla creazione dell'AMI. Il sistema avvia una nuova istanza o avvia l'istanza originale.

Fase di specializzazione

Il sistema genera i requisiti specifici del SO, come un nome del computer e un SID. Il sistema esegue anche le azioni seguenti, in base alle configurazioni specificate nel file di risposta sysprep2008.xml.

- CopyProfile: Windows Sysprep può essere configurato per eliminare tutti i profili utente, incluso il profilo amministratore integrato. Questa impostazione mantiene l'account Amministratore integrato cosicché qualsiasi personalizzazione effettuata su tale account venga trasferita alla nuova immagine. Il valore predefinito è True.

  CopyProfilesostituisce il profilo predefinito con il profilo di amministratore locale esistente. Tutti gli account connessi dopo l'esecuzione di Windows Sysprep riceveranno una copia di tale profilo e del suo contenuto al primo accesso.

  Se non si dispone di personalizzazioni specifiche del profilo utente che si desidera trasferire alla nuova immagine, modificare questa impostazione in False. Windows Sysprep rimuoverà tutti i profili utente, risparmiando tempo e spazio su disco.
- TimeZone: il fuso orario è impostato su Coordinate Universal Time (UTC) per impostazione predefinita.
- Synchronous command with order 1 (Comando sincrono con ordine 1): il sistema esegue il comando seguente che abilita l'account amministratore e specifica il requisito della password.

  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER / PASSWORDREQ:YES
- Synchronous command with order 2 (Comando sincrono con ordine 2): il sistema codifica la password dell'amministratore. Questa misura di sicurezza è progettata per impedire che l'istanza sia accessibile dopo il completamento di Windows Sysprep se non è stata attivata l'impostazione ec2setpassword.

  C:\Program Files\ Amazon\Ec2ConfigService\ ScramblePassword.exe "-u Administrator

- Synchronous command with order 3 (Comando sincrono con ordine 3): il sistema esegue il comando seguente:

  C:\Program Files\ Amazon\\ Ec2ConfigService Scripts\ SysprepSpecializePhase.cmd

  Questo comando aggiunge la seguente chiave di registro, che riattiva l'RDP:

  reg aggiungi «HKEY_LOCAL_MACHINE\ SYSTEM\\ ControlCurrentControlSet\ Terminal Server» /v fdenytsConnections /t REG_DWORD /d 0 /f

Fase Configurazione guidata

1. Con l'utilizzo del file di risposta del servizio EC2Config, il sistema specifica le configurazioni seguenti:
   - InputLocaleInputLocale< >it-US</ >
   - < SystemLocale >it-US</ SystemLocale >
   - <UILanguage>en-US</UILanguage>
   - < UserLocale >it-US</ UserLocale >
   - <HideEULAPage>true</HideEULAPage>
   - < HideWirelessSetupInOOBE >vero</ HideWirelessSetupInOOBE >
   - < NetworkLocation >Altro</ NetworkLocation >
   - < PC>3</ PC> ProtectYour ProtectYour
   - < BluetoothTaskbarIconEnabled >falso</ BluetoothTaskbarIconEnabled >
   - < TimeZone >UTC</ TimeZone >
   - <RegisteredOrganization>Amazon.com</RegisteredOrganization>
   - < RegisteredOwner >Amazon</ RegisteredOwner >

   > **Note**
   >
   > Durante le fasi di generalizzazione e di specializzazione, il servizio EC2Config monitora lo stato del SO. Se EC2Config rileva che il SO si trova in una fase di Sysprep, pubblica il messaggio seguente nel log di sistema:
   > EC2ConfigMonitorState: 0 Windows è in fase di configurazione.
   > SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Al termine della fase OOBE, il sistema esegue `SetupComplete.cmd` dal seguente percorso: `C:\Windows\Setup\Scripts\SetupComplete.cmd`. Nelle AMI pubbliche di Amazon, prima dell'aprile 2015 questo file era vuoto e non eseguiva nulla sull'immagine. Nelle AMI pubbliche datate dopo l'aprile 2015, il file include il seguente valore: call "C:\Program Files\Amazon \Ec2ConfigService\Scripts\PostSysprep.cmd".
3. Il sistema esegue `PostSysprep.cmd`, che esegue le seguenti operazioni:
   - Imposta la password Amministratore locale in modo che non scada. Se la password è scaduta, l'Amministratore potrebbe non essere in grado di effettuare l'accesso.
   - Imposta il nome della macchina MSSQLServer (se installata) in modo che sia sincronizzato con l'AMI.

Dopo Sysprep

Al termine di Windows Sysprep, i servizi EC2Config inviano il messaggio seguente all'uscita della console:

```
Windows sysprep configuration complete.
   Message: Sysprep Start
   Message: Sysprep End
```

Quindi EC2Config effettua le seguenti azioni:

1. Legge il contenuto del file config.xml ed elenca tutti i plug-in attivati.
2. Esegue tutti i plug-in "Prima che Windows sia pronto" contemporaneamente.
   - Ec2SetPassword
   - Ec2SetComputerName
   - Ec2InitializeDrives
   - Ec2EventLog
   - Ec2ConfigureRDP
   - Ec2OutputRDPCert
   - Ec2SetDriveLetter
   - Ec2WindowsActivate
   - Ec2DynamicBootVolumeSize
3. Al termine, invia un messaggio "Windows è pronto" ai log del sistema di istanza.
4. Esegue tutti i plug-in "Dopo che Windows è pronto" contemporaneamente.

- Registri Amazon CloudWatch
- UserData
- AWS Systems Manager (Gestore di sistemi)

Per ulteriori informazioni sui plug-in di Windows, consulta Utilizza il servizio EC2Config per eseguire attività durante l'avvio dell'istanza del sistema operativo Windows legacy EC2.

Eseguire Windows Sysprep con il servizio EC2Config

Per creare un'AMI standardizzata utilizzando Windows Sysprep e il servizio EC2Config, utilizzare la procedura seguente.

1. Nella console Amazon EC2 individuare o creare un'AMI che si desidera duplicare.
2. Avviare l'istanza Windows e connettersi a essa.
3. Personalizzarla.
4. Specificare le impostazioni di configurazione nel file di risposta del servizio EC2Config:

   ```
   C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml
   ```
5. Dal menu Start di Windows, scegli Tutti i programmi, quindi scegli EC2ConfigService Impostazioni.
6. Selezionare la scheda Image (Immagine) nella finestra di dialogo Ec2 Service Properties (Proprietà servizio Ec2). Per ulteriori informazioni sulle opzioni e sulle impostazioni nella finestra di dialogo Proprietà servizio Ec2, consultare Proprietà servizio Ec2.
7. Selezionare un'opzione per la password Amministratore, quindi scegliere Shutdown with Sysprep (Arresta con Sysprep) o Shutdown without Sysprep (Arresta senza Sysprep). EC2Config modifica i file delle impostazioni in base all'opzione della password selezionata.
   - Random (Casuale): EC2Config genera una password, la crittografa con la chiave dell'utente e mostra la password crittografata alla console. Questa impostazione si disattiva dopo il primo avvio, in modo che questa password persista se l'istanza viene riavviata o arrestata e avviata.
   - Specifica: la password viene memorizzata nel file di risposta Windows Sysprep in un modulo non crittografato (testo normale). Quando Windows Sysprep viene eseguito, imposta la password Amministratore. Se si esegue l'arresto in questo momento, la password viene impostata immediatamente. Quando il servizio viene avviato nuovamente, la password Amministratore viene rimossa. È importante ricordare la password, poiché non sarà più possibile recuperarla in seguito.

- Mantenere quella esistente: la password esistente dell'account Amministratore non cambia durante l'esecuzione di Windows Sysprep o il riavvio di EC2Config. È importante ricordare la password, poiché non sarà più possibile recuperarla in seguito.

8. Seleziona OK.

Quando ti viene chiesto di confermare che desideri eseguire Windows Sysprep e chiudere l'istanza, scegli Sì. EC2Config esegue Windows Sysprep. Successivamente, si verrà disconnessi dall'istanza e l'istanza verrà arrestata. Se si controlla la pagina Instances (Istanze) nella console Amazon EC2, lo stato dell'istanza cambia da `Running` a `Stopping` e infine in `Stopped`. A questo punto, è opportuno creare un'AMI da questa istanza.

È possibile richiamare manualmente lo strumento Windows Sysprep dalla riga di comando con il comando seguente:

```
"%programfiles%\amazon\ec2configservice\"ec2config.exe -sysprep""
```

> **Note**
>
> Le virgolette doppie nel comando non sono necessarie se la shell CMD è già nella directory C:\Program Files\ Amazon\\. EC2ConfigService

Tuttavia, è necessario controllare bene che le opzioni dei file XML specificate nella cartella `Ec2ConfigService\Settings` siano corrette; in caso contrario, potrebbe non essere possibile connettersi all'istanza. Per ulteriori informazioni sui file delle impostazioni, consultare File delle impostazioni di EC2Config. Per avere un esempio della configurazione e dell'esecuzione di Windows Sysprep dalla riga di comando, consulta `Ec2ConfigService\Scripts\InstallUpdates.ps1`.

Copiare un'AMI Amazon EC2

Quando ti serve una configurazione coerente delle istanze Amazon EC2 in più regioni, puoi utilizzare una singola Amazon Machine Image (AMI) come modello per avviare tutte le istanze. Tuttavia, le AMI sono Region-specific risorse: per avviare un'istanza in una regione specifica, l'AMI deve trovarsi in quella regione. Regione AWS Quindi, per utilizzare la stessa AMI in più regioni, è necessario copiarla dalla regione di origine a ciascuna regione di destinazione.

Il metodo utilizzato per copiare un'AMI dipende dal fatto che la copia avvenga tra regioni all'interno della stessa partizione o tra partizioni diverse:

- Cross-Region copia: copia le AMI tra le regioni all'interno della stessa partizione, ad esempio tra le regioni all'interno della partizione commerciale. Questo metodo di copia viene descritto in questo argomento.
- Cross-partition copia: copia le AMI da una partizione all'altra, ad esempio dalla partizione commerciale alla partizione. AWS GovCloud (US) Per informazioni su questo metodo, consulta Archiviazione e ripristino di un'AMI.
- Cross-account copia: crea una copia di un'AMI che un altro ha condiviso con la tua. Account AWS Account AWS Questo metodo di copia viene descritto in questo argomento.

Il tempo necessario per completare l'operazione per la copia delle AMI tra regioni e account diversi è stimato nel miglior modo possibile. Se hai bisogno di controllare i tempi di completamento, puoi specificare un intervallo di tempo compreso tra 15 minuti e 48 ore, assicurandoti che la tua AMI venga copiata entro il periodo di tempo richiesto. Per le operazioni di copia AMI basate sul tempo vengono applicati costi aggiuntivi. Per ulteriori informazioni, consulta le Time-based copie nella Amazon EBS User Guide.

Indice

- Considerazioni
- Costi
- Concedere le autorizzazioni per copiare le AMI Amazon EC2
- Copiare un'AMI
- Arrestare un'operazione di copia AMI in sospeso
- Come funziona la copia delle AMI Amazon EC2

Considerazioni

- Autorizzazioni per copiare le AMI – Si possono utilizzare le policy IAM per concedere o rifiutare agli utenti l'autorizzazione per copiare le AMI. A partire dal 28 ottobre 2024, puoi specificare le autorizzazioni a livello di risorsa per l'azione sull'AMI di origine. `CopyImage` Resource-level le autorizzazioni per la nuova AMI sono disponibili come in precedenza.
- Autorizzazioni di avvio e permessi del bucket Amazon S3: AWS non copia i permessi di avvio o i permessi del bucket Amazon S3 dall'AMI di origine alla nuova AMI. Al completamento dell'operazione di copia, è possibile applicare i permessi di avvio e le autorizzazioni del bucket Amazon S3 alla nuova AMI.

- Tag – È possibile copiare solo i tag AMI definiti dall'utente che sono stati collegati all'AMI. I tag di sistema (con il prefisso `aws:`) e i tag definiti dall'utente che sono collegati da altri Account AWS non verranno copiati. Quando copi un'AMI, puoi allegare nuovi tag alla nuova AMI e ai suoi snapshot di supporto.
- Quote per le copie AMI basate sul tempo: una volta raggiunta la quota di throughput cumulativa delle copie degli snapshot, le successive richieste di copia dell'AMI basate sul tempo hanno esito negativo. Per ulteriori informazioni, consulta Quotas for time-based copies nella Guida per l'utente di Amazon EBS.
- Copie da origine a destinazione supportate: la posizione dell'AMI di origine determina se puoi copiarla e quali sono le destinazioni consentite per la nuova AMI.
  - Se l'AMI di origine si trova in una regione, puoi copiarla all'interno di quella regione, in un'altra regione, in un Outpost associato a quella regione o in una zona locale in quella regione.
  - Se l'AMI di origine si trova in una zona locale, puoi copiarla all'interno di tale zona locale, nella regione padre di tale zona locale o in altre zone locali con la stessa regione principale.
  - Se l'AMI di origine si trova su un Outpost, non puoi copiarla.
- Parametri CLI per origine e destinazione: quando usi la CLI, sono supportati i seguenti parametri per specificare la posizione di origine dell'AMI da copiare e la destinazione della nuova AMI. Tieni presente che l'operazione di copia deve essere avviata nella regione di destinazione; se ometti il `--region` parametro, la destinazione assume la regione predefinita configurata nelle tue impostazioni. AWS CLI

Da origine a destinazione	Parametro per l'origine	Parametro per la destinazione
Da regione a regione	`--source-region`	`--region`
Da regione a Outpost	`--source-region`	`--destination-outpost-arn` (l'ARN dell'Outpost)
Da regione a zona locale	`--source-region` Deve essere la regione principale della zona locale.	`--destination-availability-zone` (il nome della zona locale) o `--destination-availability-zone-id` (l'ID della zona locale)

Da origine a destinazione	Parametro per l'origine	Parametro per la destinazione
Da zona locale a regione	`--source-region` Deve essere la regione principale della zona locale. La zona locale di origine viene dedotta dalla posizione dell'ID dell'AMI di origine specificato.	`--region` Deve essere la regione principale della zona locale.
Da zona locale a zona locale	`--source-region` Deve essere la regione principale della zona locale. La zona locale di origine viene dedotta dalla posizione dell'ID dell'AMI di origine specificato.	`--destination-availability-zone` (il nome della zona locale) o `--destination-availability-zone-id` (l'ID della zona locale)

Costi

La copia di un'AMI non comporta alcun costo se non viene specificata alcun tempo di completamento. Tuttavia, per le operazioni di copia AMI basate sul tempo vengono applicati costi aggiuntivi. Per ulteriori informazioni, consulta le Time-based copie nella Amazon EBS User Guide.

Vengono applicati i costi standard di archiviazione e trasferimento dati. Se copi un' EBS-backed AMI, ti verranno addebitati costi per l'archiviazione di eventuali snapshot EBS aggiuntivi.

Concedere le autorizzazioni per copiare le AMI Amazon EC2

Per copiare una EBS-backed o Amazon S3-backed AMI, sono necessarie le seguenti autorizzazioni IAM:

- `ec2:CopyImage` – Per copiare l'AMI. Per le EBS-backed AMI, concede anche il permesso di copiare le istantanee di supporto dell'AMI.

- `ec2:CreateTags` – Per taggare l'AMI di destinazione. Per le EBS-backed AMI, concede inoltre il permesso di etichettare le istantanee di supporto dell'AMI di destinazione.

Se stai copiando un'AMI supportata da un archivio dell'istanza, sono necessarie le seguenti autorizzazioni IAM aggiuntive:

- `s3:CreateBucket` – Per creare il bucket S3 nella regione di destinazione per la nuova AMI
- `s3:PutBucketOwnershipControls`— Per abilitare gli ACL per il bucket S3 appena creato in modo che gli oggetti possano essere scritti con l'ACL predefinito `aws-exec-read` https://docs.aws.amazon.com/AmazonS3/latest/userguide/acl-overview.html#canned-acl
- `s3:GetBucketAcl`— Per leggere gli ACL per il bucket di origine
- `s3:ListAllMyBuckets` – Per trovare un bucket S3 esistente per le AMI nella regione di destinazione
- `s3:GetObject` – Per leggere gli oggetti nel bucket di origine
- `s3:PutObject` – Per scrivere gli oggetti nel bucket di destinazione
- `s3:PutObjectAcl` – Per scrivere le autorizzazioni per i nuovi oggetti nel bucket di destinazione

> **Note**
>
> A partire dal 28 ottobre 2024, è possibile specificare le autorizzazioni a livello di risorsa per l'azione sull'AMI di origine. `CopyImage` Resource-level le autorizzazioni per l'AMI di destinazione sono disponibili come in precedenza. Per ulteriori informazioni, consulta CopyImage la tabella sotto Azioni definite da Amazon EC2 nel Service Authorization Reference.

Esempio di politica IAM per la copia di un' EBS-backed AMI e l'etichettatura dell'AMI e delle istantanee di destinazione

La seguente politica di esempio ti concede il permesso di copiare qualsiasi EBS-backed AMI e di etichettare l'AMI di destinazione e le relative istantanee di supporto.

> **Note**
>
> A partire dal 28 ottobre 2024, è possibile specificare gli snapshot nell'elemento `Resource`. Per ulteriori informazioni, consulta la tabella CopyImage relativa alle azioni definite da Amazon EC2 nel Service Authorization Reference.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "PermissionToCopyAllImages",
        "Effect": "Allow",
        "Action": [
            "ec2:CopyImage",
            "ec2:CreateTags"
        ],
        "Resource": [
            "arn:aws:ec2:*::image/*",
            "arn:aws:ec2:*::snapshot/*"
        ]
    }]
}
```

Esempio di politica IAM per copiare un' EBS-backed AMI ma negare l'etichettatura delle nuove istantanee

L'autorizzazione `ec2:CopySnapshot` viene concessa automaticamente quando si ottiene l'autorizzazione `ec2:CopyImage`. L'autorizzazione a taggare i nuovi snapshot di supporto può essere negata esplicitamente, annullando l'effetto `Allow` dell'azione `ec2:CreateTags`.

La seguente politica di esempio ti concede il permesso di copiare qualsiasi EBS-backed AMI, ma ti impedisce di etichettare le nuove istantanee di supporto dell'AMI di destinazione.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*::image/*",
                "arn:aws:ec2:*::snapshot/*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:::snapshot/*"
        }
    ]
}
```

Esempio di politica IAM per copiare un'AMI Amazon S3-backed e etichettare l'AMI di destinazione

La seguente politica di esempio ti concede il permesso di copiare qualsiasi Amazon S3-backed AMI nel bucket di origine specificato nella regione specificata e di etichettare l'AMI di destinazione.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "PermissionToCopyAllImages",
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": [
```

```
                "arn:aws:s3:::*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:PutObjectAcl",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amis-for-111122223333-in-us-east-2-hash"
            ]
        }
    ]
}
```

Per trovare l'Amazon Resource Name (ARN) del bucket di origine AMI, apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/, nel pannello di navigazione scegli AMI e individua il nome del bucket nella colonna Source.

> **Note**
>
> L'`s3:CreateBucket`autorizzazione è necessaria solo la prima volta che copi un'Amazon S3-backed AMI in una singola regione. Successivamente, il bucket Amazon S3 già creato nella regione viene utilizzato per archiviare tutte le AMIs future copiate in quella regione.

Copiare un'AMI

Puoi copiare un'AMI che possiedi o un'AMI condivisa con te da un altro account. Per le combinazioni di origine e destinazione supportate, consulta Considerazioni.

Console

Per copiare un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dalla barra di navigazione della console, selezionare la regione che contiene l'AMI.
3. Nel pannello di navigazione, scegli AMI per visualizzare l'elenco di AMI disponibili nella regione.
4. Se non vedi l'AMI da copiare, scegli un filtro diverso. Puoi filtrare per AMI Di mia proprietà, Immagini private, Immagini pubbliche e Immagini disabilitate.
5. Seleziona l'AMI da copiare e poi scegli Azioni, Copia AMI.
6. Nella pagina Copy Amazon Machine Image (AMI), specifica le seguenti informazioni:

   a. AMI copy name (Nome copia AMI): un nome per la nuova AMI. Puoi includere le informazioni del sistema operativo nel nome perché Amazon EC2 non fornisce tali informazioni quando si visualizzano i dettagli sull'AMI.

   b. AMI copy description (Descrizione copia AMI): per impostazione predefinita, la descrizione include informazioni relative all'AMI di origine in modo da distinguere una copia dall'originale. È possibile modificare questa descrizione se necessario.

   c. Destination region (Regione di destinazione): la Regione in cui copiare l'AMI. Per ulteriori informazioni, consultare Cross-Region copiando e Cross-account copiando.

   d. Copia tag: seleziona questa casella di spunta per includere i tag AMI definiti dall'utente durante la copia dell'AMI. I tag di sistema (con il prefisso `aws:`) e i tag definiti dall'utente che sono collegati da altri Account AWS non verranno copiati.

   e. Time-based copia: puoi specificare se l'operazione di copia viene completata entro un periodo di tempo specifico o nel migliore dei modi, come segue:

      - Per completare la copia entro un determinato intervallo di tempo:
        - Seleziona Abilita copia in base al tempo.
        - Per Durata del completamento, inserisci il numero di minuti (in incrementi di 15 minuti) consentiti per l'operazione di copia. La durata del completamento si applica a tutti gli snapshot associati all'AMI.

          Per ulteriori informazioni, consulta le Time-based copie nella Amazon EBS User Guide.
      - Per completare la copia nel modo migliore possibile:

- Lascia l'opzione Abilita copia in base al tempo deselezionata.

f. (solo EBS-backed AMI) Crittografa le istantanee EBS della copia AMI: seleziona questa casella di controllo per crittografare le istantanee di destinazione o per crittografarle nuovamente utilizzando una chiave diversa. Se è abilitata la crittografia per impostazione predefinita, la casella di spunta Crittografa snapshot EBS della copia AMI è selezionata e non può essere deselezionata. Per ulteriori informazioni, consulta Crittografia e copia.

g. (solo EBS-backed AMI) Chiave KMS: la chiave KMS da utilizzare per crittografare le istantanee di destinazione.

h. Tag: puoi contrassegnare la nuova AMI e i nuovi snapshot con gli stessi tag, oppure contrassegnarli con tag diversi.

- Per taggare la nuova AMI e gli snapshot con gli stessi tag, scegli Taggare l'immagine e gli snapshot separatamente. Alla nuova AMI e a ogni snapshot creato vengono applicati gli stessi tag.
- Per contrassegnare la nuova AMI e i nuovi snapshot con tag diversi, scegli Taggare l'immagine e gli snapshot separatamente. Alla nuova AMI e a ogni snapshot creato vengono applicati tag diversi. Tuttavia, tutti i nuovi snapshot creati ricevono gli stessi tag; non è possibile contrassegnare ogni snapshot con un tag diverso.

Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore per il tag. Ripetere per ogni tag.

i. Quando è tutto pronto per copiare l'AMI, scegli Copia AMI.

Lo stato iniziale della nuova AMI è `Pending`. L'operazione di copia AMI è completata quando lo stato è `Available`.

AWS CLI

Per copiare un'AMI da una regione a un'altra

Utilizzare il comando copy-image. È necessario specificare la regione di origine e quella di destinazione, la prima tramite il parametro `--source-region`, Puoi specificare la regione di destinazione utilizzando il parametro `--region` (oppure ometti questo parametro per utilizzare la regione predefinita configurata nelle impostazioni della tua AWS CLI).

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
```

```
    --source-region us-west-2 \
    --name my-ami \
    --region us-east-1
```

Quando si crittografa uno snapshot di destinazione durante la copia dell'AMI è necessario specificare questi parametri aggiuntivi: `--encrypted` e `--kms-key-id`.

Per copiare un'AMI da una regione a una zona locale

Utilizzare il comando copy-image. Devi specificare l'origine e la destinazione. la prima tramite il parametro `--source-region`, Puoi specificare la zona locale di destinazione utilizzando il parametro `--destination-availability-zone` (ma puoi anche utilizzare `--destination-availability-zone-id`). Tieni presente che puoi copiare un'AMI solo da una regione a una zona locale solo all'interno della stessa regione.

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region cn-north-1 \
    --destination-availability-zone cn-north-1-pkx-1a \
    --name my-ami \
    --region cn-north-1
```

Per copiare un'AMI da una zona locale a una regione

Utilizzare il comando copy-image. Devi specificare l'origine e la destinazione. la prima tramite il parametro `--source-region`, Puoi specificare la regione di destinazione utilizzando il parametro `--region` (oppure ometti questo parametro per utilizzare la regione predefinita configurata nelle impostazioni della tua AWS CLI). La zona locale di origine viene dedotta dalla posizione dell'ID dell'AMI di origine specificato. Nota che puoi copiare un'AMI solo da una zona locale alla sua regione principale.

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region cn-north-1 \
    --name my-ami \
    --region cn-north-1
```

Per copiare un'AMI da una zona locale a un'altra

Utilizzare il comando copy-image. Devi specificare l'origine e la destinazione. Puoi specificare la regione di origine della zona locale utilizzando il parametro `--source-region`. Puoi specificare

la zona locale di destinazione utilizzando il parametro `--destination-availability-zone` (ma puoi anche utilizzare `--destination-availability-zone-id`). La zona locale di origine viene dedotta dalla posizione dell'ID dell'AMI di origine specificato. Specificate la regione principale della zona locale di destinazione utilizzando il `--region` parametro (oppure omettete questo parametro per assumere la regione predefinita configurata nelle impostazioni). AWS CLI

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region cn-north-1 \
    --destination-availability-zone cn-north-1-pkx-1a \
    --name my-ami \
    --region cn-north-1
```

PowerShell

Per copiare un'AMI da una regione a un'altra

Utilizza il cmdlet Copy-EC2Image. È necessario specificare la regione di origine e quella di destinazione, la prima tramite il parametro `-SourceRegion`, È possibile specificare la regione di destinazione utilizzando il `-Region` parametro o il Set-AWSDefaultRegion cmdlet.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion us-west-2 `
    -Name my-ami `
    -Region us-east-1
```

Quando si crittografa uno snapshot di destinazione durante la copia dell'AMI è necessario specificare questi parametri aggiuntivi: `-Encrypted` e `-KmsKeyId`.

Per copiare un'AMI da una regione a una zona locale

Utilizza il cmdlet Copy-EC2Image. Devi specificare l'origine e la destinazione. la prima tramite il parametro `-SourceRegion`, Puoi specificare la zona locale di destinazione utilizzando il parametro `-DestinationAvailabilityZone` (ma puoi anche utilizzare `-DestinationAvailabilityZoneId`). Tieni presente che puoi copiare un'AMI solo da una regione a una zona locale solo all'interno della stessa regione.

```
Copy-EC2Image `
```

```
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion cn-north-1 `
    -DestinationAvailabilityZone cn-north-1-pkx-1a `
    -Name my-ami `
    -Region cn-north-1
```

Per copiare un'AMI da una zona locale a una regione

Utilizza il cmdlet Copy-EC2Image. Devi specificare l'origine e la destinazione. la prima tramite il parametro `-SourceRegion`, È possibile specificare la regione di destinazione utilizzando il `-Region` parametro o il Set-AWSDefaultRegion cmdlet. La zona locale di origine viene dedotta dalla posizione dell'ID dell'AMI di origine specificato. Nota che puoi copiare un'AMI solo da una zona locale alla sua regione principale.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion cn-north-1 `
    -Name my-ami `
    -Region cn-north-1
```

Per copiare un'AMI da una zona locale a un'altra

Utilizza il cmdlet Copy-EC2Image. Devi specificare l'origine e la destinazione. Puoi specificare la regione di origine della zona locale utilizzando il parametro `-SourceRegion`. Puoi specificare la zona locale di destinazione utilizzando il parametro `-DestinationAvailabilityZone` (ma puoi anche utilizzare `-DestinationAvailabilityZoneId`). La zona locale di origine viene dedotta dalla posizione dell'ID dell'AMI di origine specificato. Si specifica la regione padre della zona locale di destinazione utilizzando il `-Region` parametro o il Set-AWSDefaultRegion cmdlet.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion cn-north-1 `
    -DestinationAvailabilityZone cn-north-1-pkx-1a `
    -Name my-ami `
    -Region cn-north-1
```

Arrestare un'operazione di copia AMI in sospeso

Puoi arrestare una copia di AMI in sospeso usando le seguenti procedure.

Console

Per arrestare un'operazione di copia di AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dalla barra di navigazione, selezionare la regione di destinazione dal selettore di regione.
3. Nel riquadro di navigazione scegliere AMIs (AMI).
4. Selezionare l'AMI di cui arrestare la copia, quindi scegliere Operazioni, Annulla registrazione AMI.
5. Quando viene richiesta la conferma, scegliere Deregister AMI (Annulla registrazione AMI).

AWS CLI

Per arrestare un'operazione di copia di AMI

Utilizza il comando deregister-image.

```
aws ec2 deregister-image --image-id ami-0abcdef1234567890
```

PowerShell

Per interrompere un'operazione di copia AMI utilizzando

Utilizza il cmdlet Unregister-EC2Image.

```
Unregister-EC2Image -ImageId ami-0abcdef1234567890
```

Come funziona la copia delle AMI Amazon EC2

La copia di un'AMI di origine determina la creazione di una nuova AMI identica ma distinta, indicata anche come AMI di destinazione. L'AMI di destinazione ha il proprio ID dell'AMI univoco. Puoi modificare o annullare la registrazione dell'AMI di origine senza alcun effetto sull'AMI di destinazione. È vero anche il contrario.

Con un' EBS-backed AMI, ciascuna delle relative istantanee di supporto viene copiata in un'istantanea di destinazione identica ma distinta. Se si copia un AMI in una nuova regione, gli snapshot saranno copie complete (non incrementali). Se si crittografano gli snapshot di backup

non crittografati o li si crittografa in una nuova chiave KMS, gli snapshot saranno copie complete (non incrementali). Operazioni di copia successive di un AMI restituiscono copie incrementali degli snapshot di backup.

Indice

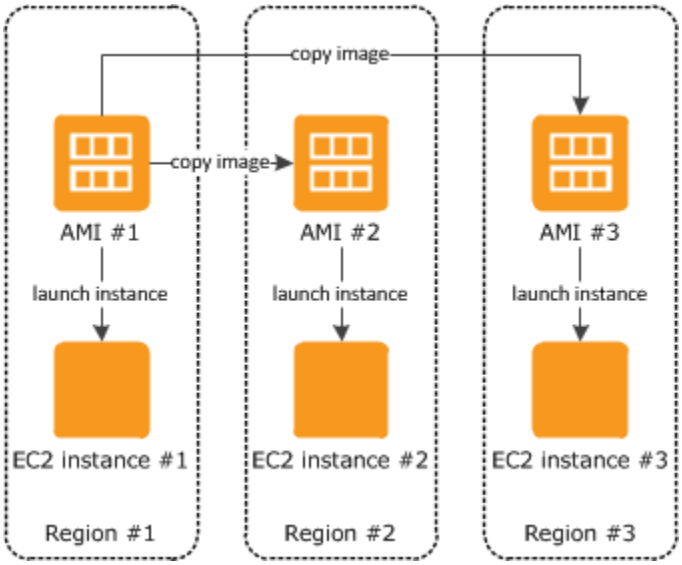
- Cross-Region copiando
- Cross-account copiando
- Time-based Operazioni di copia AMI
- Crittografia e copia

Cross-Region copiando

Copiare un'AMI tra regioni geograficamente diverse offre i seguenti vantaggi:

- Distribuzione globale coerente: la copia di un'AMI da una regione all'altra consente di avviare istanze coerenti in regioni diverse in base alla stessa AMI.
- Scalabilità: è possibile progettare e creare più facilmente applicazioni di livello mondiale che soddisfino le esigenze degli utenti, indipendentemente dalla loro posizione.
- Prestazioni: è possibile aumentare le prestazioni distribuendo l'applicazione e localizzandone i componenti critici nelle vicinanze degli utenti. È inoltre possibile sfruttare Region-specific le funzionalità, ad esempio i tipi di istanze o altri AWS servizi.
- Elevata disponibilità: progettare e distribuire applicazioni nelle regioni AWS consente di aumentare la disponibilità.

Il diagramma seguente mostra la relazione tra un'AMI di origine e due AMI copiate in regioni diverse, così come le istanze EC2 avviate da ciascuna. Quando avvii un'istanza da un'AMI, questa risiede nella stessa regione in cui risiede l'AMI. Se modifichi l'AMI di origine e desideri che tali modifiche si riflettano nelle AMIs delle regioni di destinazione, devi copiare nuovamente le AMI di origine nelle regioni di destinazione.



Quando copi per la prima volta un' S3-backed AMI Amazon in una regione, creiamo un bucket Amazon S3 per le AMI copiate in quella regione. Tutte le S3-backed AMI Amazon che copi in quella regione vengono archiviate in questo bucket. I nomi dei bucket hanno il seguente formato: amis-for- -in- -. *account region hash* Ad esempio: `amis-for-123456789012-in-us-east-2-yhjmxvp6`.

Prerequisito

Prima di copiare un'AMI devi assicurarti che il contenuto dell'AMI di origine sia aggiornato per supportare l'esecuzione in un'altra regione. Ad esempio è necessario aggiornare tutte le stringhe di connessione al database o i dati di configurazione dell'applicazione simili per individuare le risorse appropriate. Altrimenti, le istanze avviate dalla nuova AMI nella regione di destinazione potrebbero ancora utilizzare le risorse della regione di origine, il che può influire sulle prestazioni e sui costi.

Limitazioni

- Per le regioni di destinazione è previsto un limite di 300 operazioni di copia di AMI simultanee. Questo vale anche per le operazioni di copia delle AMI basate sul tempo.
- Non puoi copiare un'AMI paravirtuale (PV) in una regione che non supporta questo tipo di AMI. Per ulteriori informazioni, consulta Tipi di virtualizzazione.

Cross-account copiando

Se un'AMI di un'altra Account AWS è condivisa con la tua Account AWS, puoi copiare l'AMI condivisa. Questa operazione è nota con il nome di copia fra account. L'AMI che viene condivisa con

te è l'AMI di origine. Quando si copia l'AMI di origine, si crea una nuova AMI. La nuova AMI viene spesso definita AMI di destinazione.

Costi AMI

- Per un'AMI condivisa, l'archiviazione nella regione è a carico dell'account dell'AMI condivisa.
- Se copi un'AMI che viene condivisa con il tuo account, la proprietà dell'AMI di destinazione spetta al tuo account.
  - Al proprietario dell'AMI di origine vengono addebitati i costi di trasferimento standard di Amazon EBS o Amazon S3.
  - Ti viene addebitato il costo per l'archiviazione dell'AMI di destinazione nella regione di destinazione.

Autorizzazioni relative alle risorse

Per copiare un'AMI condivisa con te da un altro account, il proprietario dell'AMI di origine deve concedere le autorizzazioni di lettura per l'archiviazione che supporta l'AMI, non solo per l'AMI stessa. Lo storage è costituito dallo snapshot EBS associato (per un' EBS-backed AMI Amazon) o da un bucket S3 associato (per un'AMI Amazon). S3-backed Se l'AMI condivisa dispone di snapshot crittografati, il proprietario deve condividere la chiave o le chiavi. Per ulteriori informazioni sulla concessione di autorizzazioni per le risorse, per gli snapshot EBS, consulta Share an Amazon EBS snapshot with other Account AWS nella Guida per l'utente di Amazon EBS, mentre per i bucket S3 consulta Identity and access management for Amazon S3 nella Guida per l'utente di Amazon S3.

> **Note**
>
> I tag assegnati all'AMI di origine non vengono copiati tra account sull'AMI di destinazione.

Time-based Operazioni di copia AMI

Quando si avvia un'operazione di copia AMI basata sul tempo per un' EBS-backed AMI con una singola istantanea associata, si comporta allo stesso modo di una singola operazione di copia istantanea basata sul tempo e si applicano le stesse limitazioni di velocità effettiva.

Quando si avvia un'operazione di copia AMI basata sul tempo per un' EBS-backed AMI con più istantanee associate, si comporta allo stesso modo delle operazioni simultanee di copia di istantanee basate sul tempo e si applicano le stesse limitazioni di velocità effettiva. Ogni snapshot associato

genera una richiesta di copia distinta, ognuna delle quali contribuisce alla quota cumulativa di throughput di copie snapshot. La durata di completamento specificata si applica a ciascuno snapshot associato.

Per ulteriori informazioni, Time-based consulta le copie nella Amazon EBS User Guide.

Crittografia e copia

La tabella seguente mostra il supporto della crittografia per vari AMI-copying scenari. Sebbene sia possibile copiare uno snapshot non crittografato per produrne uno crittografato, non è possibile copiare uno snapshot crittografato per produrne uno non crittografato.

Scenario	Descrizione	Supportata
1	Da non crittografato a non crittografato	Sì
2	Da crittografato a crittografato	Sì
3	Da non crittografato a crittografato	Sì
4	Da crittografato a non crittografato	No

> **Note**
>
> La crittografia durante l'`CopyImage`azione si applica solo alle EBS-backed AMI Amazon. Poiché un' S3-backed AMI Amazon non utilizza istantanee, non puoi utilizzare la copia per modificarne lo stato di crittografia.

Quando si copia un'AMI senza specificare i parametri di crittografia, per impostazione predefinita, lo snapshot di supporto viene copiato con il proprio stato di crittografia originario. Pertanto, se l'AMI di origine è supportata da uno snapshot non crittografato, anche lo snapshot di destinazione risultante non sarà crittografato. Allo stesso modo, se l'istantanea dell'AMI di origine è crittografata, anche l'istantanea di destinazione risultante verrà crittografata con la stessa chiave. AWS KMS Per le AMI supportate da più snapshot, ciascuno snapshot di destinazione conserva lo stato di crittografia del suo snapshot di origine corrispondente.

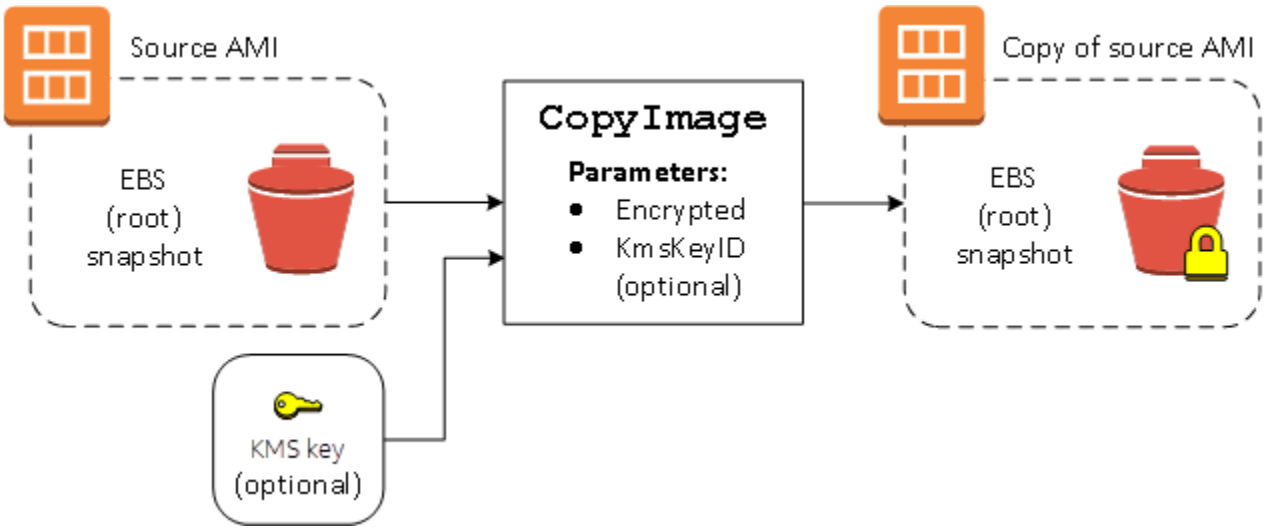
Per modificare lo stato di crittografia degli snapshot di supporto di destinazione durante una copia di AMI, puoi specificare i parametri di crittografia. L'esempio seguente mostra un caso non predefinito,

in cui i parametri di crittografia sono specificati con l'operazione `CopyImage` per modificare lo stato di crittografia dell'AMI di destinazione.

Copia di un'AMI di origine non crittografata in un'AMI di destinazione crittografata

In questo scenario, un'AMI supportata da uno snapshot di root non crittografato viene copiato in un'AMI con uno snapshot di root crittografato. L'operazione `CopyImage` viene richiamata con due parametri di crittografia, inclusa una chiave gestita dal cliente. Di conseguenza, lo stato di crittografia dello snapshot root cambia, in modo che l'AMI di destinazione sia supportata da uno snapshot root contenente gli stessi dati dello snapshot di origine, ma crittografato utilizzando la chiave specificata. Ti verranno addebitati costi di archiviazione per gli snapshot in entrambe le AMI, nonché addebiti per tutte le istanze avviate da entrambe le AMI.

> **Note**
>
> L'abilitazione della crittografia per impostazione predefinita ha lo stesso effetto dell'impostazione del parametro `Encrypted` a `true` per tutti gli snapshot nell'AMI.



L'impostazione del parametro `Encrypted` consente di crittografare il singolo snapshot per questa istanza. Se non specifichi il parametro `KmsKeyId`, per crittografare la copia snapshot viene utilizzata la chiave gestita dal cliente di default.

Per ulteriori informazioni sulla copia di AMIs con snapshot crittografati, consulta Usa la crittografia con le EBS-backed AMI.

Archiviazione e ripristino di un'AMI utilizzando S3

Puoi archiviare un'Amazon Machine Image (AMI) in un bucket Amazon S3, copiare l'AMI in un altro bucket S3 e quindi ripristinarla dal bucket S3. Archiviando e ripristinando un'AMI utilizzando i bucket S3, è possibile copiare le AMI da una AWS partizione all'altra, ad esempio dalla partizione commerciale principale alla partizione. AWS GovCloud (US) Potrai inoltre creare copie di archiviazione delle AMI memorizzandole in un bucket S3.

Le API supportate per la memorizzazione e il ripristino di un'AMI utilizzando S3 sono `CreateStoreImageTask`, `DescribeStoreImageTasks` e `CreateRestoreImageTask`.

`CopyImage`è l'API consigliata da utilizzare per copiare le AMI all'interno di una partizione. AWS Tuttavia, `CopyImage` non potrà copiare un'AMI in un'altra partizione.

Per informazioni sulle AWS partizioni, consulta *`partition`* la pagina Amazon Resource Names (ARNs) nella IAM User Guide.

> **Warning**
>
> Assicurati di rispettare tutte le leggi e i requisiti aziendali applicabili quando sposti dati tra AWS partizioni o AWS regioni, inclusi, a titolo esemplificativo, le normative governative applicabili e i requisiti di residenza dei dati.

Indice

- Casi d'uso
- Limitazioni
- Costi
- Come funzionano l'archiviazione e il ripristino delle AMI
- Crea un'attività di archiviazione delle immagini

Casi d'uso

Utilizza le API di archiviazione e ripristino per effettuare le seguenti operazioni:

- Copia un AMI tra AWS partizioni
- Creazione di copie di archiviazione delle AMI

Copia un AMI tra AWS partizioni

Archiviando e ripristinando un'AMI utilizzando i bucket S3, è possibile copiare un'AMI da una AWS partizione all'altra o da una regione all'altra. AWS Nell'esempio seguente, si copia un'AMI dalla partizione commerciale principale alla AWS GovCloud (US) partizione, in particolare da una regione all'altra. `us-east-2` `us-gov-east-1`

Per copiare un'AMI da una partizione a un'altra, completa la seguente procedura:

- Archiviare l'AMI in un bucket S3 nella regione corrente utilizzando `CreateStoreImageTask`. In questo esempio, il bucket S3 si trova in `us-east-2`.
- Monitorare lo stato di avanzamento dell'attività di archiviazione utilizzando `DescribeStoreImageTasks`. L'oggetto diventa visibile nel bucket S3 una volta completata l'attività.
- Copiare l'oggetto AMI archiviato in un bucket S3 nella partizione di destinazione utilizzando una procedura a scelta. In questo esempio, l'S3 Bucket si trova in `us-gov-east-1`.

  > **Note**
  >
  > Poiché sono necessarie AWS credenziali diverse per ogni partizione, non è possibile copiare un oggetto S3 direttamente da una partizione all'altra. Il processo per copiare un oggetto S3 tra le partizioni non rientra nell'ambito di questa documentazione. Forniamo i seguenti processi di copia come esempi, ma è necessario utilizzare il processo di copia che soddisfa i requisiti di sicurezza.
  >
  > - Per copiare un'AMI tra le partizioni, il processo di copia potrebbe essere semplice come il seguente: scarica l'oggetto dal bucket di origine su un host intermedio (ad esempio, un'istanza EC2 o un laptop), quindi carica l'oggetto dall'host intermedio al bucket di destinazione. Per ogni fase del processo, utilizza le AWS credenziali per la partizione.
  > - Per un utilizzo più duraturo, è consigliabile sviluppare un'applicazione che gestisca le copie, potenzialmente utilizzando download e caricamenti multipart S3.

- Ripristinare l'AMI dal bucket S3 nella partizione di destinazione utilizzando `CreateRestoreImageTask`. In questo esempio, l'S3 Bucket si trova in `us-gov-east-1`.
- Monitorare l'avanzamento dell'attività di ripristino descrivendo l'AMI per verificare quando il relativo stato diventa disponibile. È inoltre possibile monitorare le percentuali di avanzamento degli snapshot che costituiscono l'AMI ripristinata descrivendo gli snapshot.

Creazione di copie di archiviazione delle AMI

È possibile creare copie di archiviazione delle AMI archiviandole in un bucket S3. L'AMI è incorporata in un singolo oggetto in S3 e tutti i metadati dell'AMI (escluse le informazioni di condivisione) vengono conservati come parte dell'AMI archiviata. I dati dell'AMI vengono compressi come parte del processo di archiviazione. Le AMI che contengono dati che possono essere facilmente compressi generano oggetti più piccoli in S3. Per ridurre i costi, è possibile utilizzare livelli di archiviazione S3 meno costosi. Per maggiori informazioni, consultare Classi di archiviazione di Amazon S3 e la pagina dei prezzi di Amazon S3.

Limitazioni

- Per archiviare un'AMI, Account AWS devi possedere l'AMI e le sue istantanee, oppure l'AMI e le sue istantanee devono essere condivise direttamente con il tuo account. Non è possibile archiviare un'AMI se è condivisa solo pubblicamente.
- Solo le EBS-backed AMI possono essere archiviate utilizzando queste API.
- Le AMI paravirtual (PV) non sono supportate.
- La dimensione di un'AMI (prima della compressione) che può essere archiviata è limitata a 5.000 GB.
- Quota sulle richieste di immagini archiviate: 1.200 GB di spazio di archiviazione (dati istantanei) in corso.
- Quota sulle richieste di ripristino delle immagini: 600 GB di lavori di ripristino (dati istantanei) in corso.
- Per la durata dell'attività di archiviazione, gli snapshot non devono essere eliminati e l'entità IAM che esegue l'archiviazione deve avere accesso agli snapshot, altrimenti il processo di archiviazione avrà esito negativo.
- Non è possibile creare più copie di un'AMI nello stesso bucket S3.
- Un'AMI archiviata in un bucket S3 non può essere ripristinata con il suo ID AMI originale. È possibile mitigare questo effetto utilizzando l'alias AMI.
- Attualmente le API di archiviazione e ripristino sono supportate solo utilizzando gli AWS SDK e l' AWS Command Line Interface API Amazon EC2. Non è possibile archiviare e ripristinare un'AMI utilizzando la console Amazon EC2.

Costi

Quando si memorizzano e si ripristinano le AMI utilizzando S3, vengono addebitati i servizi utilizzati dalle API di archiviazione e ripristino e per il trasferimento dei dati. Le API utilizzano S3 e l'API EBS Direct (utilizzata internamente da queste API per accedere ai dati delle snapshot). Per ulteriori dettagli, consulta Prezzi di Amazon S3 e Prezzi di Amazon EBS.

Come funzionano l'archiviazione e il ripristino delle AMI

Per memorizzare e ripristinare un'AMI utilizzando S3, utilizza le seguenti API:

- `CreateStoreImageTask`: memorizza l'AMI in un bucket S3
- `DescribeStoreImageTasks` –: fornisce lo stato di avanzamento dell'attività di archiviazione dell'AMI
- `CreateRestoreImageTask`: ripristina l'AMI da un bucket S3

Come funzionano le API

- CreateStoreImageTask
- DescribeStoreImageTasks
- CreateRestoreImageTask
- Percorsi di file

CreateStoreImageTask

L'API `CreateStoreImageTask` archivia un'AMI come singolo oggetto in un bucket S3.

L'API crea un'attività che legge tutti i dati dall'AMI e dai relativi snapshot e quindi utilizza un caricamento in più parti S3 per archiviare i dati in un oggetto S3. L'API prende tutti i componenti dell'AMI, inclusa la maggior parte dei metadati non Region-specific AMI e tutte le istantanee EBS contenute nell'AMI, e li raggruppa in un unico oggetto in S3. I dati vengono compressi come parte del processo di caricamento in modo d ridurre la quantità di spazio utilizzato in S3, quindi l'oggetto in S3 potrebbe essere inferiore alla somma delle dimensioni degli snapshot nell'AMI.

Se sono presenti tag di AMI e snapshot visibili all'account che chiama questa API, questi saranno conservati.

L'oggetto in S3 ha lo stesso ID dell'AMI, ma con estensione `.bin`. I seguenti dati vengono memorizzati anche come tag di metadati S3 sull'oggetto S3: nome AMI, descrizione AMI, data di registrazione AMI, account proprietario AMI e un timestamp per l'operazione di archiviazione.

Il tempo necessario per completare l'attività dipende dalle dimensioni dell'AMI. Dipende anche dal numero delle altre attività in corso perché le attività vengono messe in coda. È possibile tenere traccia dello stato di avanzamento dell'attività chiamando l'API `DescribeStoreImageTasks`.

La somma delle dimensioni di tutte le AMI in corso è limitata a 1.200 GB di dati di snapshot EBS per account. Un'ulteriore creazione di attività verrà rifiutata fino a quando le attività in corso non saranno inferiori al limite. Ad esempio, se un'AMI con 200 GB di dati snapshot e un'altra AMI con 400 GB di dati snapshot sono in fase di archiviazione, verrà accettata un'altra richiesta, poiché il totale in corso è 600 GB, che è inferiore al limite. Tuttavia, se è attualmente archiviata una singola AMI con 1.200 GB di dati snapshot, le altre attività vengono rifiutate fino al completamento dell'attività.

DescribeStoreImageTasks

L'API `DescribeStoreImageTasks` descrive l'avanzamento delle attività di archiviazione dell'AMI. È possibile descrivere le attività per le AMI specificate. Se non si specificano le AMI, si ottiene un elenco impaginato di tutte le attività dell'immagine archivio che sono state elaborate negli ultimi 31 giorni.

Per ogni attività dell'AMI, la risposta indica se l'attività è `InProgress`, `Completed` o `Failed`. Per le attività `InProgress`, la risposta mostra uno stato di avanzamento in forma percentuale.

Le attività sono elencate in ordine cronologico inverso.

Al momento è possibile visualizzare solo le attività del mese precedente.

CreateRestoreImageTask

L'API `CreateRestoreImageTask` avvia un'attività che ripristina un'AMI da un oggetto S3 creato in precedenza utilizzando una richiesta `CreateStoreImageTask`.

L'attività di ripristino può essere eseguita nella stessa regione o in una regione diversa in cui è stata eseguita l'attività di archiviazione.

Il bucket S3 da cui verrà ripristinato l'oggetto AMI deve trovarsi nella stessa regione in cui è richiesta l'attività di ripristino. L'AMI sarà ripristinata in questa regione.

L'AMI viene ripristinata con i relativi metadati, ad esempio il nome, la descrizione e i mapping dei dispositivi a blocchi corrispondenti ai valori dell'AMI archiviata. Il nome deve essere univoco per le

AMI nella regione per questo account. Se non si fornisce un nome, la nuova AMI avrà lo stesso nome dell'AMI originale. L'AMI ottiene un nuovo ID AMI che viene generato al momento del processo di ripristino.

Il tempo necessario per completare l'attività di ripristino dell'AMI dipende dalle dimensioni dell'AMI. Dipende anche dal numero delle altre attività in corso perché le attività vengono messe in coda. È possibile visualizzare l'avanzamento dell'attività descrivendo l'AMI (describe-images) o i relativi snapshot EBS (describe-snapshot). Se l'attività non riesce, l'AMI e gli snapshot passano allo stato non riuscito.

La somma delle dimensioni di tutte le AMI in corso è limitata a 600 GB (in base alla dimensione dopo il ripristino) di dati istantanei EBS per account. Un'ulteriore creazione di attività verrà rifiutata fino a quando le attività in corso non saranno inferiori al limite.

Percorsi di file

Puoi utilizzare i percorsi dei file durante l'archiviazione e il ripristino delle AMI, nel modo seguente:

- Quando si archivia un'AMI in S3, il percorso del file può essere aggiunto al nome del bucket. Internamente, il sistema separa il percorso dal nome del bucket e quindi aggiunge il percorso alla chiave oggetto generata per archiviare l'AMI. Il percorso completo di un oggetto è mostrato nella risposta di una chiamata API.
- Quando si ripristina l'AMI, poiché è disponibile un parametro della chiave oggetto, il percorso può essere aggiunto all'inizio del valore della chiave oggetto.

Esempio: nome del bucket con percorso del file aggiunto

Quando archivi l'AMI, specifica il percorso del file dopo il nome del bucket.

```
amzn-s3-demo-bucket/path1/path2
```

Di seguito è riportata la chiave oggetto risultante.

```
path1/path2/ami-0abcdef1234567890.bin
```

Quando ripristini l'AMI, devi specificare sia il nome del bucket che la chiave dell'oggetto. Per alcuni esempi, consulta the section called "Crea un'attività di archiviazione delle immagini".

Crea un'attività di archiviazione delle immagini

Quando archivi un'AMI in un bucket S3, viene creata un'attività di archiviazione dell'immagine. Puoi utilizzare l'attività di archiviazione dell'immagine per monitorare l'avanzamento e l'esito del processo.

Indice

- Protezione delle AMI
- Autorizzazioni per l'archiviazione e il ripristino di AMI utilizzando S3
- Crea un'attività di archiviazione delle immagini
- Crea un'attività di ripristino delle immagini

Protezione delle AMI

È importante assicurarsi che il bucket S3 sia configurato con un livello di sicurezza sufficiente per proteggere il contenuto dell'AMI e che la sicurezza venga mantenuta per tutto il tempo che gli oggetti AMI rimangono nel bucket. Se ciò non è possibile, è preferibile non utilizzare queste API. Assicurarsi che non sia consentito l'accesso pubblico al bucket S3. Consigliamo di abilitare la Server-side crittografia per i bucket S3 in cui vengono archiviate le AMI, anche se non è obbligatorio.

Per informazioni su come impostare le impostazioni di sicurezza appropriate per i bucket S3, consultare i seguenti argomenti sulla sicurezza:

- Blocco dell'accesso pubblico all'archiviazione Amazon S3
- Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3
- Quale policy sui bucket S3 posso utilizzare per rispettare la regola s3-bucket-ssl-requests-only? AWS Config
- Abilitazione della registrazione degli accessi al server Amazon S3

Quando gli snapshot AMI vengono copiati nell'oggetto S3, i dati vengono quindi copiati tramite connessioni TLS. È possibile archiviare le AMI con snapshot crittografati, ma gli snapshot vengono poi decrittografati come parte del processo di archiviazione.

Autorizzazioni per l'archiviazione e il ripristino di AMI utilizzando S3

Se le entità principali IAM archiviano o ripristinano le AMI utilizzando Amazon S3, devi concedere loro le autorizzazioni richieste.

La seguente policy di esempio include tutte le operazioni necessarie per consentire a un'entità IAM di eseguire le attività di archiviazione e ripristino.

Puoi anche creare policy IAM che consentono alle entità principali l'accesso solo a risorse specifiche. Per altri esempi di policy, consulta Gestione degli accessi per AWS le risorse nella IAM User Guide.

> **Note**
>
> Se gli snapshot che compongono l'AMI sono crittografati o se il tuo account è abilitato per la crittografia per impostazione predefinita, l'entità principale IAM deve disporre dell'autorizzazione per usare la chiave KMS.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:PutObjectTagging",
                "s3:AbortMultipartUpload",
                "ebs:CompleteSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:ListChangedBlocks",
                "ebs:ListSnapshotBlocks",
                "ebs:PutSnapshotBlock",
                "ebs:StartSnapshot",
                "ec2:CreateStoreImageTask",
                "ec2:DescribeStoreImageTasks",
                "ec2:CreateRestoreImageTask",
                "ec2:GetEbsEncryptionByDefault",
                "ec2:DescribeTags",
                "ec2:CreateTags"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Crea un'attività di archiviazione delle immagini

Per archiviare un'AMI in un bucket S3, inizia creando un'attività di archiviazione dell'immagine. Il tempo necessario per completare l'attività dipende dalle dimensioni dell'AMI. Puoi tenere traccia dello stato di avanzamento dell'attività fino all'esito positivo o negativo.

AWS CLI

Per creare l'attività di archiviazione delle immagini

Utilizzare il comando create-store-image-task.

```
aws ec2 create-store-image-task \
    --image-id ami-0abcdef1234567890 \
    --bucket amzn-s3-demo-bucket
```

Di seguito è riportato un output di esempio.

```
{
  "ObjectKey": "ami-0abcdef1234567890.bin"
}
```

Per descrivere lo stato di avanzamento di un'attività di archiviazione delle immagini

Utilizzare il comando describe-store-image-tasks.

```
aws ec2 describe-store-image-tasks \
    --image-ids ami-0abcdef1234567890 \
    --query StoreImageTaskResults[].StoreTaskState \
    --output text
```

Di seguito è riportato un output di esempio.

```
InProgress
```

PowerShell

Per creare l'attività di archiviazione delle immagini

Utilizza il cmdlet New-EC2StoreImageTask.

```
New-EC2StoreImageTask `
    -ImageId ami-0abcdef1234567890 `
    -Bucket amzn-s3-demo-bucket
```

Di seguito è riportato un output di esempio.

```
ObjectKey         : ami-0abcdef1234567890.bin
```

Per descrivere lo stato di avanzamento di un'attività di archiviazione delle immagini

Utilizza il cmdlet Get-EC2StoreImageTask.

```
(Get-EC2StoreImageTask -ImageId ami-0abcdef1234567890).StoreTaskState
```

Di seguito è riportato un output di esempio.

```
InProgress
```

Crea un'attività di ripristino delle immagini

Devi specificare anche un nome per l'AMI ripristinata. Il nome deve essere univoco per le AMI nella regione per questo account. L'AMI ripristinata ottiene un nuovo ID AMI.

AWS CLI

Per creare un'attività di archiviazione delle immagini

Utilizzare il comando create-restore-image-task.

```
aws ec2 create-restore-image-task \
    --object-key ami-0abcdef1234567890.bin \
    --bucket amzn-s3-demo-bucket \
    --name "my-restored-ami"
```

Di seguito è riportato un output di esempio.

```
{
   "ImageId": "ami-1234567890abcdef0"
}
```

PowerShell

Per creare un'attività di archiviazione delle immagini

Utilizza il cmdlet New-EC2RestoreImageTask.

```
New-EC2RestoreImageTask `
    -ObjectKey ami-0abcdef1234567890.bin `
    -Bucket amzn-s3-demo-bucket `
    -Name "my-restored-ami"
```

Di seguito è riportato un output di esempio.

```
ImageId         : ami-1234567890abcdef0
```

Usa l'ascendenza AMI per tracciare l'origine di un'AMI

AMI ancestry ti aiuta a tracciare l'origine di un'AMI restituendo gli ID e le regioni di tutte le sue AMI antenate. Quando si crea o si copia un'AMI, la nuova AMI conserva l'ID e la regione dell'AMI di origine (principale). Ciò consente di tracciare la catena di AMI fino all'AMI principale.

Vantaggi principali

L'utilizzo di AMI ancestry ti aiuta a:

- Tieni traccia dei derivati AMI per garantire la conformità alle politiche interne.
- Identifica le AMI potenzialmente vulnerabili quando viene rilevato un problema di sicurezza in un'AMI precedente.
- Mantieni la visibilità delle origini delle AMI in più regioni.

Argomenti

- Come funziona l'ascendenza AMI

- Considerazioni
- Visualizza gli antenati delle AMI
- Identificare l'AMI di origine

Come funziona l'ascendenza AMI

L'ascendenza AMI identifica l'AMI principale utilizzata per creare l'AMI specificata, l'AMI padre del padre e così via, fino all'AMI radice. Come funziona:

- Ogni AMI mostra l'ID e la regione dell'AMI di origine (padre).
- A partire dall'AMI selezionata, l'elenco delle voci di ascendenza mostra ogni AMI principale in sequenza.
- L'elenco delle voci di ascendenza risale a ritroso fino a raggiungere l'AMI principale. L'AMI principale è una delle seguenti:
  - Un'AMI pubblica di un provider verificato (identificata dall'alias del proprietario, che è `amazon` o `aws-marketplace`).
  - Un'AMI senza antenato registrato. Ad esempio, quando si utilizza per RegisterImage creare un'AMI direttamente da un set di istantanee, non c'è un'AMI di origine da tracciare, a differenza di quando si crea un'AMI da un'istanza.
  - Un'AMI la cui AMI di origine proviene da una partizione diversa.
  - La cinquantesima AMI della lista. Il numero massimo di AMI in un elenco di antenati è 50.

Considerazioni

- L'ID e la regione dell'AMI di origine sono disponibili solo per le AMI create utilizzando CreateImage,, CopyImage o. CreateRestoreImageTask
- Per le AMI create utilizzando CreateImage (crea un'AMI da un'istanza), l'ID AMI di origine è l'ID dell'AMI utilizzata per avviare l'istanza.
- Le informazioni sull'AMI di origine non sono disponibili per:
  - AMI create utilizzando RegisterImage perché sono state create a partire da istantanee.
  - Per alcune AMI meno recenti.
- Le informazioni AMI di origine vengono conservate quando:
  - Le AMI vengono copiate tra le regioni.
  - Le AMI di origine vengono cancellate (eliminate).

  - Non hai accesso alle AMI di origine.
- Ogni elenco di antenati è limitato a 50 AMI.

Visualizza gli antenati delle AMI

È possibile visualizzare l'ascendenza di un AMI utilizzando i seguenti metodi.

Console

Per visualizzare l'ascendenza di un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona un'AMI e scegli la scheda Antenati AMI.
4. La tabella delle voci degli antenati dell'AMI elenca tutte le AMI nell'elenco degli antenati.
   - ID AMI: l'identificatore di ogni AMI nell'elenco degli antenati. La prima voce nella tabella è l'AMI selezionata, seguita dai suoi antenati.
   - ID AMI di origine: l'ID dell'AMI da cui è stata creata l'AMI nella colonna ID AMI. Un trattino (-) indica la fine dell'elenco degli antenati dell'AMI.
   - Regione AMI di origine: Regione AWS dove si trova l'AMI di origine.
   - Livello di ascendenza: la posizione nell'elenco degli antenati, dove:
     - 0 (input AMI) indica l'AMI selezionata di cui si desidera conoscere l'ascendenza.
     - I numeri crescenti mostrano gli antenati più vecchi.
     - ***n***(AMI originale) indica l'AMI principale, mentre il numero indica a che distanza risale l'elenco degli antenati.
   - Data di creazione: data di creazione dell'AMI, in formato UTC.
   - Alias del proprietario: l'alias del proprietario dell'AMI (ad esempio,). `amazon` Un trattino (-) indica che l'AMI non ha un alias proprietario.

AWS CLI

Per visualizzare l'ascendenza di un'AMI

Usa il comando get-image-ancestry e specifica l'ID AMI.

```
aws ec2 get-image-ancestry \
    --image-id ami-1111111111EXAMPLE \
    --region us-east-1
```

Di seguito è riportato un output di esempio. L'output elenca le AMI in ordine alfabetico: la prima voce è l'AMI specificata (di input), seguita dall'AMI principale, dall'AMI principale e così via e termina con l'AMI radice.

```
{
    "ImageAncestryEntries": [
        {
            "CreationDate": "2025-01-17T18:37:50.000Z",
            "ImageId": "ami-1111111111EXAMPLE", // Input AMI
            "SourceImageId": "ami-2222222222EXAMPLE",
            "SourceImageRegion": "us-east-1"

        },
        {
            "CreationDate": "2025-01-17T18:37:50.000Z",
            "ImageId": "ami-2222222222EXAMPLE", // Parent AMI
            "SourceImageId": "ami-3333333333EXAMPLE",
            "SourceImageRegion": "us-east-1"
        },
        ...
        {
            "CreationDate": "2025-01-17T18:37:50.000Z",
            "ImageId": "ami-8888888888EXAMPLE", // Root AMI
            "ImageOwnerAlias": "aws-marketplace",
            "SourceImageId": "ami-9999999999EXAMPLE",
            "SourceImageRegion": "us-east-2"
        }
    ]
}
```

PowerShell

Per visualizzare l'ascendenza di un'AMI

Utilizza il cmdlet Get-EC2ImageAncestry.

```
Get-EC2ImageAncestry -ImageId ami-1111111111EXAMPLE
```

Di seguito è riportato un output di esempio. L'output elenca le AMI in ordine di ascendenza: la prima voce è l'AMI specificata (di input), seguita dall'AMI principale, dall'AMI principale e così via e termina con l'AMI radice.

```
ImageAncestryEntries : {
    @{
        CreationDate = "2025-01-17T18:37:50.000Z"
        ImageId = "ami-1111111111EXAMPLE"    # Input AMI
        SourceImageId = "ami-2222222222EXAMPLE"
        SourceImageRegion = "us-east-1"
    },
    @{
        CreationDate = "2025-01-17T18:37:50.000Z"
        ImageId = "ami-2222222222EXAMPLE"    # Parent AMI
        SourceImageId = "ami-3333333333EXAMPLE"
        SourceImageRegion = "us-east-1"
    },
    ...
    @{
        CreationDate = "2025-01-17T18:37:50.000Z"
        ImageId = "ami-8888888888EXAMPLE"    # Root AMI
        ImageOwnerAlias = "aws-marketplace"
        SourceImageId = "ami-9999999999EXAMPLE"
        SourceImageRegion = "us-east-2"
    }
}
```

Identificare l'AMI di origine

Se hai solo bisogno di identificare l'AMI principale immediata (fonte) utilizzata per creare un'AMI, puoi utilizzare i seguenti metodi.

Console

Per identificare l'AMI di origine utilizzata per creare l'AMI selezionata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI per visualizzare i dettagli.

Le informazioni sull'AMI di origine vengono visualizzate nei seguenti campi: ID AMI di origine e Regione AMI di origine

AWS CLI

Identificare l'AMI di origine utilizzata per creare l'AMI specificata

Utilizzare il comando describe-images .

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-0abcdef1234567890 \
    --query "Images[].{ID:SourceImageId,Region:SourceImageRegion}"
```

Di seguito è riportato un output di esempio.

```
[
    {
        "ID": "ami-0abcdef1234567890",
        "Region": "us-west-2"
    }
}
```

PowerShell

Identificare l'AMI di origine utilizzata per creare l'AMI specificata

Utilizza il cmdlet Get-EC2Image.

```
Get-EC2Image -ImageId ami-0abcdef1234567890 | Select SourceImageId,
 SourceImageRegion
```

Di seguito è riportato un output di esempio.

```
SourceImageId           SourceImageRegion
-------------           -----------------
ami-0abcdef1234567890 us-west-2
```

Usa le filigrane AMI per tracciare e identificare le AMI

Una filigrana AMI è un identificatore che alleghi alle tue AMI private per tracciare la provenienza e far rispettare le politiche di governance. Le filigrane persistono per tutto il ciclo di vita dell'AMI:

- Se crei una nuova AMI da un'istanza in esecuzione avviata da un'AMI con filigrana, la nuova AMI eredita la filigrana.
- Se si copia un'AMI con filigrana, la copia riporta la filigrana.
- Se condividi un'AMI con filigrana con un altro account, la filigrana rimane visibile al destinatario.

Vantaggi principali

- Tieni traccia della provenienza tra account e aree geografiche: identifica quali AMI derivano dalle tue immagini di base approvate.
- Filtra e trova le AMI correlate nei tuoi account.
- Aiuta i consumatori AMI a scoprire e identificare le AMI affidabili associate a un progetto o a un'organizzazione.
- Applica la governance combinando le filigrane con le AMI consentite per limitare l'avvio delle istanze alle sole AMI con filigrane approvate.

Argomenti

- Come funzionano le filigrane AMI
- Autorizzazioni richieste
- Allega una filigrana a un'AMI
- Stacca una filigrana da un'AMI
- Visualizza le filigrane AMI
- Filtrare le AMI in base alla filigrana

Come funzionano le filigrane AMI

Le filigrane AMI sono identificatori strutturati che alleghi alle tue AMI. Di seguito vengono descritte le caratteristiche principali delle filigrane:

- Persiste: quando si allega una filigrana a un'AMI, questa viene trasferita a tutte le AMI derivate.

- Owner-only— Solo il proprietario dell'AMI può allegare filigrane a un'AMI.
- Visibile a tutti: chiunque abbia accesso all'AMI può visualizzarne le filigrane.
- Limite di 5: un'AMI può avere fino a un totale di 5 filigrane.
- Non disponibile sulle AMI pubbliche: non è possibile allegare filigrane alle AMI pubbliche o rendere pubbliche le AMI se sono dotate di filigrana.
- Filtrabile: puoi filtrare le AMI in base alla filigrana durante l'utilizzo. `describe-images`

Formato filigrana

Una filigrana è un oggetto strutturato con i seguenti campi:

- `WatermarkKey`— L'identificatore univoco della filigrana, composto da. *`account-id`*`:`*`watermark-name`* La parte relativa all'ID dell'account è l'ID dell' AWS account a 12 cifre del titolare dell'AMI. La parte relativa al nome in filigrana è un nome specificato dal cliente.
- `SourceImageRegion`— La regione dell'AMI a cui hai originariamente associato la filigrana.
- `SourceImageId`— L'AMI a cui hai originariamente allegato la filigrana.
- `SourceImageCreationDate`— La data di creazione dell'AMI a cui hai originariamente allegato la filigrana.
- `WatermarkCreationTime`— Il timestamp di quando hai applicato la filigrana.

Il nome della filigrana deve contenere da 3 a 128 caratteri e può contenere caratteri alfanumerici, parentesi (()), parentesi quadre ([]), spazi, punti (.), barre (/), trattini (-), virgolette singole ('), chiocciola (@) o trattini bassi (_).

Autorizzazioni richieste

Per lavorare con le filigrane AMI, sono necessarie le seguenti autorizzazioni IAM:

- `ec2:AttachImageWatermark`— Per allegare una filigrana a un'AMI.
- `ec2:DetachImageWatermark`— Per staccare una filigrana da un AMI.
- `ec2:DescribeImages`— Per visualizzare le filigrane sulle AMI.

Allega una filigrana a un'AMI

Puoi allegare una filigrana a un'AMI utilizzando la console, il AWS CLI, o. PowerShell

Console

Per allegare una filigrana a un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI.
4. Nella scheda Dettagli, nella sezione Filigrane, scegli Gestisci filigrane.
5. Inserisci un nome per la filigrana e scegli Allega.

AWS CLI

Per allegare una filigrana a un'AMI

Usa il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/attach-image-watermark.html attach-image-watermark.

```
aws ec2 attach-image-watermark \
    --image-id ami-1111111111EXAMPLE \
    --image-watermark-name "prod-baseline"
```

Di seguito è riportato un output di esempio.

```
{
    "WatermarkKey": "123456789012:prod-baseline"
}
```

PowerShell

Per allegare una filigrana a un'AMI

Utilizza il cmdlet Add-EC2ImageWatermark.

```
Add-EC2ImageWatermark `
    -ImageId ami-1111111111EXAMPLE `
    -ImageWatermarkName "prod-baseline"
```

Puoi allegare fino a 5 filigrane a una singola AMI.

Stacca una filigrana da un'AMI

Puoi staccare una filigrana da un'AMI usando la console, o. AWS CLI PowerShell

Console

Per staccare una filigrana da un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI.
4. Nella scheda Dettagli, nella sezione Filigrane, scegli Gestisci filigrane.
5. Seleziona la filigrana da rimuovere, quindi scegli Rimuovi.

AWS CLI

Per staccare una filigrana da un'AMI

Usa il comando detach-image-watermark.

```
aws ec2 detach-image-watermark \
    --image-id ami-1111111111EXAMPLE \
    --image-watermark-key "111122223333:prod-baseline"
```

PowerShell

Per staccare una filigrana da un'AMI

Utilizza il cmdlet Remove-EC2ImageWatermark.

```
Remove-EC2ImageWatermark `
    -ImageId ami-1111111111EXAMPLE `
    -ImageWatermarkKey "111122223333:prod-baseline"
```

> **Note**
>
> La rimozione di una filigrana da un'AMI non la rimuove dalle AMI derivate che già contengono la filigrana. Per garantire che le filigrane rimangano persistenti, concedi

l'`ec2:DetachImageWatermark`autorizzazione solo agli amministratori fidati che devono gestire le filigrane.

Visualizza le filigrane AMI

È possibile visualizzare le filigrane per un'AMI utilizzando la console, il AWS CLI, o. PowerShell

Console

Per visualizzare le filigrane di un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI.
4. Visualizza le filigrane nella sezione Filigrane della scheda Dettagli.

AWS CLI

Per visualizzare le filigrane per un'AMI

Utilizzare il comando describe-images .

```
aws ec2 describe-images \
    --image-ids ami-046863d776a820ccd \
    --region us-east-1
```

La risposta include l'`ImageWatermarks`array per ogni AMI.

```
{
    "Images": [
        {
            "ImageId": "ami-046863d776a820ccd",
            "Public": false,
            "OwnerId": "123456789012",
            ...
            "ImageWatermarks": [
                {
                    "WatermarkKey": "111122223333:prod-baseline",
                    "Region": "us-east-1",
```

```
                    "SourceImageId": "ami-0b752bf1df193a6c4",
                    "SourceImageCreationDate": "2024-07-10T08:15:00",
                    "CreationDate": "2024-07-12T14:30:00"
                },
                {
                    "WatermarkKey": "222222222222:security-approved",
                    "Region": "eu-north-1",
                    "SourceImageId": "ami-12345678",
                    "SourceImageCreationDate": "2024-06-01T10:00:00",
                    "CreationDate": "2024-06-05T09:45:00"
                }
            ]
        }
    ]
}
```

PowerShell

Per visualizzare le filigrane per un'AMI

Utilizza il cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-046863d776a820ccd).ImageWatermarks
```

Filtrare le AMI in base alla filigrana

Puoi filtrare le AMI in base alla filigrana utilizzando la console, il, o. AWS CLI PowerShell

Console

Per filtrare le AMI in base alla filigrana

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Nella barra di ricerca, scegli il filtro chiave Watermark e inserisci il valore della chiave Watermark.

AWS CLI

Per filtrare le AMI in base alla filigrana

Utilizza il comando describe-images con il filtro `image-watermark-key`.

```
aws ec2 describe-images \
    --filters "Name=image-watermark-key,Values=111122223333:prod-baseline"
```

Vengono restituite tutte le AMI a cui hai accesso che riportano la filigrana specificata, incluse le AMI derivate che l'hanno ereditata tramite operazioni di copia.

PowerShell

Per filtrare le AMI in base alla filigrana

Utilizzare il Get-EC2Image cmdlet con il parametro. `-Filter`

```
Get-EC2Image `
    -Filter @{Name="image-watermark-key"; Values="111122223333:prod-baseline"}
```

Ciò restituisce tutte le AMI a cui hai accesso che riportano la filigrana specificata, incluse le AMI derivate che l'hanno ereditata tramite operazioni di copia.

Tipi di istanza AMI consentiti

In qualità di proprietario dell'AMI, puoi specificare quali tipi di istanze supporta o non supporta. Ciò impedisce l'avvio su tipi di istanza incompatibili. Amazon EC2 applica i tipi di istanza consentiti al momento del lancio.

Ad esempio, se la tua AMI richiede hardware GPU, puoi limitarla ai soli tipi di istanze GPU. Se la tua AMI è incompatibile con una specifica famiglia di istanze, puoi escludere quella famiglia dai tipi di istanze consentiti.

Indice

- Come funzionano i tipi di istanza consentiti
- Imposta i tipi di istanza consentiti per un'AMI
- Visualizza i tipi di istanza consentiti per un'AMI
- Comportamento di avvio con tipi di istanza consentiti
- Considerazioni

Come funzionano i tipi di istanza consentiti

È possibile controllare i tipi di istanza consentiti tramite l'`InstanceTypeSpecification`attributo su un'AMI. Questo attributo contiene due elenchi:

- `SupportedInstanceTypes`— I tipi di istanza supportati dall'AMI. Solo questi tipi di istanza possono essere avviati con l'AMI.
- `UnsupportedInstanceTypes`— I tipi di istanza che l'AMI non supporta. Tutti gli altri tipi di istanza possono essere avviati con l'AMI.

Amazon EC2 valuta le specifiche utilizzando la seguente logica:

- Se non `InstanceTypeSpecification` è impostato, Amazon EC2 consente tutti i tipi di istanza. Questo è il comportamento che segue di default.
- Se `SupportedInstanceTypes` è impostato only, sono consentiti solo i tipi di istanza specificati. Amazon EC2 blocca tutti gli altri tipi di istanza.
- Se `UnsupportedInstanceTypes` è impostato solo, Amazon EC2 consente tutti i tipi di istanza tranne quelli specificati.
- Se entrambi gli elenchi sono impostati, il tipo di istanza deve essere presente `SupportedInstanceTypes` e non deve essere presente`UnsupportedInstanceTypes`.

Supporto per i caratteri jolly

Entrambi gli elenchi supportano i caratteri jolly che utilizzano il `*` carattere. È possibile utilizzare i caratteri jolly per abbinare più tipi di istanza senza elencarli singolarmente.

La tabella seguente mostra alcuni esempi di modelli di caratteri jolly.

Pattern	Corrispondenze
`t3.*`	Tutte le dimensioni all'interno della famiglia di `t3` istanze (ad esempio`t3.micro`,`t3.small`, e`t3.large`)
`p4d.*`	Tutte le dimensioni all'interno della famiglia di `p4d` istanze
`g5.*`	Tutte le dimensioni all'interno della famiglia di `g5` istanze

Pattern	Corrispondenze
`*xlarge`	Qualsiasi tipo di istanza di dimensioni maggiori o maggiori in tutte le famiglie di istanze
`*.12xlarge`	Qualsiasi tipo di istanza 12xlarge in tutte le famiglie di istanze

Imposta i tipi di istanza consentiti per un'AMI

Puoi impostare o modificare i tipi di istanza consentiti per un'AMI utilizzando la console Amazon EC2 o AWS Command Line Interface (AWS CLI). Per eseguire questa procedura, è necessario essere il proprietario dell'AMI.

Console

Per impostare i tipi di istanza consentiti per un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI, quindi scegli Azioni, Gestisci la specifica del tipo di istanza.
4. In Tipi di istanza supportati o Tipi di istanza non supportati, scegli Aggiungi.
5. Selezionare il tipo di istanza .
6. Selezionare Salva.

AWS CLI

Per impostare i tipi di istanza supportati per un'AMI

Utilizza il comando replace-image-instance-type-specification. L'esempio seguente consente tutti `t3` i tipi di `a2` istanza tranne`t3.micro`.

```
aws ec2 replace-image-instance-type-specification \
    --image-id ami-1234567890abcdef0 \
    --instance-type-specification '{"SupportedInstanceTypes": ["t3.*", "a2.*"],
 "UnsupportedInstanceTypes": ["t3.micro"]}'
```

Per impostare solo i tipi di istanza non supportati per un'AMI

Usa il comando seguente per bloccare tipi di istanza specifici consentendone tutti gli altri.

```
aws ec2 replace-image-instance-type-specification \
    --image-id ami-1234567890abcdef0 \
    --instance-type-specification '{"UnsupportedInstanceTypes": ["t3.micro",
 "t3.nano"]}'
```

Per rimuovere la specifica del tipo di istanza da un'AMI

Utilizzate il seguente comando senza specificare `--instance-type-specification` per rimuovere la restrizione e consentire tutti i tipi di istanza.

```
aws ec2 replace-image-instance-type-specification \
    --image-id ami-1234567890abcdef0
```

Visualizza i tipi di istanza consentiti per un'AMI

Puoi visualizzare le specifiche del tipo di istanza per un'AMI utilizzando la console Amazon EC2 o il AWS CLI.

Console

Per visualizzare i tipi di istanza consentiti per un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI.
4. Nella scheda Dettagli, visualizza i tipi di istanza supportati e non supportati.

AWS CLI

Per visualizzare le specifiche del tipo di istanza per un'AMI

Utilizza il comando describe-images. Se l'AMI ha una specifica del tipo di istanza, la risposta include il `InstanceTypeSpecification` campo.

```
aws ec2 describe-images \
```

```
    --image-ids ami-1234567890abcdef0
```

Di seguito è riportato un esempio di output per un'AMI con una specifica del tipo di istanza.

```
{
    "Images": [
        {
            "ImageId": "ami-1234567890abcdef0",
            ...
            "InstanceTypeSpecification": {
                "SupportedInstanceTypes": [
                    {
                        "InstanceType": "t3.*"
                    },
                    {
                        "InstanceType": "a2.*"
                    }
                ],
                "UnsupportedInstanceTypes": [
                    {
                        "InstanceType": "t3.micro"
                    }
                ]
            }
        }
    ]
}
```

Comportamento di avvio con tipi di istanza consentiti

Quando avvii un'istanza, Amazon EC2 verifica se il tipo di istanza specificato è compatibile con la specifica del tipo di istanza dell'AMI. Se il tipo di istanza non è consentito, Amazon EC2 blocca l'avvio e restituisce un errore.

Esempio: avvio bloccato

Il comando seguente tenta di avviare un'`t3.micro`istanza utilizzando un'AMI che non supporta`t3.micro`.

```
aws ec2 run-instances \
    --image-id ami-1234567890abcdef0 \
```

```
    --instance-type t3.micro
```

Amazon EC2 restituisce il seguente errore:

```
An error occurred (InvalidParameterCombination) when calling the RunInstances
 operation: This AMI does not support the specified instance type. Check DescribeImages
 for InstanceTypeSpecification, and try again.
```

Per risolvere questo errore, scegli un tipo di istanza supportato dall'AMI. Utilizzate il `describe-images` comando per visualizzare le specifiche del tipo di istanza dell'AMI.

Considerazioni

Tieni presente le seguenti informazioni quando utilizzi i tipi di istanza consentiti.

- Per impostazione predefinita, un'AMI non ha una specifica del tipo di istanza. Amazon EC2 consente tutti i tipi di istanza fino a quando non viene impostata esplicitamente una specifica.
- Solo il proprietario dell'AMI può impostare o modificare la specifica del tipo di istanza.
- Quando si copia un'AMI utilizzando`CopyImage`, Amazon EC2 conserva la specifica del tipo di istanza nella nuova AMI.
- Amazon EC2 applica la specifica del tipo di istanza come blocco fisso. Se il tipo di istanza non è consentito, l'avvio non riesce con un `InvalidParameterCombination` errore.
- La specifica non influisce sulle istanze esistenti. Si applica solo ai nuovi lanci.
- I modelli di avvio e i gruppi Auto Scaling che fanno riferimento a un'AMI con una specifica del tipo di istanza possono avere esito negativo se il tipo di istanza configurato non è consentito. Consigliamo di verificare la compatibilità prima di impostare una specifica sulle AMI condivise.
- L'`ReplaceImageInstanceTypeSpecification`azione sostituisce l'intera specifica. Per aggiungere o rimuovere singoli tipi di istanza, è necessario includere la specifica completa aggiornata nella richiesta.

Gestisci e monitora l'uso delle AMI

AWS offre diverse funzionalità per aiutarti a gestire e monitorare l'utilizzo dell'AMI in modo efficace. Puoi tenere traccia degli account che utilizzano le tue AMI condivise, identificare quando le tue AMI sono state utilizzate l'ultima volta e scoprire quali risorse delle tue Account AWS fanno riferimento ad AMI specifiche.

La seguente tabella offre una panoramica delle funzionalità per la gestione e il monitoraggio dell'uso delle AMI:

Funzionalità	Caso d'uso	Vantaggi principali
Report di utilizzo dell'AMI	Ottieni visibilità su quali AMI Account AWS vengono utilizzate e in che misura ciascuna AMI viene utilizzata.	• Identifica i tipi Account AWS e le risorse che fanno riferimento alle tue AMI in modo da poter annullare o disabilitare le AMI in tutta sicurezza. • Identifica le AMI non utilizzate per annullare la registrazione in modo da ridurre i costi di archiviazione. • Identifica le AMI più utilizzate.
Tracciamento ultimo utilizzo	Verifica quando la tua AMI è stata utilizzata per l'ultima volta.	• Identifica le AMI non utilizzate in modo da poter annullare la registrazione delle AMI in sicurezza. • Identifica le AMI non utilizzate per annullare la registrazione in modo da ridurre i costi di archiviazione.
Controllo dei riferimenti alle AMI	Assicurati che le tue AWS risorse utilizzino le AMI conformi più recenti.	• Controllare l'utilizzo delle AMI nel tuo account. •

Funzionalità	Caso d'uso	Vantaggi principali
		• Controllare dove viene fatto riferimento a specifiche AMI. • Garantire la conformità aggiornando le tue risorse in modo che facciano riferimento alle AMI più recenti.

Argomenti

- Visualizza l'uso dell'AMI
- Verifica quando un'AMI Amazon EC2 è stata utilizzata per l'ultima volta
- Identifica le tue risorse che fanno riferimento ad AMI specificate

Visualizza l'uso dell'AMI

Se condividi le tue Amazon Machine Images (AMI) con altri Account AWS, con organizzazioni specifiche Account AWS, unità organizzative (OU) o pubblicamente, puoi vedere come vengono utilizzate queste AMI creando report sull'utilizzo delle AMI. I report danno visibilità su:

- Quali Account AWS utilizzano le tue AMI nelle istanze EC2 o nei modelli di avvio
- Quante istanze o quanti modelli di avvio EC2 fanno riferimento a ciascuna AMI

I report sull'uso delle AMI ti aiutano a gestire le tue AMI in modo più efficace aiutandoti a:

- Identifica le AMI Account AWS e i tipi di risorse che fanno riferimento alle tue AMI in modo da poter annullare o disabilitare le AMI in tutta sicurezza.
- Identifica le AMI non utilizzate per annullare la registrazione in modo da ridurre i costi di archiviazione.
- Identificare le AMI più utilizzate.

Indice

- Come funzionano i report sull'uso delle AMI

- Crea un report sull'utilizzo dell'AMI
- Visualizza i report sull'utilizzo dell'AMI
- Elimina un report sull'utilizzo dell'AMI
- Quote dei report

Come funzionano i report sull'uso delle AMI

Per creare un report sull'uso AMI, specifica:

- L'AMI da includere nel report.
- I Account AWS da controllare (account specifici o tutti gli account).
- I tipi di risorsa da controllare (istanze EC2, modelli di avvio o entrambi).
- Per i modelli di avvio, il numero di versioni da controllare (il valore predefinito è rappresentato dalle 20 versioni più recenti).

Amazon EC2 crea un report separato per ogni AMI. Ogni report fornisce:

- Un elenco degli Account AWS utenti dell'AMI.
- Un conto delle risorse che fanno riferimento all'AMI per tipo di risorsa per account. Nota che per i modelli di avvio, se si fa riferimento a un'AMI in più versioni di un modello di avvio, il conteggio è solo 1.

> **Important**
>
> Quando generi un report sull'utilizzo dell'AMI, potrebbe non contenere l'attività più recente. L'attività delle istanze delle ultime 24 ore e l'attività del modello di avvio degli ultimi giorni potrebbero non apparire nel report.

Amazon EC2 elimina automaticamente un report 30 giorni dopo la sua creazione. Puoi scaricare i report dalla console EC2 per mantenerli localmente.

Crea un report sull'utilizzo dell'AMI

Per visualizzare come viene usata l'AMI, è necessario innanzitutto creare un report sull'utilizzo dell'AMI, specificando gli account e i tipi di risorse da includere nel report. Dopo la creazione del rapporto, è possibile visualizzarne il contenuto. Puoi anche scaricare il report dalla console EC2.

Console

Per creare un report sull'utilizzo dell'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona un AMI e scegli Operazioni, Uso dell'AMI, Visualizza il mio utilizzo dell'AMI.
4. Nella pagina Crea il mio report dell'AMI, procedi come segue:
   a. Per Tipi di risorsa, seleziona uno o più tipi di risorse da includere nel report.
   b. Per ID account, esegui una delle seguenti operazioni:
      - Scegli Specifica gli ID degli account, quindi seleziona Aggiungi ID account per ogni account da includere nel report.
      - Scegli Includi tutti gli account per generare un report su tutti gli account.
   c. Seleziona Crea il mio report sull'utilizzo dell'AMI.
5. Nella pagina AMI, seleziona la scheda Il mio uso dell'AMI.
6. Scegli l'ID di un report per visualizzarne i dettagli.

AWS CLI

Per creare un report sull'utilizzo dell'AMI per un elenco di account

Usa il comando create-image-usage-report con i seguenti parametri obbligatori:

- `--image-id`: l'ID dell'AMI da includere nel report.
- `--resource-types`: i tipi di risorse da controllare. Nel seguente esempio, i tipi di risorse da controllare sono le istanze EC2 e i modelli di avvio. Viene specificato anche il numero di versioni del modello di avvio da controllare (`version-depth=100`).

Per creare report su account specifici, usa il parametro `--account-ids` per specificare l'ID di ciascun account da includere nel report.

```
aws ec2 create-image-usage-report \
    --image-id ami-0abcdef1234567890 \
    --account-ids 111122223333 444455556666 123456789012 \
    --resource-types ResourceType=ec2:Instance \
      'ResourceType=ec2:LaunchTemplate,ResourceTypeOptions=[{OptionName=version-
depth,OptionValues=100}]'
```

Per creare un report sull'uso dell'AMI di tutti gli account

Per includere nel report tutti gli account che utilizzano l'AMI specificata, usa lo stesso comando ma ometti il parametro `--account-ids`.

```
aws ec2 create-image-usage-report \
    --image-id ami-0abcdef1234567890 \
    --resource-types ResourceType=ec2:Instance \
      'ResourceType=ec2:LaunchTemplate,ResourceTypeOptions=[{OptionName=version-
depth,OptionValues=100}]'
```

Di seguito è riportato un output di esempio.

```
{
    "ReportId": "amiur-00b877d192f6b02d0"
}
```

Per monitorare lo stato della creazione del report

Usa il comando describe-image-usage-reports e specifica l'ID del report.

```
aws ec2 describe-image-usage-reports --report-ids amiur-00b877d192f6b02d0
```

Di seguito è riportato un output di esempio. Il valore iniziale del campo `State` è `pending`. Per poter visualizzare le voci del report, lo stato deve essere `available`.

```
{
    "ImageUsageReports": [
        {
            "ImageId": "ami-0e9ae3dc21c2b3a64",
```

```
            "ReportId": "amiur-abcae3dc21c2b3999",
            "ResourceTypes": [
                {"ResourceType": "ec2:Instance"}
            ],
            "State": "pending",
            "CreationTime": "2025-09-29T13:27:12.322000+00:00",
            "ExpirationTime": "2025-10-28T13:27:12.322000+00:00"
        }
    ]
}
```

PowerShell

Per creare un report sull'utilizzo dell'AMI per un elenco di account

Utilizzare il New-EC2ImageUsageReport cmdlet con i seguenti parametri obbligatori:

- `-ImageId`: l'ID dell'AMI da includere nel report.
- `-ResourceType`: i tipi di risorse da controllare. Nel seguente esempio, i tipi di risorse da controllare sono le istanze EC2 e i modelli di avvio. Viene specificato anche il numero di versioni del modello di avvio da controllare (`'version-depth' = 100`).

Per creare report su account specifici, usa il parametro `-AccountId` per specificare l'ID di ciascun account da includere nel report.

```
New-EC2ImageUsageReport `
    -ImageId ami-0abcdef1234567890 `
    -AccountId 111122223333 444455556666 123456789012 `
    -ResourceType @(
        @{ResourceType = 'ec2:Instance'},
        @{ResourceType = 'ec2:LaunchTemplate'ResourceTypeOptions = @{'version-depth'
 = 100}
        })
```

Per creare un report sull'uso dell'AMI di tutti gli account

Per includere nel report tutti gli account che utilizzano l'AMI specificata, usa lo stesso comando ma ometti il parametro `-AccountId`.

```
New-EC2ImageUsageReport `
```

```
    -ImageId ami-0abcdef1234567890 `
    -ResourceType @(
        @{ResourceType = 'ec2:Instance'},
        @{ResourceType = 'ec2:LaunchTemplate'ResourceTypeOptions = @{'version-depth'
 = 100}
        })
```

Di seguito è riportato un output di esempio.

```
ReportId
--------
amiur-00b877d192f6b02d0
```

Per monitorare lo stato della creazione del report

Utilizzare il Get-EC2ImageUsageReport comando e specificare l'ID del report.

```
Get-EC2ImageUsageReport -ReportId amiur-00b877d192f6b02d0
```

Di seguito è riportato un output di esempio. Il valore iniziale del campo `State` è `pending`. Per poter visualizzare le voci del report, lo stato deve essere `available`.

```
ImageUsageReports
-----------------
{@{ImageId=ami-0e9ae3dc21c2b3a64; ReportId=amiur-abcae3dc21c2b3999;
 ResourceTypes=System.Object[]; State=pending; CreationTime=2025-09-29;
 ExpirationTime=2025-10-28}}
```

Visualizza i report sull'utilizzo dell'AMI

Puoi visualizzare tutti i report sull'utilizzo creati per un'AMI negli ultimi 30 giorni. Amazon EC2 elimina automaticamente un report 30 giorni dopo la sua creazione.

Per ogni rapporto, puoi vedere le risorse Account AWS che utilizzano l'AMI e, per ogni account, un conteggio delle risorse che fanno riferimento all'AMI per tipo di risorsa. Puoi inoltre vedere quando è stata avviata la creazione del report. Queste informazioni sono disponibili soltanto quando il report è nello stato Completo (console) o `available` (AWS CLI).

> **Important**
>
> Quando generi un report sull'utilizzo dell'AMI, potrebbe non contenere l'attività più recente. L'attività delle istanze delle ultime 24 ore e l'attività del modello di avvio degli ultimi giorni potrebbero non apparire nel report.

Console

Per visualizzare un report sull'utilizzo dell'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Selezionare un'AMI.
4. Seleziona la scheda I miei report sull'utilizzo.

   La lista dei report mostra:

   - Tutti i report generati negli ultimi 30 giorni per l'AMI selezionata.
   - Per ogni report, la colonna Ora di avvio del report mostra la data di creazione del report.
5. Scegli l'ID di un report per visualizzare il suo contenuto.
6. Per tornare alla scheda I miei report sull'utilizzo nella pagina dei dettagli dell'AMI, scegli Visualizza tutti i report per questa AMI.

AWS CLI

Per elencare tutti i report sull'utilizzo dell'AMI per l'AMI specificata

Utilizza il comando describe-image-usage-reports e specifica l'ID dell'AMI per ottenere un elenco dei suoi report.

```
aws ec2 describe-image-usage-reports --image-ids ami-0abcdef1234567890
```

Di seguito è riportato un output di esempio. Ogni ID del report è inserito nell'elenco insieme ai tipi di risorse sottoposti a scansione e alle date di creazione e scadenza del report. Puoi usare queste informazioni per identificare i report di cui desideri visualizzare le voci.

```
{
```

```
  "ImageUsageReports": [
    {
      "ImageId": "ami-0abcdef1234567890",
      "ReportId": "amiur-1111111111111111",
      "ResourceTypes": [
        {
          "ResourceType": "ec2:Instance"
        }
      ],
      "State": "available",
      "CreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ExpirationTime": "2025-10-28T13:27:12.322000+00:00",
      "Tags": []
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ReportId": "amiur-22222222222222222",
      "ResourceTypes": [
        {
          "ResourceType": "ec2:Instance"
        },
        {
          "ResourceType": "ec2:LaunchTemplate"
        }
      ],
      "State": "available",
      "CreationTime": "2025-10-01T13:27:12.322000+00:00",
      "ExpirationTime": "2025-10-30T13:27:12.322000+00:00",
      "Tags": []
    }
  ],
  "NextToken": "opaque"
}
```

Per visualizzare il contenuto di un report sull'utilizzo dell'AMI per l'AMI specificata

Usa il comando describe-image-usage-report-entries e specifica l'ID dell'AMI. La risposta restituisce tutti i report per l'AMI specificata, mostrando gli account che hanno usato l'AMI e il relativo numero di risorse.

```
aws ec2 describe-image-usage-report-entries --image-ids ami-0abcdef1234567890
```

Di seguito è riportato un output di esempio.

```
{
  "ImageUsageReportEntries": [
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "123412341234",
      "UsageCount": 15,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "123412341234",
      "UsageCount": 2,
      "ReportCreationTime": "2025-10-01T13:27:12.322000+00:00",
      "ReportId": "amiur-22222222222222222"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "001100110011",
      "UsageCount": 39,
      "ReportCreationTime": "2025-10-01T13:27:12.322000+00:00",
      "ReportId": "amiur-22222222222222222"
    }
  ],
  "NextToken": "opaque"
}
```

Per visualizzare il contenuto di un report sull'utilizzo dell'AMI per il report specificato

Usa il comando describe-image-usage-report-entries e specifica l'ID del report. La risposta restituisce tutte le voci del report specificato, mostrando gli account che hanno usato l'AMI e il relativo numero di risorse.

```
aws ec2 describe-image-usage-report-entries --report-ids amiur-1111111111111111
```

Di seguito è riportato un output di esempio.

```
{
  "ImageUsageReportEntries": [
```

```
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "123412341234",
      "UsageCount": 15,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:LaunchTemplate",
      "AccountId": "123412341234",
      "UsageCount": 4,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:LaunchTemplate",
      "AccountId": "001100110011",
      "UsageCount": 2,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    }
  ],
  "NextToken": "opaque"
}
```

PowerShell

Per elencare tutti i report sull'utilizzo dell'AMI per l'AMI specificata

Utilizza il Get-EC2ImageUsageReport cmdlet e specifica l'ID dell'AMI per ottenere un elenco dei relativi report.

```
Get-EC2ImageUsageReport -ImageId ami-0abcdef1234567890
```

Di seguito è riportato un output di esempio. Ogni ID del report è inserito nell'elenco insieme ai tipi di risorse sottoposti a scansione e alle date di creazione e scadenza del report. Puoi usare queste informazioni per identificare i report di cui desideri visualizzare le voci.

```
@{
```

```
    ImageUsageReports = @(
        @{
            ImageId = "ami-0abcdef1234567890"
            ReportId = "amiur-1111111111111111"
            ResourceTypes = @(
                @{
                    ResourceType = "ec2:Instance"
                }
            )
            State = "available"
            CreationTime = "2025-09-29T13:27:12.322000+00:00"
            ExpirationTime = "2025-10-28T13:27:12.322000+00:00"
        },
        @{
            ImageId = "ami-0abcdef1234567890"
            ReportId = "amiur-2222222222222222"
            ResourceTypes = @(
                @{
                    ResourceType = "ec2:Instance"
                }
            )
            State = "available"
            CreationTime = "2025-09-30T13:27:12.322000+00:00"
            ExpirationTime = "2025-10-29T13:27:12.322000+00:00"
        },
        @{
            ImageId = "ami-0abcdef1234567890"
            ReportId = "amiur-33333333333333333"
            ResourceTypes = @(
                @{
                    ResourceType = "ec2:Instance"
                }
            )
            State = "available"
            CreationTime = "2025-10-01T13:27:12.322000+00:00"
            ExpirationTime = "2025-10-30T13:27:12.322000+00:00"
        }
    )
    NextToken = "opaque"
}
```

Per visualizzare il contenuto di un report sull'utilizzo dell'AMI per l'AMI specificata

Utilizzare il Get-EC2ImageUsageReportEntry cmdlet e specificare l'ID dell'AMI. La risposta restituisce tutti i report per l'AMI specificata, mostrando gli account che hanno usato l'AMI e il relativo numero di risorse.

```
Get-EC2ImageUsageReportEntry -ImageId ami-0abcdef1234567890
```

Di seguito è riportato un output di esempio.

```
ImageUsageReportEntries : {@{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:Instance"
    AccountId = "123412341234"
    UsageCount = 15
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-1111111111111111"
    }, @{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:Instance"
    AccountId = "123412341234"
    UsageCount = 7
    ReportCreationTime = "2025-09-30T13:27:12.322000+00:00"
    ReportId = "amiur-22222222222222222"
    }...}
NextToken : opaque
```

Per visualizzare il contenuto di un report sull'utilizzo dell'AMI per il report specificato

Utilizzare il Get-EC2ImageUsageReportEntry cmdlet e specificare l'ID del report. La risposta restituisce tutte le voci del report specificato, mostrando gli account che hanno usato l'AMI e il relativo numero di risorse.

```
Get-EC2ImageUsageReportEntry -ReportId amiur-1111111111111111
```

Di seguito è riportato un output di esempio.

```
ImageUsageReportEntries : {@{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:Instance"
    AccountId = "123412341234"
    UsageCount = 15
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
```

```
    ReportId = "amiur-11111111111111111"
    }, @{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:LaunchTemplate"
    AccountId = "123412341234"
    UsageCount = 4
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-11111111111111111"
    }, @{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:LaunchTemplate"
    AccountId = "************"
    UsageCount = 2
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-11111111111111111"
    }}
NextToken : opaque
```

Elimina un report sull'utilizzo dell'AMI

Amazon EC2 elimina automaticamente un report 30 giorni dopo la sua creazione. Puoi eliminarlo manualmente prima di allora.

Console

Per eliminare un report sull'utilizzo dell'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Selezionare un'AMI.
4. Scegli la scheda Il mio uso dell'AMI.
5. Seleziona il pulsante di opzione accanto al report da eliminare e quindi scegli Elimina.

AWS CLI

Per eliminare un report sull'utilizzo dell'AMI

Usa il comando delete-image-usage-report e specifica l'ID del report.

```
aws ec2 delete-image-usage-report --report-id amiur-0123456789abcdefg
```

PowerShell

Per eliminare un report sull'utilizzo dell'AMI

Utilizzare il Remove-EC2ImageUsageReport cmdlet e specificare l'ID del report.

```
Remove-EC2ImageUsageReport -ReportId amiur-0123456789abcdefg
```

Quote dei report

Le seguenti quote si applicano alla creazione dei report sull'utilizzo dell'AMI. Le quote si applicano per Regione AWS.

Description	Quota
In-progress (`pending`) Rapporti sull'utilizzo dell'AMI per Account AWS	2.000
In-progress (`pending`) Rapporti sull'utilizzo dell'AMI per AMI	1

Verifica quando un'AMI Amazon EC2 è stata utilizzata per l'ultima volta

Amazon EC2 traccia automaticamente la data e l'ora di ultimo utilizzo dell'AMI per avviare un'istanza. Se disponi di un'AMI che non viene utilizzata per avviare un'istanza da molto tempo, valuta se l'AMI è un buon candidato per l'annullamento della registrazione o l'obsolescenza.

Considerazioni

- Quando si utilizza un'AMI per avviare un'istanza, il relativo utilizzo viene segnalato dopo 24 ore.
- Devi essere il proprietario dell'AMI per ottenere l'ora dell'ultimo avvio.
- I dati sull'utilizzo dell'AMI sono disponibili a partire da aprile 2017.

Console

Per visualizzare l'ultima data e ora di avvio di un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione a sinistra scegliere AMIs (AMI).
3. Nella barra del filtro, scegli Owned by me (Di mia proprietà).
4. Seleziona la casella di controllo relativa all'AMI.
5. Nella scheda Dettagli, trova Ultima data e ora di avvio.

AWS CLI

Per visualizzare l'ultima data e ora di avvio di un'AMI

Utilizzare il comando describe-images . Se `LastLaunchedTime` non è presente nell'output, verifica di essere il proprietario dell'AMI.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query Images[].LastLaunchedTime \
    --output text
```

Di seguito è riportato un output di esempio.

```
2025-02-17T20:22:19Z
```

Per visualizzare l'attributo dell'ultima data e ora di avvio di un'AMI

Utilizza il comando describe-image-attribute. Devi possedere l'AMI.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute lastLaunchedTime \
    --query LastLaunchedTime.Value \
    --output text
```

Di seguito è riportato un output di esempio.

```
2025-02-17T20:22:19Z
```

PowerShell

Per visualizzare l'ultima data e ora di avvio di un'AMI

Utilizza il cmdlet Get-EC2Image. Se `LastLaunchedTime` non è presente nell'output, verifica di essere il proprietario dell'AMI.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).LastLaunchedTime
```

Di seguito è riportato un output di esempio.

```
2025-02-17T20:22:19Z
```

Per visualizzare l'attributo dell'ultima data e ora di avvio di un'AMI

Utilizza il cmdlet Get-EC2ImageAttribute. Devi possedere l'AMI.

```
(Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute LastLaunchedTime).LastLaunchedTime
```

Di seguito è riportato un output di esempio.

```
2025-02-17T20:22:19Z
```

Identifica le tue risorse che fanno riferimento ad AMI specificate

Puoi identificare AWS le tue risorse che fanno riferimento a specifiche Amazon Machine Images (AMI), indipendentemente dal fatto che le AMI siano pubbliche o private o da chi le possiede. Questa visibilità ti aiuta a garantire che le tue risorse utilizzino le AMI conformi più recenti.

Vantaggi principali

Controllare i riferimenti AMI ti aiuta a:

- Controllare l'utilizzo delle AMI nel tuo account.
- Controllare dove viene fatto riferimento a specifiche AMI.
- Garantire la conformità aggiornando le tue risorse in modo che facciano riferimento alle AMI più recenti.

Argomenti

- Risorse supportate
- Come funzionano i controlli dei riferimenti AMI
- Autorizzazioni IAM richieste
- Fasi per verificare i riferimenti AMI

Risorse supportate

I riferimenti all'AMI possono essere controllati in:

- Istanze EC2
- Modelli di avvio
- Parametri SSM
- ricette di immagini Image Builder
- ricette di container Image Builder

Come funzionano i controlli dei riferimenti AMI

Funzionamento di base

Quando esegui un controllo dei riferimenti AMI:

- Specifichi quali AMI controllare.
- Scegli i tipi di risorse da scansionare.
- Ricevi un elenco delle tue risorse che si riferiscono alle AMI specificate.

Selezione dei tipi di risorsa

Nella console, selezioni i tipi di risorsa da scansionare.

Nella CLI, specifichi i tipi di risorse da scansionare utilizzando uno o entrambi i seguenti parametri CLI:

- `IncludeAllResourceTypes`: esegue la scansione di tutti i tipi di risorse supportati.
- `ResourceTypes`: esegue la scansione dei tipi di risorse specificati.

Ambito di risposta

Puoi definire l'ambito della risposta per le istanze EC2 e i modelli di avvio personalizzando i valori `ResourceTypeOptions` utilizzando il parametro `ResourceTypes`. Sia la console che il parametro `IncludeAllResourceTypes` utilizzano i valori delle opzioni predefiniti. Quando `ResourceTypes` e `IncludeAllResourceTypes` vengono utilizzati insieme, i valori dell'opzione `ResourceTypes` hanno la precedenza sui valori predefiniti.

Di seguito sono riportati i valori predefiniti:

Tipo di risorsa	Opzione di definizione dell'ambito (**`OptionName`**)	Scopo	Valori predefiniti per **`OptionValue`** e console
Istanze EC2	`state-name`	Filtra per stato dell'istanza	`pending`, `running`, `shutting-down`, `terminated`, `stopping`, `stopped` (tutti gli stati)
Modelli di avvio	`version-depth`	Specifica il numero di versioni del modello di avvio da controllare (a partire dalla versione più recente)	`10` (versioni più recenti)

Autorizzazioni IAM richieste

Per utilizzare l'API DescribeImageReferences e identificare le tue risorse che fanno riferimento a AMI specifiche, hai bisogno dei seguenti permessi IAM per descrivere le risorse:

- `ec2:DescribeInstances`
- `ec2:DescribeLaunchTemplates`
- `ec2:DescribeLaunchTemplateVersions`
- `ssm:DescribeParameters`
- `ssm:GetParameters`

- `imagebuilder:ListImageRecipes`
- `imagebuilder:ListContainerRecipes`
- `imagebuilder:GetContainerRecipe`

Esempio di politica IAM per l'utilizzo di DescribeImageReferences "Hello, World!"

La seguente policy di esempio concede le autorizzazioni per utilizzare l'API DescribeImageReferences, che include le autorizzazioni per descrivere istanze EC2, modelli di avvio, parametri Systems Manager, ricette immagine Image Builder e ricette container Image Builder.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "ec2:DescribeImageReferences",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeLaunchTemplateVersions",
    "ssm:DescribeParameters",
    "ssm:GetParameters",
    "imagebuilder:ListImageRecipes",
    "imagebuilder:ListContainerRecipes",
    "imagebuilder:GetContainerRecipe"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "ec2-images.amazonaws.com"
     ]
    }
   }
  }
```

```
 ]
}
```

Important

Consigliamo vivamente di utilizzare la policy AWS gestita `AmazonEC2ImageReferencesAccessPolicy` invece di crearla tu stesso. Creare una policy IAM personalizzata che fornisca solo le autorizzazioni necessarie richiede tempo e competenze specifiche e richiederà aggiornamenti man mano che saranno disponibili nuovi tipi di risorse.
La policy gestita `AmazonEC2ImageReferencesAccessPolicy`

- Concede tutte le autorizzazioni necessarie per utilizzare l'API DescribeImageReferences (tra cui le autorizzazioni per descrivere istanze EC2, modelli di avvio, parametri Systems Manager, ricette di container e immagini Image Builder).
- Supporta automaticamente nuovi tipi di risorse non appena diventano disponibili (particolarmente importante quando si utilizza il parametro `IncludeAllResourceTypes`).

Puoi associare la policy `AmazonEC2ImageReferencesAccessPolicy` alle identità IAM (utenti, gruppi e ruoli).
Per vedere le autorizzazioni incluse in questa policy, consulta AmazonEC2ImageReferencesAccessPolicy nella Guida di riferimento sulle policy gestite da AWS .

Fasi per verificare i riferimenti AMI

Utilizza le seguenti procedure per identificare quali delle tue AWS risorse fanno riferimento alle AMI specificate.

Console

Per identificare le risorse che fanno riferimento ad AMI specificate

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona una o più AMI per verificare i riferimenti.

4. Seleziona Azioni, Utilizzo delle AMI, Visualizza risorse di riferimento.
5. Nella pagina Visualizza risorse si riferiscono alle AMI selezionate:

   a. Per Tipi di risorsa, seleziona uno o più tipi di risorse.

   b. Seleziona Visualizza risorse.
6. Viene visualizzata la sezione Risorse che si riferiscono alle AMI selezionate. L'elenco mostra le risorse che si riferiscono alle AMI specificate. Ogni riga fornisce le seguenti informazioni:

   - ID dell'AMI: l'ID dell'AMI a cui viene fatto riferimento.
   - Tipo di risorsa: il tipo di risorsa che fa riferimento all'AMI.
   - ID della risorsa: l'ID della risorsa che fa riferimento all'AMI.

AWS CLI

Per controllare i riferimenti alle AMI per tipi di risorse specifici

Utilizza il comando describe-image-references con il parametro `--resource-types`. Nell'esempio seguente vengono controllate le istanze EC2 (ambito di applicazione in base allo stato dell'istanza), i modelli di avvio (ambito di applicazione alle 20 versioni più recenti dei modelli di avvio) e altri tipi di risorse specifici.

```
aws ec2 describe-image-references \
    --image-ids ami-0abcdef1234567890 ami-1234567890abcdef0 \
    --resource-types \
        'ResourceType=ec2:Instance,ResourceTypeOptions=[{OptionName=state-
name,OptionValues=[running,pending]}]' \
        'ResourceType=ec2:LaunchTemplate,ResourceTypeOptions=[{OptionName=version-
depth,OptionValues=[20]}]' \
        'ResourceType=ssm:Parameter' \
        'ResourceType=imagebuilder:ImageRecipe' \
        'ResourceType=imagebuilder:ContainerRecipe'
```

Di seguito è riportato un output di esempio.

```
{
    "ImageReferences": [
        {
            "ImageId": "ami-0abcdef1234567890",
            "ResourceType": "ec2:Instance",
```

```
            "Arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
        },
        {
            "ImageId": "ami-1234567890abcdef0",
            "ResourceType": "ec2:LaunchTemplate",
            "Arn": "arn:aws:ec2:us-east-1:123456789012:launch-template/
lt-1234567890abcdef0"
        }
    ]
}
```

Per controllare i riferimenti alle AMI per tutti i tipi di risorse supportati

Utilizza il comando describe-image-references con il parametro `--include-all-resource-types`.

```
aws ec2 describe-image-references \
    --image-ids ami-0abcdef1234567890 ami-1234567890abcdef0 \
    --include-all-resource-types
```

Per controllare i riferimenti alle AMI per tutti i tipi di risorse supportati e opzioni specifiche

Utilizza il comando describe-image-references con i parametri `--include-all-resource-types` e `--resource-types`. Questo esempio controlla tutti i tipi di risorse, limitando la risposta alle istanze EC2 in esecuzione o in sospeso.

```
aws ec2 describe-image-references \
    --image-ids ami-0abcdef1234567890 ami-1234567890abcdef0 \
    --include-all-resource-types \
    --resource-types
 'ResourceType=ec2:Instance,ResourceTypeOptions=[{OptionName=state-
name,OptionValues=[running,pending]}]'
```

PowerShell

Per controllare i riferimenti alle AMI per tipi di risorse specifici

Utilizza il Get-EC2ImageReference cmdlet con il parametro. `-ResourceType` Nell'esempio seguente vengono controllate le istanze EC2 (ambito di applicazione in base allo stato dell'istanza), i modelli di avvio (ambito di applicazione alle 20 versioni più recenti dei modelli di avvio) e altri tipi di risorse specifici.

```
Get-EC2ImageReference `
    -ImageId 'ami-0abcdef1234567890', 'ami-1234567890abcdef0' `
    -ResourceType @(
        @{
            ResourceType = 'ec2:Instance'
            ResourceTypeOptions = @(
                @{
                    OptionName = 'state-name'
                    OptionValues = @('running', 'pending')
                }
            )
        },
        @{
            ResourceType = 'ec2:LaunchTemplate'
            ResourceTypeOptions = @(
                @{
                    OptionName = 'version-depth'
                    OptionValues = @('20')
                }
            )
        },
        @{
            ResourceType = 'ssm:Parameter'
        },
        @{
            ResourceType = 'imagebuilder:ImageRecipe'
        },
        @{
            ResourceType = 'imagebuilder:ContainerRecipe'
        }
    )
```

Per controllare i riferimenti alle AMI per tutti i tipi di risorse supportati

Utilizzare il Get-EC2ImageReference cmdlet con il parametro. `-IncludeAllResourceTypes`

```
Get-EC2ImageReference `
    -ImageId 'ami-0abcdef1234567890', 'ami-1234567890abcdef0' `
    -IncludeAllResourceTypes
```

Per controllare i riferimenti alle AMI per tutti i tipi di risorse supportati e opzioni specifiche

Utilizzare il Get-EC2ImageReference cmdlet con entrambi i parametri e. -IncludeAllResourceTypes -ResourceType Questo esempio controlla tutti i tipi di risorse, limitando la risposta alle istanze EC2 in esecuzione o in sospeso.

```
Get-EC2ImageReference `
    -ImageId 'ami-0abcdef1234567890', 'ami-1234567890abcdef0' `
    -IncludeAllResourceTypes `
    -ResourceType @(
        @{
            ResourceType = 'ec2:Instance'
            ResourceTypeOptions = @(
                @{
                    OptionName = 'state-name'
                    OptionValues = @('running', 'pending')
                }
            )
        }
    )
```

Dichiarare un'AMI Amazon EC2 come obsoleta

Puoi dichiarare un'AMI come obsoleta per indicare che non è aggiornata e non deve essere utilizzata. Puoi inoltre specificare una data di definizione come obsoleta futura per un'AMI, indicando da quando l'AMI non sarà più aggiornata. Ad esempio, è possibile dichiarare un'AMI come obsoleta se non è più gestita attivamente oppure se è stata sostituita da una versione più recente. Per impostazione predefinita, le AMI obsolete non vengono visualizzate negli elenchi di AMI, impedendo ai nuovi utenti di utilizzare le AMI non aggiornate. Tuttavia, gli utenti e i servizi di avvio esistenti, come i modelli di avvio e i gruppi Auto Scaling, possono continuare a utilizzare un'AMI obsoleta specificandone l'ID. Per eliminare l'AMI in modo che gli utenti e i servizi non possano più utilizzarla, è necessario annullare la sua registrazione.

Dopo che un'AMI è stata dichiarata obsoleta:

- Per gli utenti AMI, l'AMI obsoleta non viene visualizzata nelle chiamate DescribeImages API a meno che non ne specifichi l'ID o specifichi che devono apparire le AMI obsolete. I proprietari delle AMI continuano a visualizzare AMI obsolete nelle chiamate API. DescribeImages
- Per gli utenti AMI, l'AMI obsoleta non è disponibile per la selezione nella console EC2. Ad esempio, un'AMI obsoleta non viene visualizzata nel catalogo AMI nella procedura guidata di avvio istanze. I proprietari delle AMI continueranno a vedere le AMI obsolete nella console EC2.

- Per gli utenti delle AMI, se si conosce l'ID di un'AMI obsoleta, è possibile continuare ad avviare istanze con l'AMI obsoleta utilizzando l'API, la CLI o gli SDK.
- I servizi di avvio, come i modelli di avvio e i gruppi Auto Scaling, possono continuare a fare riferimento alle AMI obsolete.
- Le istanze EC2 che sono state avviate tramite un'AMI che viene successivamente dichiarata come obsoleta non sono interessate e possono essere arrestate, avviate e riavviate.

È possibile dichiarare obsolete sia le AMI pubbliche che quelle private.

Indice

- Costi
- Considerazioni
- Dichiarazione di un'AMI come obsoleta
- Descrizione di AMI obsolete
- Annulla la dichiarazione dell'AMI come obsoleta

Costi

Quando si dichiara un'AMI obsoleta, l'AMI non viene eliminata. Il proprietario dell'AMI continuerà a pagare gli snapshot dell'AMI. Per interrompere il pagamento per gli snapshot, il proprietario dell'AMI deve eliminare l'AMI annullandone la registrazione.

Considerazioni

- Solo i proprietari dell'AMI possono dichiararla come obsoleta.
- Le AMI non utilizzate di recente per avviare un'istanza potrebbero essere candidate ideali per l'annullamento della registrazione o la dichiarazione come obsolete. Per ulteriori informazioni, consulta the section called "Verifica quando un'AMI è stata utilizzata per l'ultima volta".
- Puoi creare policy EBS-backed AMI di Amazon Data Lifecycle Manager per automatizzare la deprecazione delle AMI. EBS-backed Per ulteriori informazioni, consulta Create AMI lifecycle policies.
- Di default, la data di obsolescenza di tutte le AMI pubbliche è impostata a due anni dalla data di creazione dell'AMI. È possibile impostare la data di obsolescenza prima dei due anni. Per annullare la data di deprecazione o per spostarla ulteriormente a una data successiva, è necessario rendere privata l'AMI solo condividendola con account AWS specifici.

Dichiarazione di un'AMI come obsoleta

È possibile dichiarare un'AMI come obsoleta in una data e un'ora specifiche. Devi possedere l'AMI.

Il limite massimo per la data di obsolescenza è di 10 anni dalla data attuale, tranne per le AMI pubbliche, per cui il limite superiore è 2 anni dalla data di creazione. Non puoi specificare una data passata.

Console

Come dichiarare obsoleta un'AMI in una data specifica

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel navigatore a sinistra, scegli AMIs (AMI).
3. Nella barra del filtro, scegli Owned by me (Di mia proprietà).
4. Seleziona l'AMI, quindi scegli Actions (Operazioni), Manage AMI Deprecation (Gestisci deprecazione AMI). Puoi selezionare più AMI per impostare la stessa data di deprecazione di più AMI contemporaneamente.
5. Seleziona la casella di spunta Abilita e poi inserisci la data e l'ora di deprecazione.
6. Scegli Save (Salva).

AWS CLI

Come dichiarare obsoleta un'AMI in una data specifica

Utilizza il comando enable-image-deprecation. Se si specifica un valore in secondi, Amazon EC2 arrotonda i secondi al minuto più vicino.

```
aws ec2 enable-image-deprecation \
    --image-id ami-0abcdef1234567890 \
    --deprecate-at "2025-04-15T13:17:12.000Z"
```

PowerShell

Come dichiarare obsoleta un'AMI in una data specifica

Utilizza il cmdlet Enable-EC2ImageDeprecation. Se si specifica un valore in secondi, Amazon EC2 arrotonda i secondi al minuto più vicino.

```
Enable-EC2ImageDeprecation `
    -ImageId ami-0abcdef1234567890 `
    -DeprecateAt 2025-04-15T13:17:12.000Z
```

Descrizione di AMI obsolete

Puoi visualizzare la data e l'ora di obsolescenza di un'AMI e filtrare le AMI per data di obsolescenza.

Console

Per visualizzare la data di dichiarazione di un'AMI come obsoleta

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel navigatore a sinistra, scegli AMIs (AMI) e quindi seleziona l'AMI.
3. Controlla il campo Tempo di obsolescenza (se hai selezionato la casella di spunta accanto all'AMI, è posizionata nella scheda Dettagli). Il campo mostra la data e l'ora di deprecazione dell'AMI. Se il campo è vuoto, l'AMI non è deprecata.

Per filtrare le AMI in base alla data di dichiarazione di un'AMI come obsoleta

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel navigatore a sinistra, scegli AMIs (AMI).
3. Dalla barra del filtro, scegli Owned by me (Di mia proprietà) o Private images (Immagini private) (le immagini private includono AMI condivise con te e di tua proprietà).
4. Nella barra Search (Cerca) inserisci **`Deprecation time`** (mentre inserisci le lettere, viene visualizzato il filtro Deprecation time [Tempo di deprecazione]), quindi scegli un operatore, una data e un'ora.

AWS CLI

Quando descrivi tutte le AMI, i risultati dipendono dal fatto che tu sia un utente AMI o il proprietario dell'AMI.

- Utente AMI: per impostazione predefinita, quando descrivi tutte le AMI, vengono escluse le AMI obsolete condivise con te ma non di tua proprietà. Per includere le AMI obsolete nei risultati, specifica l'opzione `--include-deprecated`.

- Proprietario AMI: quando descrivi tutte le AMI, vengono incluse tutte le AMI di tua proprietà, comprese quelle obsolete. Non puoi escludere le AMI obsolete di tua proprietà utilizzando l'opzione `--no-include-deprecated`.

Per includere le AMI obsolete nella descrizione di tutte le AMI per un account

Utilizza il seguente comando describe-images.

```
aws ec2 describe-images
    --owners 123456789012 \
    --include-deprecated
```

Per descrivere le AMI obsolete per il tuo account

Utilizza il seguente comando describe-images.

```
aws ec2 describe-images \
    --owners self \
    --query "Images[?DeprecationTime!=null].ImageId" \
    --output text
```

Di seguito è riportato un output di esempio.

```
ami-0abcdef1234567890
```

Come descrivere la data di dichiarazione di un'AMI come obsoleta

Utilizza il seguente comando describe-images. Se `DeprecationTime` non è presente nell'output, l'AMI non è obsoleta né è stata impostata per diventare obsoleta in futuro.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[].DeprecationTime \
    --output text
```

Di seguito è riportato un output di esempio.

```
2025-05-01T00:00:00.000Z
```

PowerShell

Per elencare le AMI obsolete per il tuo account

Utilizza il cmdlet Get-EC2Image.

```
(Get-EC2Image -Owner self | Where-Object {$_.DeprecationTime -ne $null}).ImageId
```

Di seguito è riportato un output di esempio.

```
ami-0abcdef1234567890
```

Come descrivere la data di dichiarazione di un'AMI come obsoleta

Utilizza il cmdlet Get-EC2Image. Se `DeprecationTime` non è presente nell'output, l'AMI non è obsoleta né è stata impostata per diventare obsoleta in futuro.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).DeprecationTime
```

Di seguito è riportato un output di esempio.

```
2025-05-01T00:00:00.000Z
```

Annulla la dichiarazione dell'AMI come obsoleta

Puoi annullare la dichiarazione di un'AMI come obsoleta e rimuovere così la data e l'ora di obsolescenza. Per eseguire questa procedura, è necessario essere il proprietario dell'AMI.

Console

Come annullare la dichiarazione di un'AMI come obsoleta

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel navigatore a sinistra, scegli AMIs (AMI).
3. Nella barra del filtro, scegli Owned by me (Di mia proprietà).
4. Seleziona l'AMI, quindi scegli Actions (Operazioni), Manage AMI Deprecation (Gestisci deprecazione AMI). Puoi selezionare più AMI per annullare la deprecazione di più AMI contemporaneamente.

5. Deseleziona la casella di spunta Abilita, quindi scegli Salva.

AWS CLI

Come annullare la deprecazione di un'AMI

Utilizza il seguente comando disable-image-deprecation.

```
aws ec2 disable-image-deprecation --image-id ami-0abcdef1234567890
```

PowerShell

Come annullare la deprecazione di un'AMI

Utilizza il cmdlet Disable-EC2ImageDeprecation.

```
Disable-EC2ImageDeprecation -ImageId ami-0abcdef1234567890
```

Disattivare un'AMI Amazon EC2

È possibile disabilitare un'AMI per impedirne l'utilizzo per gli avvii delle istanze. Non è possibile avviare nuove istanze da un'AMI disabilitata. È possibile riabilitare un'AMI disabilitata al fine di utilizzarla nuovamente per gli avvii delle istanze.

È possibile disabilitare sia le AMI pubbliche sia quelle private.

Per ridurre i costi di storage per le EBS-backed AMI disattivate che vengono utilizzate raramente, ma che devono essere conservate a lungo termine, è possibile archiviare le istantanee associate. Per ulteriori informazioni, consulta Snapshot Archive Amazon EBS nella Guida per l'utente di Amazon EBS.

Indice

- Come funziona la disattivazione delle AMI
- Costi
- Prerequisiti
- Autorizzazioni IAM richieste
- Disabilitazione di un'AMI
- Descrizione delle AMI disabilitate

- Re-enable un'AMI disattivata

Come funziona la disattivazione delle AMI

> **Warning**
>
> La disabilitazione di un'AMI rimuove tutte le relative autorizzazioni di avvio.

Quando un'AMI è disabilitata:

- Lo stato dell'AMI cambia in `disabled`.
- Non è possibile condividere un'AMI disabilitata. Se un'AMI in precedenza era pubblica o condivisa, viene resa privata. Se un'AMI è stata condivisa con un' Account AWS organizzazione o un'unità organizzativa, questa perde l'accesso all'AMI disattivata.
- Per impostazione predefinita, un'AMI disabilitata non viene visualizzata nelle chiamate API DescribeImages.
- Un'AMI disabilitata non viene visualizzata nel filtro della console Di mia proprietà. Per trovare le AMI disabilitate, usa il filtro della console Immagini disabilitate.
- Non è possibile selezionare un'AMI disabilitata per gli avvii delle istanze nella console EC2. Ad esempio, un'AMI disabilitata non viene visualizzata nel catalogo AMI nella procedura guidata di avvio delle istanze o durante la creazione di un modello di istanza.
- I servizi di avvio, come i modelli di avvio e i gruppi con dimensionamento automatico, possono continuare a fare riferimento alle AMI obsolete. I successivi avvii delle istanze da un'AMI disattivata avranno esito negativo, quindi consigliamo di aggiornare i modelli di avvio e i gruppi con dimensionamento automatico in modo che facciano riferimento solo alle AMI disponibili.
- Le istanze EC2 che sono state avviate tramite un'AMI che viene successivamente disabilitata non sono interessate e possono essere arrestate, avviate e riavviate.
- Non è possibile eliminare snapshot associati alle AMI disabilitate. Il tentativo di eliminare uno snapshot associato restituisce l'errore `snapshot is currently in use`.

Quando un'AMI viene abilitata nuovamente:

- Lo stato dell'AMI cambia in `available` e può essere utilizzata per avviare le istanze.
- L'AMI può essere condivisa.

- Gli Account AWS, le organizzazioni e le unità organizzative che hanno perso l'accesso all'AMI quando era disabilitata non riottengono automaticamente l'accesso, ma è possibile condividere nuovamente l'AMI con loro.

Costi

Quando si disabilita un'AMI, l'AMI non viene eliminata. Se l'AMI è un' EBS-backed AMI, continui a pagare per le istantanee EBS dell'AMI. Se desideri mantenere l'AMI, potresti essere in grado di ridurre i costi di archiviazione archiviando gli snapshot. Per ulteriori informazioni, consulta Snapshot Archive Amazon EBS nella Guida per l'utente di Amazon EBS. Se non si desidera conservare l'AMI e i relativi snapshot, è necessario annullare la registrazione dell'AMI ed eliminare gli snapshot. Per ulteriori informazioni, consulta Annullare la registrazione di un'AMI.

Prerequisiti

Per disabilitare o riabilitare un'AMI, devi essere il proprietario dell'AMI.

Autorizzazioni IAM richieste

Per disabilitare e riabilitare un'AMI, devi disporre delle seguenti autorizzazioni IAM:

- `ec2:DisableImage`
- `ec2:EnableImage`

Disabilitazione di un'AMI

Puoi disattivare un'AMI utilizzando la console EC2 o (). AWS Command Line Interface AWS CLI Per eseguire questa procedura, è necessario essere il proprietario dell'AMI.

Console

Come disabilitare un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra scegliere AMIs (AMI).
3. Nella barra del filtro, scegli Owned by me (Di mia proprietà).
4. Seleziona l'AMI, quindi scegli Operazioni, Disabilita AMI. È possibile selezionare più AMI per disabilitarle contemporaneamente.

5. Nella finestra Disabilita AMI, scegli Disabilita AMI.

AWS CLI

Disabilitazione di un'AMI

Utilizza il seguente comando disable-image.

```
aws ec2 disable-image --image-id ami-0abcdef1234567890
```

PowerShell

Come disabilitare un'AMI

Utilizza il cmdlet Disable-EC2Image.

```
Disable-EC2Image -ImageId ami-0abcdef1234567890
```

Descrizione delle AMI disabilitate

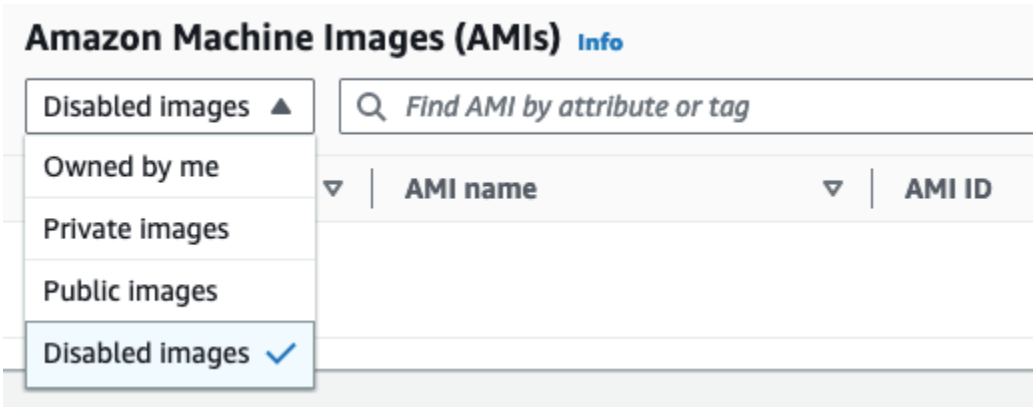
È possibile disabilitare un'AMI utilizzando la console EC2 oppure la AWS CLI.

Devi essere il proprietario delle AMI per visualizzare le AMI disabilitate. Poiché le AMI disabilitate vengono rese private, non puoi visualizzarle se non ne sei il proprietario.

Console

Visualizzazione delle AMI disabilitate

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra scegliere AMIs (AMI).
3. Dalla barra dei filtri, scegli Immagini disabilitate.



AWS CLI

Per impostazione predefinita, quando descrivi tutte le AMI, le AMI disabilitate non vengono visualizzate nei risultati. Per includere le AMI disabilitate nei risultati, specifica l'opzione `--include-disabled`. Il campo `State` per un'AMI è `disabled` se l'AMI è disabilitata.

Per includere le AMI disabilitate nella descrizione di tutte le AMI per un account

Utilizza il seguente comando describe-images.

```
aws ec2 describe-images \
    --owners 123456789012 \
    --include-disabled
```

Per fare un elenco delle AMI disabilitate per il tuo account

Utilizza il seguente comando describe-images.

```
aws ec2 describe-images \
    --owners self \
    --include-disabled \
    --filters Name=state,Values=disabled \
    --query Images[].ImageId \
    --output text
```

Di seguito è riportato un output di esempio.

```
ami-0abcdef1234567890
```

Per descrivere lo stato di un'AMI

Utilizza il seguente comando describe-images. Se `DeprecationTime` non è presente nell'output, l'AMI non è obsoleta né è stata impostata per diventare obsoleta in futuro.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[].State \
    --output text
```

Di seguito è riportato un output di esempio.

```
disabled
```

PowerShell

Per impostazione predefinita, quando descrivi tutte le AMI, le AMI disabilitate non vengono visualizzate nei risultati. Per includere le AMI disabilitate nei risultati, specifica il parametro `-IncludeDisabled`. Il campo `State` per un'AMI è `disabled` se l'AMI è disabilitata.

Per fare un elenco delle AMI disabilitate per il tuo account

Utilizza il cmdlet Get-EC2Image.

```
(Get-EC2Image `
    -Owner self `
    -IncludeDisabled $true | Where-Object {$_.State -eq "disabled"}).ImageId
```

Di seguito è riportato un output di esempio.

```
ami-0abcdef1234567890
```

Per descrivere lo stato di un'AMI

Utilizza il cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).State.Value
```

Di seguito è riportato un output di esempio.

```
disabled
```

Re-enable un'AMI disattivata

È possibile abilitare nuovamente un'AMI disabilitata. Per eseguire questa procedura, è necessario essere il proprietario dell'AMI.

Console

Riabilitazione di un'AMI disabilitata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra scegliere AMIs (AMI).
3. Dalla barra dei filtri, scegli Immagini disabilitate.
4. Seleziona l'AMI, quindi scegli Operazioni, Abilita AMI. È possibile selezionare più AMI per riabilitarle contemporaneamente.
5. Nella finestra Abilita AMI, scegli Abilita.

AWS CLI

Riabilitazione di un'AMI disabilitata

Utilizza il seguente comando enable-image.

```
aws ec2 enable-image --image-id ami-0abcdef1234567890
```

PowerShell

Riabilitazione di un'AMI disabilitata

Utilizza il cmdlet Enable-EC2Image.

```
Enable-EC2Image -ImageId ami-0abcdef1234567890
```

Annullare la registrazione di un'AMI Amazon EC2

Quando annulli la registrazione di un'AMI, Amazon EC2 la elimina definitivamente. Dopo aver annullato la registrazione di un'AMI, non puoi più utilizzarla per avviare nuove istanze. Potresti considerare di annullare la registrazione di un'AMI quando hai terminato di utilizzarla.

Per proteggerti dall'annullamento accidentale o dannoso della registrazione di un'AMI, puoi attivare la protezione dall'annullamento della registrazione. Se annulli accidentalmente la registrazione di un' EBS-backed AMI, puoi utilizzare il Cestino per ripristinarla solo se la ripristini entro il periodo di tempo consentito prima che venga eliminata definitivamente.

Quando annulli la registrazione di un'AMI, allo stesso tempo puoi facoltativamente eliminare gli snapshot associati. Tuttavia, se uno snapshot è associato a più AMI, non verrà eliminato anche se specificato per l'eliminazione, ma l'AMI verrà comunque annullata. Qualsiasi snapshot non eliminato continuerà a sostenere i costi di archiviazione.

L'annullamento della registrazione di un'AMI non ha ripercussioni sulle istanze avviate dall'AMI. Puoi continuare a utilizzare queste istanze. Per impostazione predefinita, l'annullamento della registrazione di un'AMI non ha inoltre alcun effetto sugli snapshot creati durante il processo di creazione dell'AMI. Continuerai a sostenere i costi di utilizzo per tali istanze e i costi di archiviazione per gli snapshot. Pertanto, per evitare di incorrere in costi inutili, consigliamo di terminare tutte le istanze ed eliminare tutti gli snapshot non necessari. Puoi eliminare gli snapshot automaticamente durante l'annullamento della registrazione o manualmente dopo la stessa. Per ulteriori informazioni, consulta Evita i costi derivanti da risorse non utilizzate.

Per le istanze avviate da un'AMI che viene successivamente annullata, è comunque possibile visualizzare alcune informazioni di alto livello sull'AMI utilizzando il comando. `describe-instance-image-metadata` AWS CLI Per ulteriori informazioni, consulta describe-instance-image-metadata.

Indice

- Considerazioni
- Annullare la registrazione di un'AMI
- Evita i costi derivanti da risorse non utilizzate
- Proteggere un'AMI Amazon EC2 dall'annullamento della registrazione

Considerazioni

- Non è possibile annullare la registrazione di un'AMI che non è di proprietà dell'account.
- Non è possibile utilizzare Amazon EC2 per annullare la registrazione di un'AMI gestita dal servizio. AWS Backup Utilizzalo invece AWS Backup per eliminare i punti di ripristino corrispondenti nel vault di backup. Per ulteriori informazioni, consulta la sezione Eliminazione dei backup nella Guida per gli sviluppatori di AWS Backup .

Annullare la registrazione di un'AMI

Puoi annullare la registrazione delle AMI e delle EBS-backed AMI Amazon. S3-backed Per le EBS-backed AMI, puoi opzionalmente eliminare contemporaneamente le istantanee associate. Tuttavia, se uno snapshot è associato ad altre AMI, non verrà eliminato anche se specificato per l'eliminazione.

Console

Come annullare la registrazione di un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Dalla barra dei filtri, scegliere Di mia proprietà per un elenco delle AMI disponibili, oppure scegliere Immagini disabilitate per un elenco delle AMI disabilitate.
4. Selezionare l'AMI di cui annullare la registrazione.
5. Scegli Actions (Operazioni), quindi Deregister AMI (Annulla registrazione AMI).
6. (Facoltativo) Per eliminare gli snapshot associati durante l'annullamento della registrazione, seleziona la casella di controllo Elimina gli snapshot associati.

   > **Note**
   >
   > Se uno snapshot è associato ad altre AMI, non viene eliminato, anche se la casella di controllo è selezionata.

7. Scegli Annulla registrazione AMI.

   Potrebbero essere necessari alcuni minuti prima che la console rimuova l'AMI dall'elenco. Scegliere Refresh (Aggiorna) per aggiornare lo stato.

AWS CLI

Come annullare la registrazione di un'AMI

Utilizza il seguente comando deregister-image.

```
aws ec2 deregister-image --image-id ami-0abcdef1234567890
```

Per annullare la registrazione di un'AMI ed eliminare gli snapshot associati

Utilizza il seguente comando deregister-image e specifica il parametro `--delete-associated-snapshots`. Nota che se uno snapshot è associato ad altre AMI, non viene eliminato, anche se specifichi questo parametro.

```
aws ec2 deregister-image \
    --image-id ami-0abcdef1234567890 \
    --delete-associated-snapshots
```

PowerShell

Come annullare la registrazione di un'AMI

Utilizza il cmdlet Unregister-EC2Image.

```
Unregister-EC2Image -ImageId ami-0abcdef1234567890
```

Per annullare la registrazione di un'AMI ed eliminare gli snapshot associati

Utilizzare il Unregister-EC2Image cmdlet e specificare il parametro. `-DeleteAssociatedSnapshots` Nota che se uno snapshot è associato ad altre AMI, non viene eliminato, anche se specifichi questo parametro.

```
Unregister-EC2Image `
    -ImageId ami-0abcdef1234567890 `
    -DeleteAssociatedSnapshots
```

Evita i costi derivanti da risorse non utilizzate

Annullare la registrazione di un'AMI non comporta, per impostazione predefinita, l'eliminazione di tutte le risorse associate a tale AMI. Queste risorse includono le istantanee per le EBS-backed AMI e i file in Amazon S3 per le AMI Amazon. S3-backed Quando annulli la registrazione di un'AMI, inoltre, non termini o arresti le istanze avviate da tale AMI.

Continuerai a sostenere i costi per l'archiviazione degli snapshot e dei file, e sosterrai i costi per tutte le istanze in esecuzione.

Per evitare di incorrere in questi tipi di costi non necessari, consigliamo di eliminare tutte le risorse non necessarie.

EBS-backed AMI

- Elimina gli snapshot associati durante l'annullamento della registrazione dell'AMI. Per ulteriori informazioni, consulta Annullare la registrazione di un'AMI.
- Se annulli la registrazione di un'AMI senza eliminare gli snapshot associati, puoi eliminare gli snapshot manualmente. Lo snapshot del volume root dell'istanza creato durante la creazione dell'AMI ha il seguente formato di descrizione:

```
Created by CreateImage(i-1234567890abcdef0) for ami-0abcdef1234567890
```

- Se non hai più bisogno delle istanze avviate dall'AMI, puoi arrestarle o terminarle. Per elencare le istanze, filtra in base all'ID dell'AMI.

AMI Amazon S3-backed

- Elimina il bundle in Amazon S3 utilizzando il comando ec2-delete-bundle (strumenti AMI).
- Se il bucket Amazon S3 è vuoto dopo aver eliminato il bundle e non hai più bisogno di quel bucket, puoi eliminare il bucket.
- Se non hai più bisogno delle istanze avviate dall'AMI, puoi terminarle. Per elencare le istanze, filtra in base all'ID dell'AMI.

Proteggere un'AMI Amazon EC2 dall'annullamento della registrazione

Puoi attivare la protezione dall'annullamento della registrazione su un'AMI per impedirne l'eliminazione accidentale o dannosa. Quando attivi la protezione dall'annullamento della registrazione, la registrazione dell'AMI non può essere annullata da nessun utente, indipendentemente dalle autorizzazioni IAM di cui dispone. Se desideri annullare la registrazione dell'AMI, devi prima disattivare la protezione dall'annullamento della registrazione su di essa.

Quando attivi la protezione dall'annullamento della registrazione su un'AMI, hai la possibilità di includere un tempo di raffreddamento di 24 ore. Questo tempo di raffreddamento è il periodo durante il quale la protezione dall'annullamento della registrazione rimane attiva dopo la sua disattivazione. Durante questo tempo di raffreddamento, non è possibile annullare la registrazione dell'AMI. Al termine del tempo di raffreddamento, la registrazione dell'AMI può essere annullata.

La protezione dall'annullamento della registrazione viene disattivata di default in tutte le AMI esistenti e nuove.

Attivare la protezione dall'annullamento della registrazione

Per attivare la protezione dall'annullamento della registrazione, usa le procedure seguenti.

Console

Per attivare la protezione dall'annullamento della registrazione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Dalla barra dei filtri, scegliere Di mia proprietà per un elenco delle AMI disponibili, oppure scegliere Immagini disabilitate per un elenco delle AMI disabilitate.
4. Seleziona l'AMI su cui desideri attivare la protezione dall'annullamento della registrazione, poi scegli Operazioni, Gestisci la protezione dall'annullamento della registrazione cancellazione dell'AMI.
5. Nella finestra di dialogo Gestisci la protezione dall'annullamento della registrazione dell'AMI, puoi attivare la protezione dall'annullamento della registrazione con o senza un tempo di raffreddamento. Scegli una delle seguenti opzioni:
   - Abilita con un tempo di raffreddamento di 24 ore: con un tempo di raffreddamento, la registrazione dell'AMI non può essere annullata per 24 ore quando la protezione dall'annullamento della registrazione viene disattivata.
   - Abilita senza tempo di raffreddamento: senza tempo di attesa, la registrazione dell'AMI può essere annullata immediatamente quando la protezione dall'annullamento della registrazione viene disattivata.
6. Scegli Save (Salva).

AWS CLI

Per attivare la protezione dall'annullamento della registrazione

Utilizza il comando enable-image-deregistration-protection. Per abilitare il tempo di raffreddamento facoltativo, includi l'opzione `--with-cooldown`.

```
aws ec2 enable-image-deregistration-protection \
    --image-id ami-0abcdef1234567890 \
    --with-cooldown
```

PowerShell

Per attivare la protezione dall'annullamento della registrazione

Utilizza il cmdlet Enable-EC2ImageDeregistrationProtection. Per abilitare il tempo di raffreddamento facoltativo, imposta il parametro `-WithCooldown` su `true`.

```
Enable-EC2ImageDeregistrationProtection `
    -ImageId ami-0abcdef1234567890 `
    -WithCooldown $true
```

Disattivare la protezione dall'annullamento della registrazione

Per disattivare la protezione dall'annullamento della registrazione, usa le procedure seguenti.

Se hai scelto di includere un tempo di raffreddamento di 24 ore quando hai attivato la protezione dall'annullamento della registrazione per l'AMI, quando disattivi la protezione dall'annullamento della registrazione, non potrai annullare immediatamente la registrazione dell'AMI. Il tempo di raffreddamento è il periodo di 24 ore durante il quale la protezione dall'annullamento della registrazione rimane attiva dopo la sua disattivazione. Durante questo tempo di raffreddamento, non è possibile annullare la registrazione dell'AMI. Dopo il termine del tempo di raffreddamento, la registrazione dell'AMI può essere annullata.

Console

Per disattivare la protezione dall'annullamento della registrazione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Dalla barra dei filtri, scegliere Di mia proprietà per un elenco delle AMI disponibili, oppure scegliere Immagini disabilitate per un elenco delle AMI disabilitate.
4. Seleziona l'AMI di cui disattivare la protezione dall'annullamento della registrazione, poi scegli Operazioni, Gestisci la protezione dall'annullamento della registrazione cancellazione dell'AMI.
5. Nella finestra di dialogo Gestisci la protezione dall'annullamento della registrazione dell'AMI, scegli Disabilita.
6. Scegli Save (Salva).

AWS CLI

Per disattivare la protezione dall'annullamento della registrazione

Utilizza il comando disable-image-deregistration-protection.

```
aws ec2 disable-image-deregistration-protection --image-id ami-0abcdef1234567890
```

PowerShell

Per disattivare la protezione dall'annullamento della registrazione

Utilizza il cmdlet Disable-EC2ImageDeregistrationProtection.

```
Disable-EC2ImageDeregistrationProtection -ImageId ami-0abcdef1234567890
```

Comportamento di avvio delle istanze con le modalità di avvio di Amazon EC2

All'avvio di un computer, il primo software in esecuzione è responsabile dell'inizializzazione della piattaforma e fornisce un'interfaccia al sistema operativo per eseguire operazioni specifiche della piattaforma.

Amazon EC2 supporta due varianti del software in modalità di avvio: Unified Extensible Firmware Interface (UEFI) e BIOS legacy.

Possibili parametri della modalità di avvio su un'AMI

Un'AMI può avere uno dei seguenti valori per i parametri della modalità di avvio: `uefi`, `legacy-bios` o `uefi-preferred`. Il parametro della modalità di avvio dell'AMI è facoltativo. Le istanze avviate da AMI che non dispongono di parametri della modalità di avvio utilizzano il valore predefinito del tipo di istanza.

Scopo del parametro della modalità di avvio dell'AMI

Il parametro della modalità di avvio dell'AMI segnala ad Amazon EC2 quale modalità di avvio utilizzare quando si avvia un'istanza. Quando il parametro della modalità di avvio è impostato su `uefi`, EC2 tenta di avviare l'istanza su UEFI. Se il sistema operativo non è configurato per supportare UEFI, l'avvio dell'istanza avrà esito negativo.

Parametro della modalità di avvio UEFI Preferred

Con il parametro della modalità di avvio `uefi-preferred`, puoi creare AMI che supportano sia la variante UEFI che BIOS legacy. Se il parametro della modalità di avvio è impostato su `uefi-preferred` e se il tipo di istanza supporta UEFI, l'istanza viene avviata su UEFI. Se il tipo di istanza non supporta UEFI, l'istanza viene avviata su BIOS legacy.

> **Warning**
>
> Alcune funzionalità, ad esempio l'avvio protetto UEFI, sono disponibili solo per le istanze con modalità di avvio UEFI. Quando si utilizza il parametro `uefi-preferred` AMI boot mode con un tipo di istanza che non supporta UEFI, l'istanza verrà avviata come Legacy BIOS e la UEFI-dependent funzionalità verrà disabilitata. Se ti affidi alla disponibilità di una UEFI-dependent funzionalità, imposta il parametro della modalità di avvio AMI su`uefi`.

Modalità di avvio predefinite per tipi di istanza

- Tipi di istanza Graviton: UEFI
- Tipi di istanze Intel e AMD: BIOS Legacy

Supporto di zona

L'avvio UEFI non è supportato nelle zone Wavelength.

Argomenti della modalità avvio

- Requisiti per lanciare un'istanza EC2 in modalità di avvio UEFI
- Determinare il parametro della modalità di avvio di un'AMI di Amazon EC2
- Determinare le modalità di avvio supportate di un tipo di istanza EC2
- Determinare la modalità di avvio di un'istanza EC2
- Determinare la modalità di avvio del sistema operativo per l'istanza EC2
- Impostare la modalità di avvio di un'AMI Amazon EC2
- Variabili UEFI per istanze Amazon EC2
- UEFI Secure Boot per istanze Amazon EC2

Requisiti per lanciare un'istanza EC2 in modalità di avvio UEFI

La modalità di avvio di un'istanza è determinata dalla configurazione dell'AMI, dal sistema operativo in essa contenuto e dal tipo di istanza. Per lanciare un'istanza in modalità di avvio UEFI, è necessario soddisfare i seguenti requisiti.

AMI

L'AMI deve essere configurata per l'UEFI nel modo seguente:

- Sistema operativo: il sistema operativo contenuto nell'AMI deve essere configurato per utilizzare UEFI; in caso contrario, l'avvio dell'istanza avrà esito negativo. Per ulteriori informazioni, consulta Determinare la modalità di avvio del sistema operativo per l'istanza EC2.
- Parametro della modalità di avvio dell'AMI: il parametro della modalità di avvio dell'AMI deve essere impostato su `uefi` o `uefi-preferred`. Per ulteriori informazioni, consulta Determinare il parametro della modalità di avvio di un'AMI di Amazon EC2.

Linux – Le seguenti AMI di Linux supportano UEFI:

- Amazon Linux 2023
- Amazon Linux 2 (solo tipi di istanze Graviton)

Per altre AMI Linux, devi configurare l'AMI, importare l'AMI tramite VM Import/Export o importare l'AMI tramite. CloudEndure

Windows – Le seguenti AMI Windows supportano UEFI:

- Windows_Server-2025-* (ad eccezione delle AMI con il prefisso del nome) `BIOS-`
- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base
- TPM-Windows_Server-2016-English-Core-Base

Tipo di istanza

Tutte le istanze basate sul sistema AWS Nitro supportano sia UEFI che Legacy BIOS, ad eccezione delle seguenti: istanze bare metal, DL1, G4ad, P4, u-3tb1, u-6tb1, u-9tb1, u-12tb1, u-18tb1, u-18tb1, u-24tb1 e VT1. Per ulteriori informazioni, consulta the section called “Modalità di avvio del tipo di istanza”.

La tabella seguente mostra che la modalità di avvio di un'istanza (indicata dalla colonna Modalità di avvio dell'istanza risultante) è determinata dalla combinazione del parametro della modalità di avvio dell'AMI (colonna 1), della configurazione della modalità di avvio del sistema operativo contenuto nell'AMI (colonna 2) e del supporto della modalità di avvio del tipo di istanza (colonna 3).

Parametro della modalità di avvio dell'AMI	Configurazione della modalità di avvio del sistema operativo	Supporto della modalità di avvio del tipo di istanza	Modalità di avvio dell'istanza risultante
UEFI	UEFI	UEFI	UEFI
BIOS legacy	BIOS legacy	BIOS legacy	BIOS legacy
UEFI Preferred	UEFI	UEFI	UEFI
UEFI Preferred	UEFI	UEFI e BIOS legacy	UEFI
UEFI Preferred	BIOS legacy	BIOS legacy	BIOS legacy
UEFI Preferred	BIOS legacy	UEFI e BIOS legacy	BIOS legacy
Nessuna modalità di avvio specificata - ARM	UEFI	UEFI	UEFI
Nessuna modalità di avvio specificata - x86	BIOS legacy	UEFI e BIOS legacy	BIOS legacy

Determinare il parametro della modalità di avvio di un'AMI di Amazon EC2

Il parametro della modalità di avvio dell'AMI è facoltativo. Un'AMI può avere uno dei seguenti valori per i parametri della modalità di avvio: `uefi`, `legacy-bios` o `uefi-preferred`.

Alcune AMI non dispongono di parametri della modalità di avvio. Quando un'AMI non dispone di parametri della modalità di avvio, le istanze avviate da tale AMI utilizzano il valore predefinito del tipo di istanza, vale a dire `uefi` su Graviton, e `legacy-bios` sui tipi di istanza Intel e AMD.

Console

Per determinare il parametro della modalità di avvio di un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli AMI, e quindi seleziona l'AMI.
3. Ispeziona il campo Modalità di avvio.
   - Il valore uefi indica che l'AMI supporta UEFI.
   - Il valore uefi-preferred indica che l'AMI supporta sia UEFI sia BIOS legacy.
   - Se non è presente un valore, le istanze avviate dall'AMI utilizzano il valore predefinito del tipo di istanza.

Per determinare il parametro della modalità di avvio di un'AMI all'avvio di un'istanza

Quando si avvia un'istanza utilizzando la procedura guidata di avvio dell'istanza, nella fase di selezione dell'AMI, controlla il campo Boot mode (Modalità di avvio). Per ulteriori informazioni, consulta Immagini di applicazioni e sistema operativo (Amazon Machine Image).

AWS CLI

Per determinare il parametro della modalità di avvio di un'AMI

Utilizza il comando describe-images per determinare la modalità di avvio di un'AMI.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-id ami-0abcdef1234567890 \
    --query Images[].BootMode \
    --output text
```

Di seguito è riportato un output di esempio.

```
uefi
```

Nell'output, il valore `uefi` indica che l'AMI supporta UEFI. Il valore `uefi-preferred` indica che l'AMI supporta sia UEFI che BIOS legacy. Se non è presente un valore, le istanze avviate dall'AMI utilizzano il valore predefinito del tipo di istanza.

PowerShell

Per determinare il parametro della modalità di avvio di un'AMI

Utilizza il cmdlet Get-EC2Image per determinare la modalità di avvio di un'AMI.

```
Get-EC2Image -Region us-east-1 `
    -ImageId ami-0abcdef1234567890 | Format-List Name, BootMode, TpmSupport
```

Di seguito è riportato un output di esempio.

```
Name       : TPM-Windows_Server-2016-English-Full-Base-2023.05.10
BootMode   : uefi
TpmSupport : v2.0
```

Nell'output, il valore `BootMode` indica la modalità di avvio dell'AMI. Il valore `uefi` indica che l'AMI supporta UEFI. Il valore `uefi-preferred` indica che l'AMI supporta sia UEFI che BIOS legacy. Se non è presente un valore, le istanze avviate dall'AMI utilizzano il valore predefinito del tipo di istanza.

Determinare le modalità di avvio supportate di un tipo di istanza EC2

Puoi determinare le modalità di avvio supportate di un tipo di istanza.

La console Amazon EC2 non mostra le modalità di avvio supportate da un tipo di istanza.

AWS CLI

Utilizza il comando describe-instance-types per determinare le modalità di avvio supportate di un tipo di istanza. Il parametro `--query` filtra l'output per riportare solo le modalità di avvio supportate.

L'esempio seguente mostra che il tipo di istanza specificato supporta entrambe le modalità di avvio UEFI e Legacy BIOS.

```
aws ec2 describe-instance-types \
    --instance-types m5.2xlarge \
    --query "InstanceTypes[*].SupportedBootModes"
```

Di seguito è riportato un output di esempio.

```
[
    [
        "legacy-bios",
        "uefi"
    ]
]
```

L'esempio seguente mostra che `t2.xlarge` supporta solo BIOS Legacy.

```
aws ec2 describe-instance-types \
    --instance-types t2.xlarge \
    --query "InstanceTypes[*].SupportedBootModes"
```

Di seguito è riportato un output di esempio.

```
[
    [
        "legacy-bios"
    ]
]
```

PowerShell

Utilizza il cmdlet Get-EC2InstanceType per determinare le modalità di avvio supportate di un tipo di istanza.

L'esempio seguente mostra che `m5.2xlarge` supporta entrambe le modalità di avvio UEFI e BIOS Legacy.

```
Get-EC2InstanceType -InstanceType m5.2xlarge | Format-List InstanceType,
 SupportedBootModes
```

Di seguito è riportato un output di esempio.

```
InstanceType       : m5.2xlarge
SupportedBootModes : {legacy-bios, uefi}
```

L'esempio seguente mostra che `t2.xlarge` supporta solo BIOS Legacy.

```
Get-EC2InstanceType -InstanceType t2.xlarge | Format-List InstanceType,
 SupportedBootModes
```

Di seguito è riportato un output di esempio.

```
InstanceType       : t2.xlarge
SupportedBootModes : {legacy-bios}
```

Per determinare i tipi di istanza che supportano UEFI

Puoi determinare i tipi di istanza che supportano UEFI. La console Amazon EC2 non mostra il supporto UEFI di un tipo di istanza.

AWS CLI

I tipi di istanza disponibili variano in base alla Regione AWS. Per visualizzare i tipi di istanza disponibili che supportano UEFI in una regione, utilizza il comando describe-instance-types. Includi il parametro `--filters` per assegnare i risultati ai tipi di istanza che supportano UEFI e il parametro `--query` per assegnare l'output al valore di `InstanceType`.

```
aws ec2 describe-instance-types \
    --filters Name=supported-boot-mode,Values=uefi \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

I tipi di istanza disponibili variano in base alla Regione AWS. Per vedere i tipi di istanza disponibili che supportano Get-EC2InstanceType l'UEFI in una regione, usa il cmdlet.

```
Get-EC2InstanceType -Filter @{Name="supported-boot-mode"; Values="uefi"} |
 Sort-Object @{E={$_.ProcessorInfo.SupportedArchitectures}}, InstanceType |
 Format-Table InstanceType, SupportedBootModes, `
      @{Name="SupportedArchitectures"; E={$_.ProcessorInfo.SupportedArchitectures}}
```

Per determinare i tipi di istanza che supportano UEFI Secure Boot e mantengono le variabili non volatili

Le istanze bare metal non supportano UEFI Secure Boot e le variabili non volatili, quindi questi esempi le escludono dall'output. Per informazioni su UEFI Secure Boot, consulta UEFI Secure Boot per istanze Amazon EC2..

AWS CLI

Utilizza il comando describe-instance-types ed escludi le istanze bare metal dall'output.

```
aws ec2 describe-instance-types \
    --filters Name=supported-boot-mode,Values=uefi Name=bare-metal,Values=false \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Utilizza il Get-EC2InstanceType cmdlet ed escludi le istanze bare metal dall'output.

```
Get-EC2InstanceType -Filter `
      @{Name="supported-boot-mode"; Values="uefi"}, `
      @{Name="bare-metal"; Values="false"} |
 Sort-Object @{E={$_.ProcessorInfo.SupportedArchitectures}}, InstanceType |
 Format-Table InstanceType, SupportedBootModes, `
      @{Name="SupportedArchitectures"; E={$_.ProcessorInfo.SupportedArchitectures}}
```

Determinare la modalità di avvio di un'istanza EC2

La modalità di avvio di un'istanza viene visualizzata nel campo Modalità di avvio della console Amazon EC2 e dal parametro `currentInstanceBootMode` nella AWS CLI.

Quando viene avviata un'istanza, il valore per il parametro della modalità di avvio è determinato dal valore del parametro della modalità di avvio dell'AMI utilizzata per avviarla, come segue:

- Un'AMI con un parametro della modalità di avvio di `uefi` crea un'istanza con un parametro `currentInstanceBootMode` di `uefi`.
- Un'AMI con un parametro della modalità di avvio di `legacy-bios` crea un'istanza con un parametro `currentInstanceBootMode` di `legacy-bios`.
- Un'AMI con un parametro della modalità di avvio di `uefi-preferred` crea un'istanza con un parametro`currentInstanceBootMode` di `uefi` se il tipo di istanza supporta UEFI. In caso contrario, crea un'istanza con un parametro `currentInstanceBootMode` di `legacy-bios`.

- Un'AMI senza alcun valore per il parametro della modalità di avvio crea un'istanza con un parametro `currentInstanceBootMode` che dipende dal fatto che l'architettura AMI sia ARM o x86 e dalla modalità di avvio supportata del tipo di istanza. La modalità di avvio predefinita è `uefi` su istanze Graviton e `legacy-bios` su tipi di istanza Intel e AMD.

Console

Per determinare la modalità di avvio di un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e seleziona l'istanza desiderata.
3. Nella scheda Details (Dettagli) controlla il campo Boot mode (Modalità di avvio).

AWS CLI

Per determinare la modalità di avvio di un'istanza

Utilizza il comando describe-instances per determinare la modalità di avvio di un'istanza. Puoi inoltre determinare la modalità di avvio dell'AMI utilizzata per creare l'istanza.

```
aws ec2 describe-instances \
    --region us-east-1 \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].BootMode \
    --output text
```

Di seguito è riportato un output di esempio.

```
uefi
```

PowerShell

Per determinare la modalità di avvio di un'istanza

Utilizza il cmdlet Get-EC2Image per determinare la modalità di avvio di un'istanza. Puoi inoltre determinare la modalità di avvio dell'AMI utilizzata per creare l'istanza.

```
(Get-EC2Instance `
```

```
    -InstanceId i-1234567890abcdef0).Instances | Format-List BootMode,
 CurrentInstanceBootMode, InstanceType, ImageId
```

Di seguito è riportato un output di esempio.

```
BootMode                : uefi
CurrentInstanceBootMode : uefi
InstanceType            : c5a.large
ImageId                 : ami-0abcdef1234567890
```

Determinare la modalità di avvio del sistema operativo per l'istanza EC2

La modalità di avvio dell'AMI indica ad Amazon EC2 quale modalità di avvio utilizzare per avviare un'istanza. Per verificare se il sistema operativo dell'istanza è configurato per UEFI, devi connetterti all'istanza tramite SSH (istanze Linux) o RDP (istanze Windows).

Consulta le istruzioni relative al sistema operativo della tua istanza.

Linux

Per determinare la modalità di avvio del sistema operativo dell'istanza

1. Connettiti alla tua istanza Linux usando SSH.
2. Per visualizzare la modalità di avvio del sistema operativo, prova una delle seguenti operazioni:

   - Eseguire il seguente comando seguente.

     ```
     [ec2-user ~]$ sudo /usr/sbin/efibootmgr
     ```

     Output previsto da un'istanza avviata in modalità di avvio UEFI

     ```
     BootCurrent: 0001
     Timeout: 0 seconds
     BootOrder: 0000,0001
     Boot0000* UiApp
     Boot0001* UEFI Amazon Elastic Block Store vol-xyz
     ```

   - Esegui il comando seguente per verificare l'esistenza della directory `/sys/firmware/efi`. Questa directory esiste solo se l'istanza viene avviata utilizzando UEFI. Se la directory non esiste, il comando restituisce `Legacy BIOS Boot Detected`.

```
[ec2-user ~]$ [ -d /sys/firmware/efi ] && echo "UEFI Boot Detected" || echo
 "Legacy BIOS Boot Detected"
```

Output previsto da un'istanza avviata in modalità di avvio UEFI

```
UEFI Boot Detected
```

Output previsto da un'istanza avviata in modalità di avvio BIOS Legacy

```
Legacy BIOS Boot Detected
```

- Esegui il comando seguente per verificare che EFI venga visualizzata nell'output `dmesg`.

```
[ec2-user ~]$ dmesg | grep -i "EFI"
```

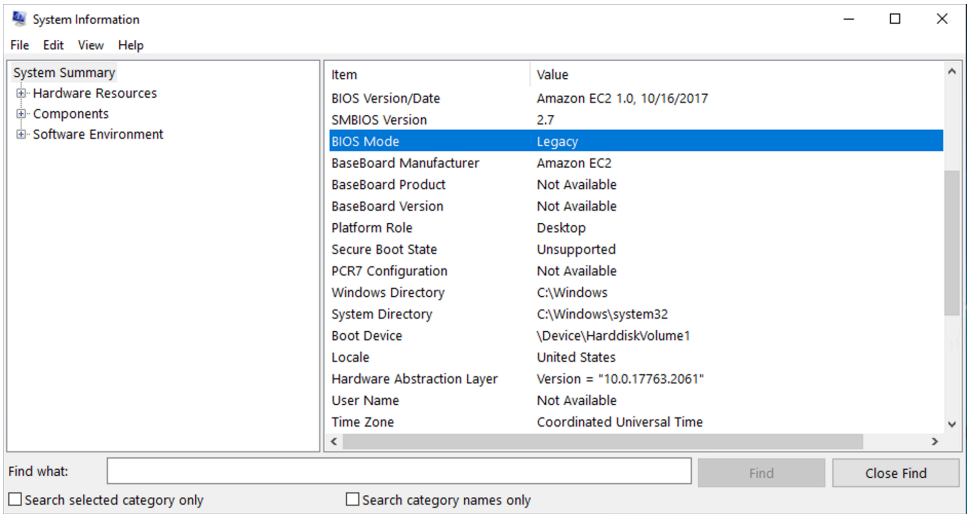
Output previsto da un'istanza avviata in modalità di avvio UEFI

```
[    0.000000] efi: Getting EFI parameters from FDT:
[    0.000000] efi: EFI v2.70 by EDK II
```

Windows

Per determinare la modalità di avvio del sistema operativo dell'istanza

1. Connettiti all'istanza Windows utilizzando RDP.
2. Vai a System Information (Informazioni di sistema) e controlla la riga BIOS Mode (Modalità BIOS).



Impostare la modalità di avvio di un'AMI Amazon EC2

Per impostazione predefinita, un'AMI eredita la modalità di avvio dell'istanza EC2 utilizzata per creare l'AMI. Ad esempio, se crei un'AMI da un'istanza EC2 in esecuzione su BIOS legacy, la modalità di avvio della nuova AMI è `legacy-bios`. Se crei un'AMI da un'istanza EC2 con modalità di avvio `uefi-preferred`, la modalità di avvio della nuova AMI sarà `uefi-preferred`.

Quando registri un'AMI, puoi impostare la modalità di avvio dell'AMI su `uefi`, `legacy-bios` o `uefi-preferred`.

Quando la modalità di avvio dell'AMI è impostata su `uefi-preferred`, l'istanza si avvia come segue:

- Per i tipi di istanza che supportano sia UEFI che BIOS legacy (ad esempio `m5.large`), l'istanza si avvia utilizzando UEFI.
- Per i tipi di istanza che supportano solo BIOS legacy (ad esempio `m4.large`), l'istanza si avvia utilizzando tale modalità.

Se imposti la modalità di avvio dell'AMI su `uefi-preferred`, il sistema operativo deve essere in grado di supportare sia la modalità UEFI che BIOS legacy.

Per convertire un' BIOS-based istanza Legacy esistente in UEFI o un' UEFI-basedistanza esistente in Legacy BIOS, devi prima modificare il volume e il sistema operativo dell'istanza per supportare la modalità di avvio selezionata. Creare quindi uno snapshot del volume. Infine, crea un'AMI dallo snapshot

Considerazioni

- L'impostazione del parametro della modalità di avvio dell'AMI non configura automaticamente il sistema operativo per la modalità di avvio specificata. Devi prima apportare le modifiche adeguate al volume e al sistema operativo dell'istanza per supportare l'avvio tramite la modalità di avvio selezionata. Altrimenti, l'AMI risultante non è utilizzabile. Ad esempio, se stai convertendo un'istanza BIOS-based Windows legacy in UEFI, puoi utilizzare lo strumento MBR2GPT di Microsoft per convertire il disco di sistema da MBR a GPT. Le modifiche necessarie sono specifiche del sistema operativo. Per ulteriori informazioni, consulta il manuale del sistema operativo in uso.
- Non puoi utilizzare il comando register-image o il cmdlet Register-EC2Image per creare un'AMI che supporti sia NitroTPM che UEFI Preferred.
- Alcune funzionalità, ad esempio l'avvio protetto UEFI, sono disponibili solo per le istanze con modalità di avvio UEFI. Quando si utilizza il parametro `uefi-preferred` AMI boot mode con un tipo di istanza che non supporta UEFI, l'istanza viene avviata come Legacy BIOS e la funzionalità è disabilitata. UEFI-dependent Se ti affidi alla disponibilità di una UEFI-dependent funzionalità, imposta il parametro della modalità di avvio AMI su. `uefi`

AWS CLI

Per impostare la modalità di avvio di un'AMI

1. Apporta le modifiche appropriate al volume e al sistema operativo dell'istanza per supportare l'avvio utilizzando la modalità di avvio selezionata. Le modifiche necessarie sono specifiche del sistema operativo. Per ulteriori informazioni, consulta il manuale del sistema operativo in uso.

   > **Warning**
   >
   > Se non si esegue questa fase, l'AMI non sarà utilizzabile.

2. Per trovare l'ID del volume dell'istanza, utilizza il comando describe-instances. Verrà creato uno snapshot del volume nella fase successiva.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].BlockDeviceMappings
```

Di seguito è riportato un output di esempio.

```
[
    [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "AttachTime": "2024-07-11T01:05:51+00:00",
                "DeleteOnTermination": true,
                "Status": "attached",
                "VolumeId": "vol-1234567890abcdef0"
            }
        }
    ]
]
```

3. Per creare uno snapshot del volume, utilizza il comando create-snapshot. Utilizza l'ID del volume della fase precedente.

```
aws ec2 create-snapshot \
    --volume-id vol-01234567890abcdef \
    --description "my snapshot"
```

Di seguito è riportato un output di esempio.

```
{
    "Description": "my snapshot",
    "Encrypted": false,
    "OwnerId": "123456789012",
    "Progress": "",
    "SnapshotId": "snap-0abcdef1234567890",
    "StartTime": "",
    "State": "pending",
    "VolumeId": "vol-01234567890abcdef",
    "VolumeSize": 30,
    "Tags": []
}
```

4. Attendi che lo stato dello snapshot sia `completed` prima di passare alla fase successiva. Per ottenere lo stato dello snapshot, utilizza il comando describe-snapshots con l'ID dello snapshot ottenuto nel passaggio precedente.

```
aws ec2 describe-snapshots \
    --snapshot-ids snap-0abcdef1234567890 \
    --query Snapshots[].State \
    --output text
```

Di seguito è riportato un output di esempio.

```
completed
```

5. Per creare una nuova AMI, utilizza il comando register-image. Utilizza il valore di `SnapshotId` dall'output di CreateSnapshot.

   - Per impostare la modalità di avvio su UEFI, aggiungi il parametro `--boot-mode` con valore `uefi`.

     ```
     aws ec2 register-image \
        --description "my image" \
        --name "my-image" \
        --block-device-mappings "DeviceName=/dev/
     sda1,Ebs={SnapshotId=snap-0abcdef1234567890,DeleteOnTermination=true}" \
        --root-device-name /dev/sda1 \
        --virtualization-type hvm \
        --ena-support \
        --boot-mode uefi
     ```

   - Per impostare la modalità di avvio su `uefi-preferred`, imposta il valore di `--boot-mode` su `uefi-preferred`

     ```
     aws ec2 register-image \
        --description "my description" \
        --name "my-image" \
        --block-device-mappings "DeviceName=/dev/
     sda1,Ebs={SnapshotId=snap-0abcdef1234567890,DeleteOnTermination=true}" \
        --root-device-name /dev/sda1 \
        --virtualization-type hvm \
        --ena-support \
        --boot-mode uefi-preferred
     ```

6. (Facoltativo) Per verificare che l'AMI appena creata disponga della modalità di avvio specificata, utilizza il comando describe-images.

```
aws ec2 describe-images \
    --image-id ami-1234567890abcdef0 \
    --query Images[].BootMode \
    --output text
```

Di seguito è riportato un output di esempio.

```
uefi
```

PowerShell

Per impostare la modalità di avvio di un'AMI

1. Apporta le modifiche appropriate al volume e al sistema operativo dell'istanza per supportare l'avvio utilizzando la modalità di avvio selezionata. Le modifiche necessarie sono specifiche del sistema operativo. Per ulteriori informazioni, consulta il manuale del sistema operativo in uso.

   > **Warning**
   >
   > Se non si esegue questa fase, l'AMI non sarà utilizzabile.

2. Per trovare l'ID del volume dell'istanza, utilizza il cmdlet Get-EC2Instance.

   ```
   (Get-EC2Instance `
       -InstanceId i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
   ```

   Di seguito è riportato un output di esempio.

   ```
   AssociatedResource  :
   AttachTime          : 7/11/2024 1:05:51 AM
   DeleteOnTermination : True
   Operator            :
   Status              : attached
   VolumeId            : vol-01234567890abcdef
   ```

3. Per creare uno snapshot del volume, utilizza il cmdlet New-EC2Snapshot. Utilizza l'ID del volume della fase precedente.

```
New-EC2Snapshot `
    -VolumeId vol-01234567890abcdef `
    -Description "my snapshot"
```

Di seguito è riportato un output di esempio.

```
AvailabilityZone          :
Description               : my snapshot
Encrypted                 : False
FullSnapshotSizeInBytes   : 0
KmsKeyId                  :
OwnerId                   : 123456789012
RestoreExpiryTime         :
SnapshotId                : snap-0abcdef1234567890
SseType                   :
StartTime                 : 4/25/2025 6:08:59 PM
State                     : pending
StateMessage              :
VolumeId                  : vol-01234567890abcdef
VolumeSize                : 30
```

4. Attendi che lo stato dello snapshot sia `completed` prima di passare alla fase successiva. Per ottenere lo stato dello snapshot, utilizza il cmdlet Get-EC2Snapshot con l'ID dello snapshot del passaggio precedente.

```
(Get-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890).State.Value
```

Di seguito è riportato un output di esempio.

```
completed
```

5. Per creare una nuova AMI, utilizza il cmdlet Register-EC2Image. Utilizza il valore di `SnapshotId` dall'output di New-EC2Snapshot.

   - Per impostare la modalità di avvio su UEFI, aggiungi il parametro `-BootMode` con valore `uefi`.

```
$block = @{SnapshotId=snap-0abcdef1234567890}
Register-EC2Image `
```

```
    -Description "my image" `
    -Name "my-image" `
    -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block} `
    -RootDeviceName /dev/xvda `
    -EnaSupport $true `
    -BootMode uefi
```

- Per impostare la modalità di avvio su `uefi-preferred`, imposta il valore di `-BootMode` su `uefi-preferred`

```
$block = @{SnapshotId=snap-0abcdef1234567890}
Register-EC2Image `
    -Description "my image" `
    -Name "my-image" `
    -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block} `
    -RootDeviceName /dev/xvda `
    -EnaSupport $true `
    -BootMode uefi-preferred
```

6. (Facoltativo) Per verificare che l'AMI appena creata disponga della modalità di avvio specificata, utilizza il cmdlet Get-EC2Image.

```
(Get-EC2Image `
    -ImageId ami-1234567890abcdef0).BootMode.Value
```

Di seguito è riportato un output di esempio.

```
uefi
```

Variabili UEFI per istanze Amazon EC2

Quando si avvia un'istanza in cui la modalità di avvio è impostata su UEFI, viene creato un archivio chiave-valore per le variabili. L'archivio può essere utilizzato da UEFI e dal sistema operativo dell'istanza per l'archiviazione delle variabili UEFI.

Le variabili UEFI vengono utilizzate dal bootloader e dal sistema operativo per configurare il startup iniziale del sistema. Consentono al sistema operativo di gestire alcune impostazioni del processo di avvio, come l'ordine di avvio, o di gestire le chiavi per UEFI Secure Boot.

> **Warning**
>
> Chiunque sia in grado di connettersi all'istanza (e potenzialmente a qualsiasi software in esecuzione sull'istanza) o chiunque disponga delle autorizzazioni per utilizzare l'GetInstanceUefiDataAPI sull'istanza può leggere le variabili. Non è necessario archiviare dati sensibili, ad esempio password o informazioni di identificazione personale, nell'archivio variabili UEFI.

Persistenza delle variabili UEFI

- Per le istanze avviate prima del 10 maggio 2022 incluso, le variabili UEFI vengono cancellate al riavvio o all'arresto.
- Per le istanze avviate a partire dall'11 maggio 2022, le variabili UEFI contrassegnate come non volatili vengono mantenute al riavvio e. stop/start
- Le istanze bare metal non preservano le variabili UEFI non volatili nelle operazioni di istanza. stop/start

UEFI Secure Boot per istanze Amazon EC2

UEFI Secure Boot si basa sul processo di avvio sicuro di lunga data di Amazon EC2 e fornisce un'ulteriore difesa approfondita che aiuta i clienti a proteggere il software dalle minacce che persistono tra i riavvii. Garantisce che l'istanza avvia solo il software firmato con chiavi crittografiche. Le chiavi sono archiviate nel database delle chiavi dell'archivio delle variabili non volatili UEFI. UEFI Secure Boot impedisce la modifica non autorizzata del flusso di avvio dell'istanza.

Indice

- Come funziona UEFI Secure Boot con le istanze Amazon EC2
- Requisiti per l'avvio sicuro UEFI su Amazon EC2
- Verifica dell'abilitazione di un'istanza Amazon EC2 per UEFI Secure Boot
- Creare un'AMI di Linux con chiavi personalizzate di UEFI Secure Boot
- Crea il AWS blob binario per UEFI Secure Boot

Come funziona UEFI Secure Boot con le istanze Amazon EC2

UEFI Secure Boot è una caratteristica specificata in UEFI, che fornisce la verifica dello stato della catena di avvio. È progettato per garantire che solo i file binari UEFI verificati crittograficamente vengano eseguiti dopo l'inizializzazione automatica del firmware. Questi file binari includono i driver UEFI e il bootloader principale, oltre a componenti caricati a catena.

UEFI Secure Boot specifica quattro database chiave, utilizzati in una catena di attendibilità. I database sono archiviati nell'archivio delle variabili UEFI.

La catena di attendibilità è la seguente:

Database delle chiavi della piattaforma (Platform Key, PK)

Il database PK è il root di attendibilità. Contiene una singola chiave PK pubblica che viene utilizzata nella catena di attendibilità per l'aggiornamento del database delle chiavi di scambio delle chiavi (Key Exchange Key, KEK).

Per modificare il database PK, è necessario disporre della chiave PK privata per firmare una richiesta di aggiornamento. Ciò include l'eliminazione del database PK scrivendo una chiave PK vuota.

Database delle chiavi di scambio delle chiavi (KEK)

Il database KEK è un elenco di chiavi KEK pubbliche utilizzate nella catena di attendibilità per l'aggiornamento dei database delle firme (DB) e denylist (dbx).

Per modificare il database KEK pubblico, è necessario disporre della chiave PK privata per firmare una richiesta di aggiornamento.

Database firma (DB)

Il database DB è un elenco di chiavi pubbliche e hash utilizzati nella catena di attendibilità per convalidare tutti i file binari di avvio UEFI.

Per modificare il database db, è necessario disporre della chiave PK privata o di chiavi KEK private per firmare una richiesta di aggiornamento.

Database di denylist firme (dbx)

Il database dbx è un elenco di chiavi pubbliche e hash binari che non sono attendibili e vengono utilizzati nella catena di attendibilità come file di revoca.

Il database dbx ha sempre la precedenza su tutti gli altri database di chiavi.

Per modificare il database dbx, è necessario disporre della chiave PK privata o di chiavi KEK private per firmare una richiesta di aggiornamento.

Il forum UEFI mantiene un dbx disponibile al pubblico per molti binari e certificati noti all'indirizzo. https://uefi.org/revocationlistfile

> **Important**
>
> UEFI Secure Boot applica la convalida della firma su qualsiasi file binario UEFI. Per consentire l'esecuzione di un binario UEFI in UEFI Secure Boot, lo devi firmare con una delle chiavi db private descritte sopra.

Per impostazione predefinita, UEFI Secure Boot è disabilitato e il sistema è in modalità `SetupMode`. Quando il sistema è in modalità `SetupMode`, tutte le variabili chiave possono essere aggiornate senza una firma crittografica. Quando il PK è impostato, UEFI Secure Boot è abilitato e viene chiuso. SetupMode

Requisiti per l'avvio sicuro UEFI su Amazon EC2

Quando avvii un'istanza Amazon EC2 con un'AMI supportata e un tipo di istanza supportato, tale istanza convaliderà automaticamente i binari di avvio UEFI rispetto al suo database UEFI Secure Boot. e non sono necessarie ulteriori configurazioni. Puoi configurare UEFI Secure Boot su un'istanza anche dopo l'avvio.

> **Note**
>
> UEFI Secure Boot protegge l'istanza e il suo sistema operativo dalle modifiche del flusso di avvio. Se crei una nuova AMI da un'AMI di origine con UEFI Secure Boot abilitato e modifichi certi parametri durante il processo di copia, come cambiare `UefiData` all'interno dell'AMI, puoi disabilitare UEFI Secure Boot.

Indice

- AMI supportate
- Tipi di istanze supportati

AMI supportate

AMI di Linux

Per lanciare un'istanza Linux, l'AMI di Linux deve avere UEFI Secure Boot abilitato.

Amazon Linux supporta UEFI Secure Boot a partire dal rilascio AL2023 2023.1. Tuttavia, UEFI Secure Boot non è abilitato nelle AMI predefinite. Per ulteriori informazioni, consulta la sezione UEFI Secure Boot nella Guida per l'utente di AL2023. Le versioni precedenti delle AMI Amazon Linux non sono abilitate per UEFI Secure Boot. Per utilizzare un'AMI supportata, è necessario eseguire una serie di passaggi di configurazione sulla propria AMI Linux. Per ulteriori informazioni, consulta Creare un'AMI di Linux con chiavi personalizzate di UEFI Secure Boot.

AMI di Windows

Per lanciare un'istanza Windows, l'AMI di Linux deve avere UEFI Secure Boot abilitato. Per trovare un'AMI AWS Windows preconfigurata per UEFI Secure Boot con chiavi Microsoft, consulta Trova le AMI di Windows Server configurate con NitroTPM e UEFI Secure Boot nella Guida di riferimento alle AMI di Windows. AWS

Al momento l'importazione di Windows con UEFI Secure Boot tramite il comando import-image non è supportata.

Tipi di istanze supportati

Tutti i tipi di istanze virtualizzate che supportano UEFI supportano anche UEFI Secure Boot. Per i tipi di istanza che supportano UEFI Secure Boot, consulta Requisiti per la modalità di avvio UEFI.

> **Note**
>
> I tipi di istanza bare metal non supportano UEFI Secure Boot.

Verifica dell'abilitazione di un'istanza Amazon EC2 per UEFI Secure Boot

Puoi usare le procedure seguenti per determinare se Amazon EC2 è abilitato per UEFI Secure Boot.

Istanze Linux

Per verificare se un'istanza Linux è abilitata per UEFI Secure Boot, utilizza l'utilità `mokutil`. Installa `mokutil` se non è già presente nell'istanza. Per le istruzioni di installazione per Amazon Linux 2,

consulta Trovare e installare pacchetti software su un'istanza Amazon Linux 2. Per altre distribuzioni Linux, consulta la relativa documentazione specifica.

Per verificare se un'istanza Linux è abilitata per UEFI Secure Boot

Connettiti alla tua istanza ed esegui il seguente comando come `root` in una finestra del terminale.

```
mokutil --sb-state
```

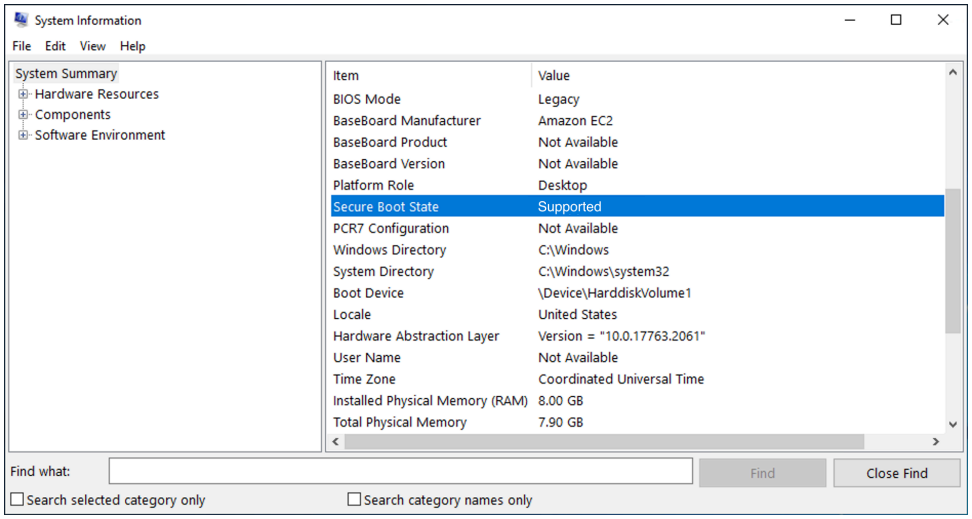
Di seguito è riportato un output di esempio.

- Se UEFI Secure Boot è abilitato, l'output contiene `SecureBoot enabled`.
- Se UEFI Secure Boot non è abilitato, l'output contiene `SecureBoot disabled` o `Failed to read SecureBoot`.

Istanze Windows

Per verificare se un'istanza Windows è abilitata per UEFI Secure Boot

1. Connettiti alla tua istanza.
2. Apri lo strumento msinfo32.
3. Controlla il campo Secure Boot State (Stato Secure Boot). Se UEFI Secure Boot è abilitato, il valore è Supportato, come mostrato nell'immagine seguente.



È inoltre possibile utilizzare il PowerShell cmdlet di Windows `Confirm-SecureBootUEFI` per verificare lo stato di avvio sicuro. Per ulteriori informazioni sul cmdlet, vedere Confirm-SecureBootUEFI la documentazione Microsoft.

Creare un'AMI di Linux con chiavi personalizzate di UEFI Secure Boot

Queste istruzioni mostrano come creare un'AMI di Linux con UEFI Secure Boot e chiavi private personalizzate. Amazon Linux supporta UEFI Secure Boot a partire dal rilascio AL2023 2023.1. Per ulteriori informazioni, consulta UEFI Secure Boot on AL2023 nella Guida per l'utente di Amazon Linux 2023.

> **Important**
>
> La procedura seguente è destinata esclusivamente agli utenti esperti. Per utilizzare queste procedure è necessario disporre di una conoscenza sufficiente del flusso di avvio della distribuzione SSL e Linux.

Prerequisiti

- Verranno utilizzati i seguenti strumenti:
  - OpenSSL — https://www.openssl.org/
  - efivar — https://github.com/rhboot/efivar
  - efitools — https://git.kernel.org/pub/scm/linux/kernel/git/jejb/efitools.git/
  - Comando get-instance-uefi-data
- L'istanza Linux deve essere stata avviata con un'AMI Linux che supporta la modalità di avvio UEFI e deve contenere dati non volatili.

Le istanze appena create senza chiavi UEFI Secure Boot vengono create in `SetupMode`, che ti consente di registrare le tue chiavi. Alcune AMI sono preconfigurate con UEFI Secure Boot e non è possibile modificare le chiavi esistenti. Se desideri modificare le chiavi, devi creare una nuova AMI basata sull'AMI originale.

Sono disponibili due modi per propagare le chiavi nell'archivio delle variabili, descritti di seguito sotto Opzione A e Opzione B. L'Opzione A descrive come farlo dall'interno dell'istanza, imitando il flusso di hardware reale. L'Opzione B descrive come creare un blob binario, che viene poi passato come file

con codifica base64 quando si crea l'AMI. Per entrambe le opzioni, è necessario innanzitutto creare le tre coppie di chiavi, utilizzate per la catena di attendibilità.

Per creare un'AMI di Linux che supporti UEFI Secure Boot, prima devi creare le tre coppie di chiavi e quindi completare l'Opzione A o l'Opzione B, ma non entrambe:

- Attività 1 - Creare coppie di chiavi
- Attività 2 - Opzione A: aggiunta delle chiavi all'archivio delle variabili dall'interno dell'istanza
- Attività 2 - Opzione B: creazione di un blob binario contenente un archivio delle variabili preriempito

Attività 1 - Creare coppie di chiavi

UEFI Secure Boot si basa sui seguenti tre database di chiavi, utilizzati in una catena di attendibilità: la chiave di piattaforma (PK), la chiave di scambio delle chiavi (KEK) e il database delle firme (DB).[1]

Crea ciascuna chiave sull'istanza. Per preparare le chiavi pubbliche in un formato valido per lo standard UEFI Secure Boot, devi creare un certificato per ciascuna chiave. `DER` definisce il formato SSL (codifica binaria di un formato). Devi quindi convertire ogni certificato in un elenco di firme UEFI, che è il formato binario compreso da UEFI Secure Boot. Infine, devi firmare ogni certificato con la chiave pertinente.

Processi

- Preparazione alla creazione delle coppie di chiavi
- Coppia di chiavi 1: crea la chiave della piattaforma (PK)
- Coppia di chiavi 2: crea la chiave di scambio chiave (KEK)
- Coppia di chiavi 3: crea il database delle firme (DB)
- Firma l'immagine di avvio (kernel) con la chiave privata.

Preparazione alla creazione delle coppie di chiavi

Prima di creare le coppie di chiavi, crea un identificatore univoco globale (GUID) da utilizzare nella generazione delle chiavi.

1. Collegati all'istanza.
2. Esegui il comando seguente in un prompt della shell.

```
uuidgen --random > GUID.txt
```

Coppia di chiavi 1: crea la chiave della piattaforma (PK)

La PK è il root di attendibilità per le istanze UEFI Secure Boot. La PK privata viene utilizzata per aggiornare la KEK, che a sua volta può essere utilizzata per aggiungere chiavi autorizzate al database delle firme (DB).

Lo X.509 standard viene utilizzato per creare la coppia di chiavi. Per informazioni sullo standard, consulta X.509 Wikipedia.

Per creare la PK

1. Crea la chiave. Devi assegnare un nome alla variabile PK.

   ```
   openssl req -newkey rsa:4096 -nodes -keyout PK.key -new -x509 -sha256 -days 3650 -
   subj "/CN=Platform key/" -out PK.crt
   ```

   Vengono specificati i seguenti parametri:

   - `-keyout PK.key`: il file della chiave privata.
   - `-days 3650`: il numero di giorni per cui il certificato è valido.
   - `-out PK.crt`: il certificato che viene utilizzato per creare la variabile UEFI.
   - `CN=Platform key`: il nome comune (CN) della chiave. Puoi inserire il nome della tua organizzazione invece di*Platform key*.
2. Crea il certificato.

   ```
   openssl x509 -outform DER -in PK.crt -out PK.cer
   ```
3. Converti il certificato in un elenco di firme UEFI.

   ```
   cert-to-efi-sig-list -g "$(< GUID.txt)" PK.crt PK.esl
   ```
4. Firma l'elenco delle firme UEFI con la PK privata (autofirmata).

   ```
   sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt PK PK.esl PK.auth
   ```

Coppia di chiavi 2: crea la chiave di scambio chiave (KEK)

La KEK privata viene utilizzata per aggiungere chiavi al db, ossia l'elenco delle firme autorizzate da avviare sul sistema.

Per creare la KEK

1. Crea la chiave.

```
openssl req -newkey rsa:4096 -nodes -keyout KEK.key -new -x509 -sha256 -days 3650 -
subj "/CN=Key Exchange Key/" -out KEK.crt
```

2. Crea il certificato.

```
openssl x509 -outform DER -in KEK.crt -out KEK.cer
```

3. Converti il certificato in un elenco di firme UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" KEK.crt KEK.esl
```

4. Firma l'elenco delle firme con la PK privata.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt KEK KEK.esl KEK.auth
```

Coppia di chiavi 3: crea il database delle firme (DB)

L'elenco db contiene chiavi autorizzate per l'avvio sul sistema. Per modificare l'elenco, è necessaria la KEK privata. Le immagini di avvio saranno firmate con la chiave privata creata in questa fase.

Per creare il db

1. Crea la chiave.

```
openssl req -newkey rsa:4096 -nodes -keyout db.key -new -x509 -sha256 -days 3650 -
subj "/CN=Signature Database key/" -out db.crt
```

2. Crea il certificato.

```
openssl x509 -outform DER -in db.crt -out db.cer
```

3. Converti il certificato in un elenco di firme UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" db.crt db.esl
```

4. Firma l'elenco delle firme con la KEK privata.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k KEK.key -c KEK.crt db db.esl db.auth
```

Firma l'immagine di avvio (kernel) con la chiave privata.

Per Ubuntu 22.04, le seguenti immagini richiedono le firme.

```
/boot/efi/EFI/ubuntu/shimx64.efi
/boot/efi/EFI/ubuntu/mmx64.efi
/boot/efi/EFI/ubuntu/grubx64.efi
/boot/vmlinuz
```

Per firmare un'immagine

Utilizza una sintassi come la seguente per firmare un'immagine.

```
sbsign --key db.key --cert db.crt --output /boot/vmlinuz /boot/vmlinuz
```

> **Note**
>
> Devi firmare tutti i nuovi kernel. Di solito, */boot/vmlinuz* esegue un collegamento simbolico all'ultimo kernel installato.

Per informazioni sulla catena di avvio e sulle immagini richieste, consulta la documentazione per la distribuzione.

[1] Grazie alla ArchWiki community per tutto il lavoro svolto. I comandi per creare il PK, creare il KEK, creare il DB e firmare l'immagine provengono da Creating keys, creato dal team and/or di ArchWiki manutenzione, che ha collaborato. ArchWiki

Attività 2 - Opzione A: aggiunta delle chiavi all'archivio delle variabili dall'interno dell'istanza

Dopo avere creato le tre coppie di chiavi, puoi connetterti alla tua istanza e aggiungere le chiavi all'archivio delle variabili dall'interno dell'istanza completando le fasi seguenti. Altrimenti, completa i passaggi indicati in the section called "Attività 2 - Opzione B: creazione di un blob binario contenente un archivio delle variabili preriempito".

Fasi dell'Opzione A:

- Fase 1: avvio di un'istanza che supporti UEFI Secure Boot
- Fase 2: configurazione di un'istanza per supportare UEFI Secure Boot
- Fase 3: creazione di un'AMI dall'istanza

Fase 1: avvio di un'istanza che supporti UEFI Secure Boot

Quando avvii un'istanza con i seguenti prerequisiti, l'istanza sarà pronta per essere configurata per supportare UEFI Secure Boot. È possibile abilitare il supporto per UEFI Secure Boot su un'istanza solo al momento dell'avvio; non è possibile abilitarlo in un secondo momento.

Prerequisiti

- AMI: l'AMI Linux deve supportare la modalità di avvio UEFI. Per verificare che l'AMI supporti la modalità di avvio UEFI, il parametro della modalità di avvio AMI deve essere uefi. Per ulteriori informazioni, consulta Determinare il parametro della modalità di avvio di un'AMI di Amazon EC2.

  Nota che fornisce AWS solo AMI Linux configurate per supportare UEFI per i tipi di istanza. Graviton-based AWS attualmente non fornisce AMI Linux x86_64 che supportano la modalità di avvio UEFI. Puoi configurare un'AMI personalizzata che supporta la modalità di avvio UEFI per tutte le architetture. Per utilizzare un'AMI personalizzata che supporta la modalità di avvio UEFI, devi eseguire una serie di passaggi di configurazione sulla tua AMI. Per ulteriori informazioni, consulta Impostare la modalità di avvio di un'AMI Amazon EC2.
- Tipo di istanza: tutti i tipi di istanze virtualizzate che supportano UEFI supportano anche UEFI Secure Boot. I tipi di istanza bare metal non supportano UEFI Secure Boot. Per i tipi di istanza che supportano UEFI Secure Boot, consulta Requisiti per la modalità di avvio UEFI.
- Avvia l'istanza dopo il rilascio di UEFI Secure Boot. Solo le istanze avviate dopo il 10 maggio 2022 (quando è stato rilasciato UEFI Secure Boot) possono supportare UEFI Secure Boot.

Dopo avere avviato l'istanza, puoi verificare che sia pronta per essere configurata per supportare UEFI Secure Boot (in altre parole, puoi procedere alla Fase 2) verificando se i dati UEFI sono presenti. La presenza di dati UEFI indica che i dati non volatili sono persistenti.

Per verificare se l'istanza è pronta per la fase 2

Utilizza il comando get-instance-uefi-data e specifica l'ID dell'istanza.

```
aws ec2 get-instance-uefi-data --instance-id i-1234567890abcdef0
```

L'istanza è pronta per la fase 2 se i dati UEFI sono presenti nell'output. Se l'output è vuoto, l'istanza non può essere configurata per supportare UEFI Secure Boot. Ciò può verificarsi se l'istanza è stata avviata prima che il supporto UEFI Secure Boot fosse disponibile. Avvia una nuova istanza e riprova.

Fase 2: configurazione di un'istanza per supportare UEFI Secure Boot

Registrazione delle coppie di chiavi nell'archivio delle variabili UEFI dell'utente sull'istanza

> **Warning**
>
> Le immagini di avvio devono essere firmate dopo avere registrato le chiavi, altrimenti non potrai avviare l'istanza.

Dopo avere creato gli elenchi di firme UEFI firmati (`PK`, `KEK` e `db`), gli elenchi devono essere iscritti al firmware UEFI.

La scrittura nella variabile `PK` è possibile solo se:

- Nessuna PK è ancora iscritta, nel qual caso la variabile `SetupMode` ha il valore `1`. Per verificarlo, utilizza il comando seguente. L'output è `1` o `0`.

  ```
  efivar -d -n 8be4df61-93ca-11d2-aa0d-00e098032b8c-SetupMode
  ```

- La nuova PK è firmata dalla chiave privata della PK esistente.

Per registrare le chiavi nell'archivio delle variabili UEFI dell'utente

I seguenti comandi devono essere eseguiti sull'istanza.

Se SetupMode è abilitato (il valore è`1`), le chiavi possono essere registrate eseguendo i seguenti comandi sull'istanza:

```
[ec2-user ~]$ efi-updatevar -f db.auth db
```

```
[ec2-user ~]$ efi-updatevar -f KEK.auth KEK
```

```
[ec2-user ~]$ efi-updatevar -f PK.auth PK
```

Per verificare che UEFI Secure Boot sia abilitato

Per verificare che UEFI Secure Boot sia abilitato, attieniti alla procedura descritta in Verifica dell'abilitazione di un'istanza Amazon EC2 per UEFI Secure Boot.

Ora puoi esportare il tuo archivio di variabili UEFI con il comando get-instance-uefi-data CLI oppure puoi continuare con il passaggio successivo e firmare le immagini di avvio per il riavvio in un'istanza UEFI Secure. Boot-enabled

Fase 3: creazione di un'AMI dall'istanza

Per creare un'AMI dall'istanza, puoi utilizzare la console o l'API `CreateImage`, la CLI o gli SDK. Per le istruzioni relative alla console, consulta la sezione Crea un' EBS-backed AMI Amazon. Per le istruzioni sull'API, consulta. CreateImage

> **Note**
>
> L'API `CreateImage` copia automaticamente l'archivio delle variabili UEFI dell'istanza nell'AMI. La console utilizza l'API `CreateImage`. Dopo avere avviato le istanze utilizzando questa AMI, le istanze avranno lo stesso archivio delle variabili UEFI.

Attività 2 - Opzione B: creazione di un blob binario contenente un archivio delle variabili preriempito

Dopo aver creato le tre coppie di chiavi, puoi creare un blob binario contenente un archivio delle variabili preriempito contenente le chiavi UEFI Secure Boot. Altrimenti, completa i passaggi indicati in the section called "Attività 2 - Opzione A: aggiunta delle chiavi all'archivio delle variabili dall'interno dell'istanza".

> **Warning**
>
> Le immagini di avvio devono essere firmate prima di registrare le chiavi, altrimenti non potrai avviare l'istanza.

Fase dell'opzione B:

- Fase 1: creazione di un nuovo archivio delle variabili o aggiornamento di un archivio esistente
- Fase 2: caricamento del blob binario al momento della creazione dell'AMI

Fase 1: creazione di un nuovo archivio delle variabili o aggiornamento di un archivio esistente

Puoi creare l'archivio delle variabili non in linea senza un'istanza in esecuzione utilizzando lo strumento python-uefivars. Lo strumento può creare un nuovo archivio delle variabili a partire dalle chiavi. Lo script attualmente supporta il formato EDK2, il AWS formato e una rappresentazione JSON più facile da modificare con strumenti di livello superiore.

Per creare l'archivio delle variabili non in linea senza un'istanza in esecuzione

1. Scarica lo strumento al seguente link.

   ```
   https://github.com/awslabs/python-uefivars
   ```

2. Crea un nuovo archivio delle variabili a partire dalle chiavi eseguendo il comando seguente. Questo creerà un blob binario con codifica base64 in .bin. *your_binary_blob* Lo strumento supporta anche l'aggiornamento di un blob binario utilizzando il parametro. `-I`

   ```
   ./uefivars.py -i none -o aws -O your_binary_blob.bin -P PK.esl -K KEK.esl --db
    db.esl --dbx dbx.esl
   ```

Fase 2: caricamento del blob binario al momento della creazione dell'AMI

Utilizza register-image per passare i dati dell'archivio delle variabili UEFI. Per il parametro `--uefi-data` specifica il blob binario, mentre per il parametro `--boot-mode` specifica `uefi`.

```
aws ec2 register-image \
    --name uefi_sb_tpm_register_image_test \
    --uefi-data $(cat your_binary_blob.bin) \
    --block-device-mappings "DeviceName=/dev/sda1,Ebs=
 {SnapshotId=snap-0123456789example,DeleteOnTermination=true}" \
    --architecture x86_64 \
    --root-device-name /dev/sda1 \
    --virtualization-type hvm \
    --ena-support \
    --boot-mode uefi
```

Crea il AWS blob binario per UEFI Secure Boot

Puoi completare le fasi seguenti per personalizzare le variabili UEFI Secure Boot durante la creazione di un'AMI. La KEK che viene utilizzata in queste fasi è in vigore a partire da settembre 2021. Se Microsoft aggiorna la KEK, devi utilizzare la KEK più recente.

Per creare il AWS blob binario

1. Crea un elenco di firme PK vuoto.

```
touch empty_key.crt
cert-to-efi-sig-list empty_key.crt PK.esl
```

2. Scarica i certificati KEK.

```
https://go.microsoft.com/fwlink/?LinkId=321185
```

3. Avvolgi i certificati KEK in un elenco di firme UEFI (`siglist`).

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_KEK.esl MicCorKEKCA2011_2011-06-24.crt
```

4. Scarica i certificati db di Microsoft.

```
https://www.microsoft.com/pkiops/certs/MicWinProPCA2011_2011-10-19.crt
https://www.microsoft.com/pkiops/certs/MicCorUEFCA2011_2011-06-27.crt
```

5. Genera l'elenco delle firme db.

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_db.esl MicWinProPCA2011_2011-10-19.crt
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_UEFI_db.esl MicCorUEFCA2011_2011-06-27.crt
cat MS_Win_db.esl MS_UEFI_db.esl > MS_db.esl
```

6. L'Unified Extensible Firmware Interface Forum (UEFI) non fornisce più i file DBX. Ora sono forniti da Microsoft su. GitHub Scarica l'ultimo aggiornamento DBX dal repository degli aggiornamenti di Microsoft Secure Boot all'indirizzo. https://github.com/microsoft/secureboot_objects
7. Decomprimi il file update-binary firmato.

Crea `SplitDbxContent.ps1` con il contenuto dello script seguente. In alternativa, è possibile installare lo script da PowerShell Gallery utilizzando. `Install-Script -Name SplitDbxContent`

```
<#PSScriptInfo

.VERSION 1.0

.GUID ec45a3fc-5e87-4d90-b55e-bdea083f732d

.AUTHOR Microsoft Secure Boot Team

.COMPANYNAME Microsoft

.COPYRIGHT Microsoft

.TAGS Windows Security

.LICENSEURI

.PROJECTURI

.ICONURI

.EXTERNALMODULEDEPENDENCIES

.REQUIREDSCRIPTS

.EXTERNALSCRIPTDEPENDENCIES

.RELEASENOTES
Version 1.0: Original published version.

#>

<#
.DESCRIPTION
 Splits a DBX update package into the new DBX variable contents and the signature
 authorizing the change.
 To apply an update using the output files of this script, try:
 Set-SecureBootUefi -Name dbx -ContentFilePath .\content.bin -SignedFilePath .
\signature.p7 -Time 2010-03-06T19:17:21Z -AppendWrite'
```

```
.EXAMPLE
.\SplitDbxAuthInfo.ps1 DbxUpdate_x64.bin
#>


# Get file from script input
$file  = Get-Content -Encoding Byte $args[0]

# Identify file signature
$chop = $file[40..($file.Length - 1)]
if (($chop[0] -ne 0x30) -or ($chop[1] -ne 0x82 )) {
    Write-Error "Cannot find signature"
    exit 1
}

# Signature is known to be ASN size plus header of 4 bytes
$sig_length = ($chop[2] * 256) + $chop[3] + 4
$sig = $chop[0..($sig_length - 1)]

if ($sig_length -gt ($file.Length + 40)) {
    Write-Error "Signature longer than file size!"
    exit 1
}

# Content is everything else
$content = $file[0..39] + $chop[$sig_length..($chop.Length - 1)]

# Write signature and content to files
Set-Content -Encoding Byte signature.p7 $sig
Set-Content -Encoding Byte content.bin $content
```

Utilizza lo script per decomprimere i file DBX firmati.

```
PS C:\Windows\system32> SplitDbxContent.ps1 .\dbx.bin
```

In questo modo vengono creati due file: `signature.p7` e `content.bin`. Utilizza `content.bin` nella fase successiva.

8. Crea un archivio delle variabili UEFI usando lo script `uefivars.py`.

```
./uefivars.py -i none -o aws -O uefiblob-microsoft-keys-empty-pk.bin -P ~/PK.esl -K
 ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx ~/content.bin
```

9. Controlla il blob binario e l'archivio delle variabili UEFI.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o json | less
```

10. È possibile aggiornare il blob passandolo nuovamente allo stesso strumento.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o aws -O uefiblob-
microsoft-keys-empty-pk.bin -P ~/PK.esl -K ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx
 ~/content.bin
```

Output previsto

```
Replacing PK
Replacing KEK
Replacing db
Replacing dbx
```

Usa la crittografia con le EBS-backed AMI

Le AMI supportate dagli snapshot Amazon EBS possono utilizzare la crittografia Amazon EBS. Gli snapshot sia dei dati che dei volumi root possono essere crittografati e collegati a un'AMI. Puoi avviare le istanze e copiare le immagini con supporto completo della crittografia EBS. I parametri di crittografia per queste operazioni sono supportati in tutte le regioni in cui AWS KMS è disponibile.

Le istanze EC2 con volumi EBS crittografati vengono avviate dalle AMIs come le altre istanze. Inoltre, quando avvii un'istanza da una AMI basata su snapshot EBS non crittografati, puoi crittografare alcuni o tutti i volumi durante l'avvio.

Come i volumi EBS, le istantanee nelle AMI possono essere crittografate in base all'impostazione predefinita AWS KMS key o con una chiave gestita dal cliente specificata dall'utente. In ogni caso, devi comunque disporre dell'autorizzazione per utilizzare la Chiave KMS selezionata.

Le AMI con istantanee crittografate possono essere condivise tra gli account. AWS Per ulteriori informazioni, consulta Informazioni sull'utilizzo delle AMI condivise in Amazon EC2.

Crittografia con EBS-backed AMI: argomenti

- Instance-launching scenari
- Image-copying scenari

Instance-launching scenari

Le istanze Amazon EC2 vengono lanciate dalle AMI utilizzando l'`RunInstances`azione con parametri forniti tramite la mappatura dei dispositivi a blocchi, tramite o utilizzando direttamente l'API Console di gestione AWS o l'interfaccia a riga di comando di Amazon EC2. Per ulteriori informazioni, consulta Mappature dei dispositivi a blocchi per i volumi sulle istanze Amazon EC2. Per esempi di controllo della mappatura dei dispositivi a blocchi da AWS CLI, consulta Launch, List e Terminate EC2 Instances.

Per impostazione predefinita, senza parametri di crittografia espliciti, un'operazione `RunInstances` mantiene lo stato della crittografia esistente degli snapshot di origine di un'AMI e ripristina i volumi EBS da tali snapshot. Se è abilitata la crittografia per impostazione predefinita, tutti i volumi creati dall'AMI (sia da snapshot crittografati che non crittografati) vengono crittografati. Se non è abilitata la crittografia predefinita, l'istanza mantiene lo stato della crittografia dell'AMI.

Puoi anche avviare un'istanza e contemporaneamente applicare un nuovo stato della crittografia ai restanti volumi fornendo i parametri di crittografia. Di conseguenza, si registrano i seguenti comportamenti:

Avvio senza parametri di crittografia

- Uno snapshot non crittografato viene ripristinato su un volume non crittografato, a meno che non sia abilitata la crittografia predefinita, nel cui caso tutti i volumi appena creati verranno crittografati.
- Uno snapshot crittografato di cui sei il proprietario viene ripristinato su un volume crittografato sulla stessa Chiave KMS.
- Un'istantanea crittografata che non possiedi (ad esempio, l'AMI è condivisa con te) viene ripristinata su un volume crittografato dalla chiave KMS predefinita del tuo AWS account.

I comportamenti predefiniti possono essere sovrascritti fornendo i parametri di crittografia. I parametri disponibili sono `Encrypted` e `KmsKeyId`. La sola impostazione del parametro `Encrypted` comporta le seguenti operazioni:

Comportamenti di avvio dell'istanza con **`Encrypted`** impostati, ma nessun **`KmsKeyId`** specificato

- Uno snapshot non crittografato viene ripristinato su un volume EBS crittografato dalla chiave KMS di default del tuo account AWS .
- Uno snapshot crittografato di cui sei il proprietario viene ripristinato su un volume EBS crittografato dalla stessa Chiave KMS. (Pertanto, il parametro `Encrypted` non ha alcun effetto.)

- Un'istantanea crittografata che non possiedi (ovvero, l'AMI è condivisa con te) viene ripristinata in un volume crittografato dalla chiave KMS predefinita del tuo AWS account. (Pertanto, il parametro `Encrypted` non ha alcun effetto.)

L'impostazione dei parametri `Encrypted` e `KmsKeyId` consente di specificare una Chiave KMS non predefinita per un'operazione di crittografia. Risultano i seguenti comportamenti:

Viene impostata un'istanza con **`Encrypted`** e **`KmsKeyId`**

- Uno snapshot non crittografato viene ripristinato su un volume EBS crittografato dalla Chiave KMS specificata.
- Uno snapshot crittografato viene ripristinato su un volume EBS crittografato non sulla Chiave KMS originale, ma sulla Chiave KMS specificata.

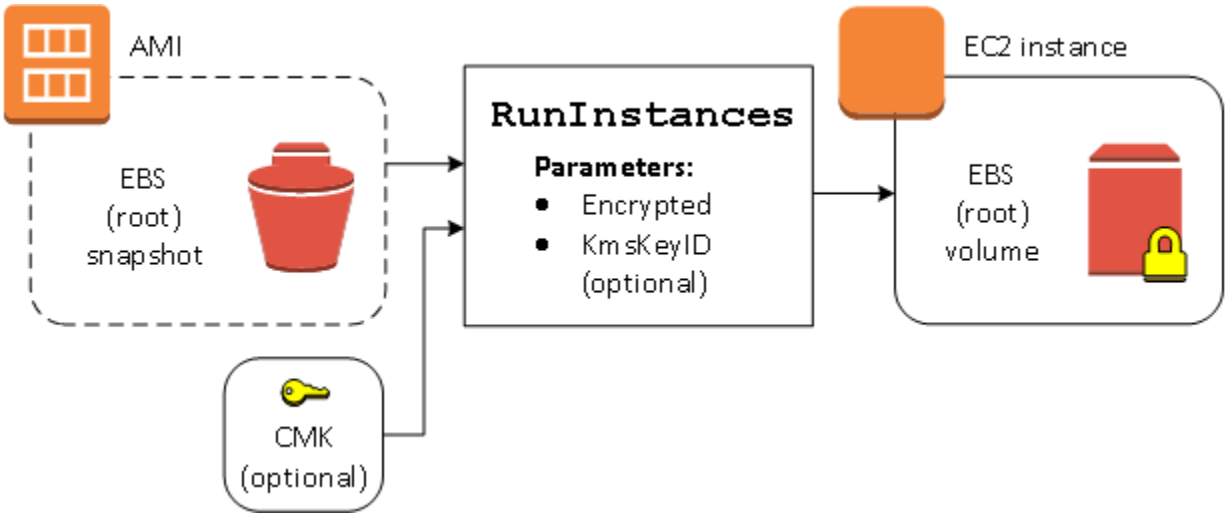
L'invio di `KmsKeyId` senza l'impostazione del parametro `Encrypted` causa un errore.

Le seguenti sezioni offrono esempi di avvio di istanze dalle AMI utilizzando parametri di crittografia non predefiniti. In ognuno dei seguenti scenari, i parametri forniti all'operazione `RunInstances` portano a un cambiamento dello stato della crittografia durante il ripristino di un volume da uno snapshot.

Per informazioni sull'utilizzo della console per avviare un'istanza da un'AMI, consulta Avviare un'istanza Amazon EC2.

Crittografia di un volume durante l'avvio

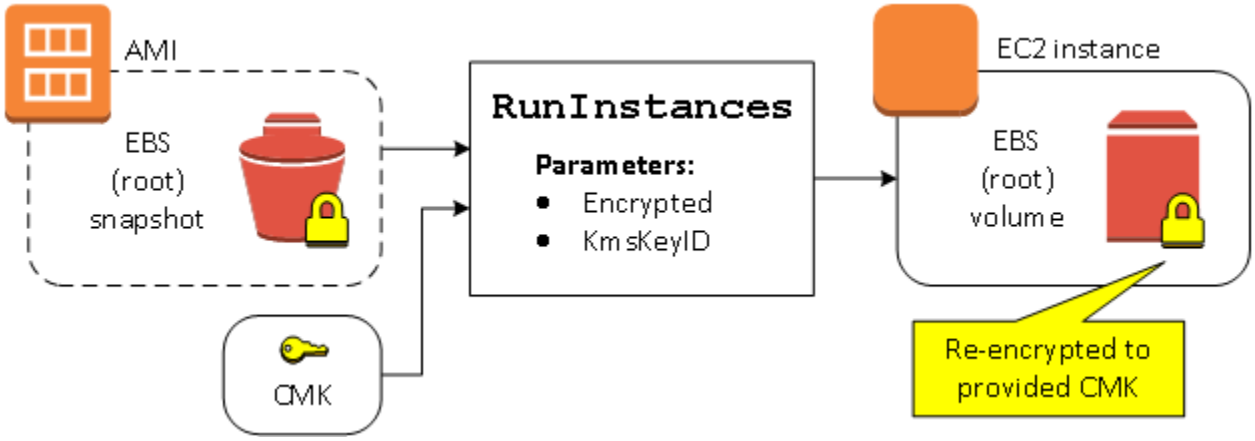
In questo esempio, viene utilizzata un'AMI basata su uno snapshot non crittografato per avviare un'istanza EC2 con un volume EBS crittografato.



Il parametro `Encrypted` da solo comporta la crittografia del volume per questa istanza. La fornitura di un parametro `KmsKeyId` è facoltativa. Se non viene specificato alcun ID della chiave KMS, per crittografare il volume viene utilizzata la chiave KMS predefinita dell' AWS account. Per crittografare il volume su una Chiave KMS diversa di tua proprietà, specifica il parametro `KmsKeyId`.

Re-encrypt un volume durante l'avvio

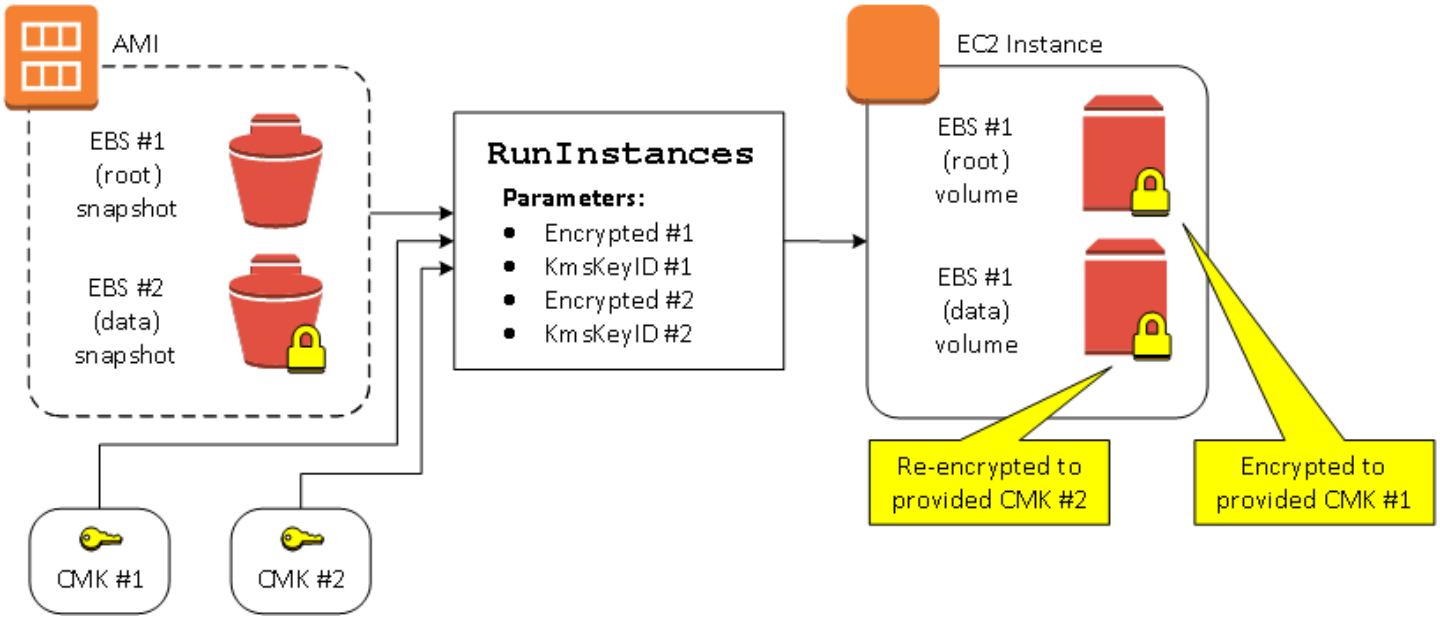
In questo esempio, viene utilizzata un'AMI basata su uno snapshot crittografato per avviare un'istanza EC2 con un volume EBS crittografato da una nuova Chiave KMS.



Se sei il proprietario dell'AMI e non fornisci parametri di crittografia, l'istanza risultante ha un volume crittografato dalla stessa Chiave KMS dello snapshot. Se invece condividi l'AMI anziché esserne il proprietario e non fornisci parametri di crittografia, il volume viene crittografato dalla Chiave KMS predefinita. Con i parametri di crittografia forniti come illustrato, il volume viene crittografato dalla Chiave KMS specificata.

Cambio dello stato della crittografia di più volumi durante l'avvio

In questo esempio più complesso, viene utilizzata un'AMI basata su più snapshot (ognuno con il proprio stato della crittografia) per avviare un'istanza EC2 con un volume appena crittografato e un volume crittografato nuovamente.



In questo scenario, l'operazione `RunInstances` viene fornita con parametri di crittografia per ognuno degli snapshot di origine. Quando sono specificati tutti i parametri di crittografia possibili, l'istanza risultante è la stessa indipendentemente dal fatto che tu sia il proprietario dell'AMI.

Image-copying scenari

Le AMI di Amazon EC2 sono copiate utilizzando l'operazione `CopyImage` tramite la Console di gestione AWS o utilizzando direttamente l'API o la CLI di Amazon EC2.

Per impostazione predefinita, senza parametri di crittografia espliciti, un'azione `CopyImage` mantiene lo stato della crittografia esistente degli snapshot di origine di un'AMI durante la copia. Puoi anche copiare un'AMI e contemporaneamente applicare un nuovo stato della crittografia agli snapshot EBS associati fornendo i parametri di crittografia. Di conseguenza, si registrano i seguenti comportamenti:

Copia senza parametri di crittografia

- Uno snapshot non crittografato viene copiato su un altro snapshot non crittografato, a meno che non sia abilitata la crittografia predefinita, nel cui caso tutti gli snapshot appena creati verranno crittografati.

- Uno snapshot crittografato di cui sei il proprietario viene copiato su uno snapshot crittografato con la stessa Chiave KMS.
- Un'istantanea crittografata che non possiedi (ovvero, l'AMI è condivisa con te) viene copiata in un'istantanea crittografata dalla chiave KMS predefinita del tuo AWS account.

Tutti questi comportamenti predefiniti possono essere sovrascritti fornendo i parametri di crittografia. I parametri disponibili sono `Encrypted` e `KmsKeyId`. La sola impostazione del parametro `Encrypted` comporta le seguenti operazioni:

Copy-image comportamenti con **`Encrypted`** set, ma non specificato **`KmsKeyId`**

- Uno snapshot non crittografato viene copiato su uno snapshot crittografato dalla chiave KMS di default dell'account AWS .
- Uno snapshot crittografato viene copiato su uno snapshot crittografato dalla stessa Chiave KMS. (Pertanto, il parametro `Encrypted` non ha alcun effetto.)
- Un'istantanea crittografata che non possiedi (ovvero, l'AMI è condivisa con te) viene copiata in un volume crittografato dalla chiave KMS predefinita del tuo AWS account. (Pertanto, il parametro `Encrypted` non ha alcun effetto.)

L'impostazione di entrambi i parametri `Encrypted` e `KmsKeyId` consente di specificare una Chiave KMS gestita dal cliente per un'operazione di crittografia. Risultano i seguenti comportamenti:

Copy-image comportamenti con entrambi e set **`Encrypted`** **`KmsKeyId`**

- Uno snapshot non crittografato viene copiato su uno snapshot crittografato dalla Chiave KMS specificata.
- Uno snapshot crittografato viene copiato su uno snapshot crittografato non sulla Chiave KMS originale, ma sulla Chiave KMS specificata.

L'invio di `KmsKeyId` senza l'impostazione del parametro `Encrypted` causa un errore.

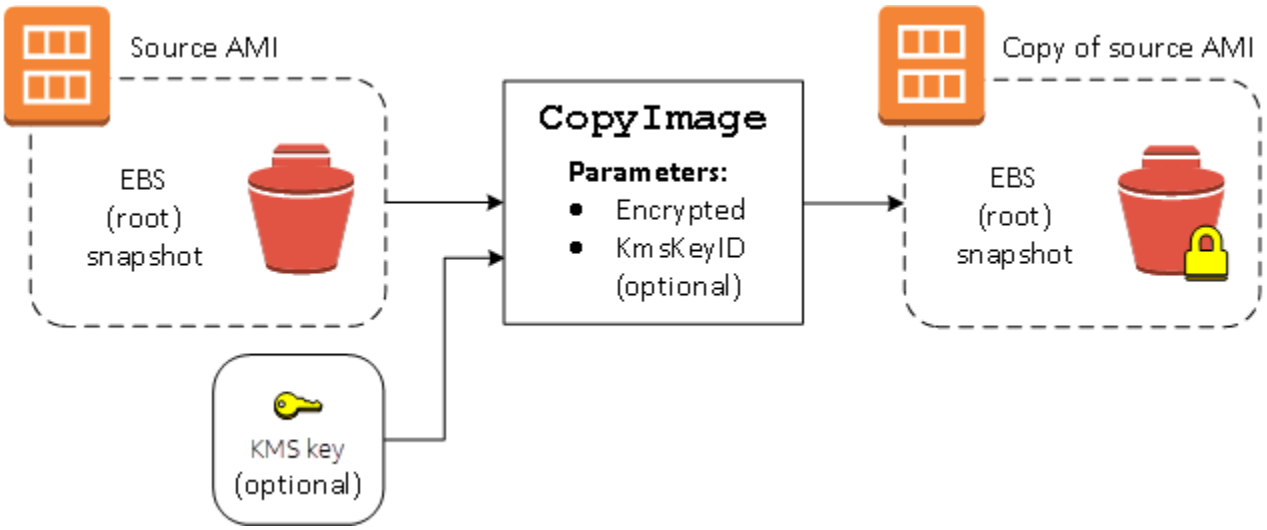
La seguente sezione offre un esempio della copia di un'AMI utilizzando parametri di crittografia non predefiniti, il che porta a una modifica dello stato di crittografia.

Per istruzioni dettagliate sull'utilizzo della console, consulta Copiare un'AMI Amazon EC2.

Crittografia di un'immagine non crittografata durante la copia

In questo scenario, un'AMI supportata da uno snapshot di root non crittografato viene copiato in un'AMI con uno snapshot di root crittografato. L'operazione `CopyImage` viene richiamata con due parametri di crittografia, inclusa una chiave gestita dal cliente. Di conseguenza, lo stato di crittografia dello snapshot root cambia, in modo che l'AMI di destinazione sia supportata da uno snapshot root contenente gli stessi dati dello snapshot di origine, ma crittografato utilizzando la chiave specificata. Ti verranno addebitati costi di archiviazione per gli snapshot in entrambe le AMI, nonché addebiti per tutte le istanze avviate da entrambe le AMI.

> **Note**
>
> L'abilitazione della crittografia per impostazione predefinita ha lo stesso effetto dell'impostazione del parametro `Encrypted` a `true` per tutti gli snapshot nell'AMI.



L'impostazione del parametro `Encrypted` consente di crittografare il singolo snapshot per questa istanza. Se non specifichi il parametro `KmsKeyId`, per crittografare la copia snapshot viene utilizzata la chiave gestita dal cliente di default.

> **Note**
>
> Puoi inoltre copiare un'immagine con più snapshot e configurare lo stato di crittografia di ognuno.

Informazioni sull'utilizzo delle AMI condivise in Amazon EC2

Un'AMI condivisa è un'AMI creata da uno sviluppatore e resa disponibile per gli altri sviluppatori. Uno dei modi più semplici per iniziare a familiarizzare con Amazon EC2, consiste nell'utilizzare un'AMI condivisa con i componenti necessari e procedere poi all'aggiunta dei contenuti personalizzati. Puoi anche creare AMI personalizzate e condividerle con altri utenti.

Utilizza le AMI condivise a tuo rischio e pericolo. Amazon non può garantire l'integrità o la sicurezza delle AMI condivise da altri utenti Amazon EC2. Di conseguenza, ti consigliamo di trattare le AMI condivise come faresti con qualsiasi altro codice esterno che pensi di distribuire nel tuo data center con la dovuta cautela. Ti consigliamo di scaricare le AMI da un'origine attendibile, come un provider verificato.

Fornitore verificato

Nella console Amazon EC2, le AMI pubbliche di proprietà di Amazon o di un partner Amazon verificato sono contrassegnate dalla dicitura Verified provider (fornitore verificato).

Puoi anche utilizzare il AWS CLI comando describe-images per identificare le AMI pubbliche che provengono da un provider verificato. Le immagini pubbliche di Amazon o di un partner verificato hanno un proprietario con alias, `amazon`, `aws-backup-vault` o `aws-marketplace`. Nell'output della CLI, vengono visualizzati questi valori per `ImageOwnerAlias`. Gli altri utenti non possono creare un alias per le proprie AMI. Ciò consente di cercare con facilità le AMI di Amazon o dei fornitori verificati.

Per diventare un fornitore verificato, è necessario registrarsi come venditore sul Marketplace AWS. Una volta effettuata la registrazione, è possibile inserire l'AMI nell'elenco di Marketplace AWS. Per ulteriori informazioni, consulta Guida introduttiva come venditore e AMI-based prodotti nella Guida per i venditori. Marketplace AWS

Argomenti sulle AMI condivise

- Trova AMI condivise da usare per le istanze Amazon EC2
- Preparati a usare AMI condivise per Linux
- Controlla il rilevamento e l'uso delle AMI in Amazon EC2 con le AMI consentite
- Rendi la tua AMI disponibile pubblicamente per l'utilizzo in Amazon EC2
- Capire il blocco dell'accesso pubblico per le AMI
- Condivisione di un'AMI con organizzazioni e unità organizzative

- Condividi un'AMI con uno specifico AWS account
- Annulla la condivisione di un'AMI con la tua Account AWS
- Consigli per creare AMI Linux condivise

Se stai cercando informazioni su altri argomenti

- Per informazioni sulla creazione di un'AMI, consulta the section called “Crea un' S3-backed AMI Amazon” o the section called “Creare un'AMI”.
- Per ulteriori informazioni sulla creazione, la distribuzione e la gestione delle applicazioni in Marketplace AWS, consulta la Documentazione di Marketplace AWS.

Trova AMI condivise da usare per le istanze Amazon EC2

Puoi utilizzare la console Amazon EC2 o la riga di comando per cercare AMI condivise pubbliche o private da usare con le tue istanze Amazon EC2.

Le AMI sono una risorsa basata sulla regione. Quindi, quando cerchi un'AMI condivisa (pubblica o privata), devi cercarla nella stessa regione da cui viene condivisa. Per rendere un'AMI disponibile in un'altra regione, copiala nella regione desiderata e condividila. Per ulteriori informazioni, consulta Copiare un'AMI Amazon EC2.

Console

La console fornisce un campo filtro AMI. Puoi anche restringere le tue ricerche utilizzando i filtri forniti nel campo Cerca.

Per cercare un'AMI condivisa

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Nel primo filtro, scegli una delle seguenti opzioni:
   - Immagini private: elenca tutte le AMI condivise con te.
   - Immagini pubbliche: elenca tutte le AMI pubbliche.
4. (Facoltativo) Per visualizzare solo le immagini pubbliche di Amazon, seleziona il campo Cerca, quindi, dalle opzioni del menu, seleziona Alias proprietario, quindi = e infine amazon.
5. (Facoltativo) Aggiungi filtri per restringere la ricerca alle AMI che soddisfano i tuoi requisiti.

Per trovare un'AMI pubblica condivisa da un fornitore verificato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione seleziona AMI Catalog (catalogo AMI).
3. Scegli Community AMIs (AMI community).
4. Nel riquadro Affina risultati, seleziona Fornitore verificato. L'etichetta Verified provider (fornitore verificato) indica le AMI provenienti da Amazon o da un partner verificato.

AWS CLI

Utilizzare il comando describe-images per visualizzare un elenco delle AMI. Puoi definire l'ambito dell'elenco in base ai tipi di AMI di tuo interesse, come illustrato negli esempi seguenti.

Per elencare tutte le AMI pubbliche

Il comando seguente consente di elencare tutte le AMI pubbliche, incluse quelle di tua proprietà.

```
aws ec2 describe-images --executable-users all
```

Per elencare le AMI con permessi di avvio espliciti

Il comando seguente consente di elencare le AMI per le quali disponi di permessi di avvio espliciti. Questo elenco non include le AMI di tua proprietà.

```
aws ec2 describe-images --executable-users self
```

Per elencare le AMI di proprietà di fornitori verificati

Il comando seguente consente di elencare le AMI di proprietà di fornitori verificati. Le AMI pubbliche di proprietà di fornitori verificati (sia Amazon che fornitori verificati) hanno un proprietario con alias, visualizzato come `amazon`, `aws-backup-vault` o `aws-marketplace` nel campo dell'account. Ciò che consente di cercare con facilità le AMI di fornitori verificati. Gli altri utenti non possono creare un alias per le proprie AMI.

```
aws ec2 describe-images \
    --owners amazon aws-marketplace \
    --query 'Images[*].[ImageId]' \
    --output text
```

Per elencare le AMI di proprietà di un account

Il comando seguente consente di elencare le AMI di proprietà dell' Account AWS specificato.

```
aws ec2 describe-images --owners 123456789012
```

Per definire l'ambito delle AMI tramite un filtro

Per ridurre il numero delle AMI visualizzate, utilizza un filtro per visualizzare un elenco con soltanto i tipi di AMI desiderati. Ad esempio, utilizza il seguente filtro per visualizzare solo le EBS-backed AMI.

```
--filters "Name=root-device-type,Values=ebs"
```

PowerShell

Usa il Get-EC2Image cmdlet (Tools for Windows PowerShell) per elencare le AMI. Puoi definire l'ambito dell'elenco in base ai tipi di AMI di tuo interesse, come illustrato negli esempi seguenti.

Per elencare tutte le AMI pubbliche

Il comando seguente consente di elencare tutte le AMI pubbliche, incluse quelle di tua proprietà.

```
Get-EC2Image -ExecutableUser all
```

Per elencare le AMI con permessi di avvio espliciti

Il comando seguente consente di elencare le AMI per le quali disponi di permessi di avvio espliciti. Questo elenco non include le AMI di tua proprietà.

```
Get-EC2Image -ExecutableUser self
```

Per elencare le AMI di proprietà di fornitori verificati

Il comando seguente consente di elencare le AMI di proprietà di fornitori verificati. Le AMI pubbliche di proprietà di fornitori verificati (sia Amazon che fornitori verificati) hanno un proprietario con alias, visualizzato come `amazon`, `aws-backup-vault` o `aws-marketplace` nel campo dell'account. Ciò che consente di cercare con facilità le AMI di fornitori verificati. Gli altri utenti non possono creare un alias per le proprie AMI.

```
Get-EC2Image -Owner amazon aws-marketplace
```

Per elencare le AMI di proprietà di un account

Il comando seguente consente di elencare le AMI di proprietà dell' Account AWS specificato.

```
Get-EC2Image -Owner 123456789012
```

Per definire l'ambito delle AMI tramite un filtro

Per ridurre il numero delle AMI visualizzate, utilizza un filtro per visualizzare un elenco con soltanto i tipi di AMI desiderati. Ad esempio, utilizza il seguente filtro per visualizzare solo le AMI. EBS-backed

```
-Filter @{Name="root-device-type"; Values="ebs"}
```

Preparati a usare AMI condivise per Linux

Prima di utilizzare un'AMI per Linux condivisa, completa le fasi seguenti per verificare che non siano presenti credenziali preinstallate che consentirebbero l'accesso indesiderato di una terza parte all'istanza e che non sia stato preconfigurato l'accesso remoto che potrebbe consentire l'invio di dati sensibili a una terza parte. Controlla la documentazione della distribuzione Linux utilizzata dall'AMI per informazioni su come migliorare la sicurezza del sistema.

Per assicurarti di non perdere accidentalmente l'accesso all'istanza, ti consigliamo di avviare due sessioni SSH e di tenere la seconda sessione aperta finché non hai rimosso le credenziali che non riconosci e finché non hai verificato di poter accedere all'istanza tramite SSH.

1. Identificare e disabilitare le chiavi SSH pubbliche non autorizzate. L'unica chiave presente nel file deve essere quella utilizzata per avviare l'AMI. Il comando seguente consente di individuare i file `authorized_keys`:

   ```
   [ec2-user ~]$ sudo find / -name "authorized_keys" -print -exec cat {} \;
   ```

2. Disabilitare l'autenticazione basata su password per l'utente root. Aprire il file `sshd_config` e modificare la riga `PermitRootLogin` come segue:

   ```
   PermitRootLogin without-password
   ```

In alternativa, è possibile disabilitare la funzione di accesso all'istanza come utente root:

```
PermitRootLogin No
```

Riavviare il servizio sshd.

3. Controllare la presenza di altri utenti in grado di accedere all'istanza. Gli utenti con privilegi superuser sono particolarmente pericolosi. Rimuovere o bloccare la password degli account sconosciuti.
4. Verificare la presenza di porte aperte inutilizzate e con in esecuzione servizi di rete in attesa di connessioni in entrata.
5. Per impedire la registrazione remota preconfigurata, elimina il file di configurazione esistente e riavviare il servizio `rsyslog`. Ad esempio:

```
[ec2-user ~]$ sudo rm /etc/rsyslog.conf
[ec2-user ~]$ sudo service rsyslog restart
```

6. Verifica che tutti i processi cron siano legittimi.

Se rilevi un'AMI pubblica che ritieni rappresentare un rischio per la sicurezza, contatta il team di sicurezza AWS . Per ulteriori informazioni, visita il Centro di Sicurezza AWS.

Controlla il rilevamento e l'uso delle AMI in Amazon EC2 con le AMI consentite

Per controllare il rilevamento e l'uso delle Amazon Machine Image (AMI) da parte degli utenti nel tuo Account AWS, puoi utilizzare la funzionalità AMI consentite. Puoi specificare i criteri che le AMI devono soddisfare per essere visibili e disponibili all'interno del tuo account. Quando i criteri sono abilitati, gli utenti che avviano le istanze vedranno e avranno accesso solo alle AMI che soddisfano i criteri specificati. Ad esempio, è possibile specificare un elenco di provider di AMI affidabili come criteri, e solo le AMI di questi provider saranno visibili e disponibili per l'uso.

Prima di abilitare le impostazioni delle AMI consentite, puoi abilitare la modalità di controllo per visualizzare in anteprima quali AMI saranno visibili e disponibili per l'uso (se presenti). Ciò consente di affinare i criteri in base alle esigenze per garantire che solo le AMI previste siano visibili e disponibili per gli utenti del tuo account. Inoltre, puoi utilizzare il comando describe-instance-image-metadata per identificare le istanze avviate con AMI che non soddisfano i criteri specificati. Queste

informazioni possono aiutarti a decidere se aggiornare le configurazioni di avvio per utilizzare AMI conformi (ad esempio, specificando una AMI diversa in un modello di lancio) o modificare i criteri per consentire queste AMI.

Puoi specificare le impostazioni delle AMI consentite a livello di account, direttamente nell'account o utilizzando una policy dichiarativa. Queste impostazioni devono essere configurate in ogni Regione AWS in cui si desidera controllare l'utilizzo delle AMI. L'utilizzo di una policy dichiarativa consente di applicare le impostazioni contemporaneamente su più regioni, nonché su più account. Quando viene utilizzata una policy dichiarativa, non è possibile modificare le impostazioni direttamente all'interno di un account. Questo argomento illustra la modalità di configurazione delle impostazioni direttamente all'interno di un account. Per informazioni sull'utilizzo delle policy dichiarative, consulta Policy dichiarative nella Guida per l'utente di AWS Organizations .

> **Note**
>
> La funzionalità delle AMI consentite controlla solo il rilevamento e l'utilizzo di AMI pubbliche o AMI condivise con l'account. Non si limita alle AMI di proprietà dell'account. Indipendentemente dai criteri impostati, le AMI create dal tuo account sono sempre rilevabili e utilizzabili dagli utenti nel tuo account.

Principali vantaggi delle AMI consentite

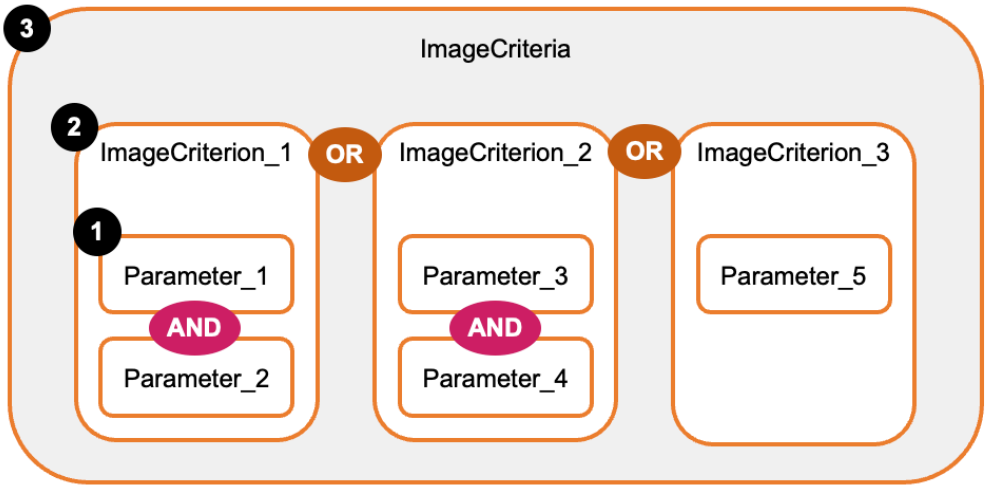
- Conformità e sicurezza: gli utenti possono rilevare e utilizzare solo le AMI che soddisfano i criteri specificati, riducendo il rischio di utilizzo di AMI non conformi.
- Gestione efficiente: riducendo il numero di AMI consentite, la gestione di quelle rimanenti diventa più semplice ed efficiente.
- Implementazione centralizzata a livello di account: configurare le impostazioni delle AMI consentite a livello di account, direttamente all'interno dell'account o tramite una policy dichiarativa. Ciò fornisce un modo centralizzato ed efficiente per controllare l'utilizzo delle AMI sull'intero account.

Indice

- Come funzionano le AMI consentite
- Best practice per l'implementazione di AMI consentite
- Autorizzazioni IAM richieste
- Gestisci le impostazioni per le AMI consentite

Come funzionano le AMI consentite

Per controllare quali AMI possono essere individuate e utilizzate nel tuo account, definisci una serie di criteri in base ai quali valutare le AMI. I criteri sono costituiti da uno o più `ImageCriterion`, come mostra il diagramma seguente. Il diagramma è seguito da una spiegazione.



La configurazione ha tre livelli:

- 1 – Valori dei parametri
  - Multi-value parametri:
    - `ImageProviders`
    - `ImageNames`
    - `MarketplaceProductCodes`

      Un'AMI può corrispondere a qualsiasi valore entro un parametro per essere consentita.

      Esempio: `ImageProviders` = `amazon` OR account `111122223333` OR account `444455556666` (La logica di valutazione dei valori dei parametri non è riportata nel diagramma).
    - `ImageWatermarks`
  - Single-value parametri:
    - `CreationDateCondition`
    - `DeprecationTimeCondition`
- 2 – `ImageCriterion`
  - Raggruppa più parametri con logica AND.

  - Un'AMI deve corrispondere a tutti i parametri all'interno di un `ImageCriterion` per essere consentita.
  - Esempio: `ImageProviders` = `amazon` AND `CreationDateCondition` = 300 giorni o meno
- 3 – `ImageCriteria`
  - Raggruppa più `ImageCriterion` con logica OR.
  - Un'AMI può corrispondere qualsiasi `ImageCriterion` per essere consentita.
  - Crea la configurazione completa rispetto alla quale vengono valutate le AMI.

Argomenti

- Parametri per le AMI consentite
- Configurazione delle AMI consentite
- Come vengono valutati i criteri
- Limits
- Operazioni per le AMI consentite

Parametri per le AMI consentite

Puoi configurare i seguenti parametri per creare `ImageCriterion`:

`ImageProviders`

I fornitori di AMI le cui AMI sono consentite.

I valori validi sono alias definiti da AWS e Account AWS ID come segue:

- `amazon`: un alias che identifica le AMI create da Amazon o da fornitori verificati
- `aws-marketplace`— Un alias che identifica le AMI create da provider verificati nel Marketplace AWS
- `aws-backup-vault` – Un alias che identifica le AMI di backup che risiedono in account di vault logicamente isolata di AWS di ripristino. Se utilizzi la funzionalità AWS Backup logically air-gapped vault, assicurati che questo alias sia incluso come provider AMI.
- Account AWS ID: uno o più ID a 12 cifre Account AWS
- `none` – Indica che solo le AMI create dal tuo account possono essere rilevate e utilizzate. Le AMI pubbliche o condivise non possono essere rilevate e utilizzate. Quando specificato, non è possibile specificare altri criteri.

`ImageNames`

I nomi delle AMI consentite, utilizzando corrispondenze esatte o caratteri jolly (`?` o `*`).

`MarketplaceProductCodes`

I codici di Marketplace AWS prodotto per le AMI consentite.

`CreationDateCondition`

L'età massima per le AMI consentite.

`DeprecationTimeCondition`

Il periodo massimo di obsolescenza per le AMI consentite.

`ImageWatermarks`

Un elenco di filtri per filigrane. Il filtro consente un'AMI se una filigrana sull'AMI corrisponde a qualsiasi voce del filtro (logica OR). Ogni filtro può includere i seguenti campi:

- `WatermarkKey`— La chiave della filigrana da abbinare () `account-id:watermark-name`
- `SourceImageRegion`— La regione dell'AMI a cui hai originariamente associato la filigrana
- `MaximumDaysSinceSourceImageCreated`— L'età massima dell'AMI di origine al momento dell'applicazione della filigrana
- `MaximumDaysSinceWatermarkCreated`— Il numero massimo di giorni da quando hai applicato la filigrana

Per i valori e i vincoli validi per ciascun criterio, consulta ImageCriterionRequest l'Amazon EC2 API Reference.

Configurazione delle AMI consentite

La configurazione di base per le AMI consentite è la configurazione `ImageCriteria` che definisce i criteri per le AMI consentite. La seguente struttura JSON indica i parametri che possono essere specificati:

```
{
    "State": "enabled" | "disabled" | "audit-mode",
    "ImageCriteria" : [
        {
            "ImageProviders": ["string",...],
            "MarketplaceProductCodes": ["string",...],
            "ImageNames":["string",...],
```

```
            "CreationDateCondition" : {
                "MaximumDaysSinceCreated": integer
            },
            "DeprecationTimeCondition" : {
                "MaximumDaysSinceDeprecated": integer
            },
            "ImageWatermarks": [
                {
                    "WatermarkKey": "string",
                    "SourceImageRegion": "string",
                    "MaximumDaysSinceSourceImageCreated": integer,
                    "MaximumDaysSinceWatermarkCreated": integer
                },...
            ]
         },
         ...
}
```

ImageCriteria esempio

L'`ImageCriteria`esempio seguente ne configura cinque`ImageCriterion`. Un'AMI è consentita se corrisponde a uno di questi `ImageCriterion`. Per informazioni su come vengono valutati i criteri, consulta Come vengono valutati i criteri.

```
{
    "ImageCriteria": [
        // ImageCriterion 1: Allow Marketplace AWS AMIs with product code
 "abcdefg1234567890"
        {
            "MarketplaceProductCodes": [
                "abcdefg1234567890"
            ]
        },
        // ImageCriterion 2: Allow AMIs from providers whose accounts are
        // "123456789012" OR "123456789013" AND AMI age is less than 300 days
        {
            "ImageProviders": [
                "123456789012",
                "123456789013"
            ],
            "CreationDateCondition": {
                "MaximumDaysSinceCreated": 300
            }
```

```
        },
        // ImageCriterion 3: Allow AMIs from provider whose account is "123456789014"
        // AND with names following the pattern "golden-ami-*"
        {
            "ImageProviders": [
                "123456789014"
            ],
            "ImageNames": [
                "golden-ami-*"
            ]
        },
        // ImageCriterion 4: Allow AMIs from Amazon or verified providers
        // AND which aren't deprecated
        {
            "ImageProviders": [
                "amazon"
            ],
            "DeprecationTimeCondition": {
                "MaximumDaysSinceDeprecated": 0
            }
        },
        // ImageCriterion 5: Allow AMIs that carry an approved watermark
        // from account "111122223333" AND the watermark was applied less than 90 days
 ago
        {
            "ImageWatermarks": [
                {
                    "WatermarkKey": "111122223333:prod-baseline",
                    "MaximumDaysSinceWatermarkCreated": 90
                }
            ]
        }
    ]
}
```

Come vengono valutati i criteri

La seguente tabella illustra le regole di valutazione che determinano se un'AMI è consentita, mostrando come l'operatore AND o OR viene applicato a ciascun livello:

Livello di valutazione	Operatore	Requisito per essere un'AMI consentita
Valori dei parametri per `ImageProviders`, `ImageNames` `MarketplaceProductCodes`, e `ImageWatermarks`	`OR`	L'AMI deve corrispondere almeno a un valore in ogni elenco di parametri
`ImageCriterion`	`AND`	L'AMI deve corrispondere a tutti i parametri di ogni `ImageCriterion`
`ImageCriteria`	`OR`	L'AMI deve rispettare uno qualsiasi dei `ImageCriterion`

Utilizzando le regole di valutazione precedenti, vediamo come applicarle all'ImageCriteria esempio:

- `ImageCriterion1`: Consente le AMI con il codice del Marketplace AWS prodotto `abcdefg1234567890`

  `OR`

- `ImageCriterion` 2: consente le AMI che soddisfano entrambi questi criteri:
  - Di proprietà di uno degli account `123456789012` `OR` `123456789013`
    - `AND`
  - Creato negli ultimi 300 giorni

  `OR`

- `ImageCriterion` 3: consente le AMI che soddisfano entrambi questi criteri:
  - Di proprietà dell'account `123456789014`
    - `AND`
  - Denominato con il modello `golden-ami-*`

  `OR`

- `ImageCriterion` 4: consente le AMI che soddisfano entrambi questi criteri:
  - Pubblicato da Amazon o da fornitori verificati (specificato dall'alias `amazon`)
    - `AND`
  - Non obsoleto (massimo giorni dalla data di obsolescenza `0`)

  `OR`
- `ImageCriterion5`: Consente le AMI con una filigrana corrispondente a:
  - Chiave Watermark `111122223333:prod-baseline`
    - `AND`
  - Hai applicato la filigrana meno di 90 giorni fa

Limits

I `ImageCriteria` possono includere fino a:

- 10 `ImageCriterion`

Ogni `ImageCriterion` può includere fino a:

- 200 valori per `ImageProviders`
- 50 valori per `ImageNames`
- 50 valori per `MarketplaceProductCodes`
- 50 valori per `ImageWatermarks`

Esempio di limiti

Utilizzando i ImageCriteria esempio precedenti:

- Ce ne sono 5`ImageCriterion`. È possibile aggiungerne fino a 5 alla richiesta per raggiungere il limite di 10.
- Nel primo `ImageCriterion`, c'è 1 valore per `MarketplaceProductCodes`. È possibile aggiungere fino a 49 elementi a questo `ImageCriterion` per raggiungere il limite di 50.
- Nel secondo `ImageCriterion`, ci sono 2 valori per `ImageProviders`. È possibile aggiungere fino a 198 elementi a questo `ImageCriterion` per raggiungere il limite di 200.

- Nel terzo `ImageCriterion`, c'è 1 valore per `ImageNames`. È possibile aggiungere fino a 49 elementi a questo `ImageCriterion` per raggiungere il limite di 50.

Operazioni per le AMI consentite

La funzionalità AMI consentite dispone di tre stati operativi per la gestione dei criteri delle immagini: abilitato, disabilitato e modalità di controllo. Queste consentono di abilitare o disabilitare i criteri relativi alle immagini o di rivederli secondo necessità.

Abilitato

Quando le AMI consentite sono abilitate:

- Vengono applicati i `ImageCriteria`.
- Solo le AMI consentite sono rilevabili nella console EC2 e dalle API che utilizzano immagini (ad esempio, che descrivono, copiano, archiviano o eseguono altre azioni che utilizzano immagini).
- Le istanze possono essere avviate solo utilizzando le AMI consentite.

Disabilitato

Quando le AMI consentite sono disabilitate:

- Non vengono applicati i `ImageCriteria`.
- Non viene posta alcuna restrizione alla rilevabilità o all'utilizzo delle AMI.

Modalità di controllo

Nella modalità di controllo:

- Vengono applicati i `ImageCriteria`, ma non viene posta alcuna restrizione alla rilevabilità o all'utilizzo delle AMI.
- Nella console EC2, per ogni AMI, il campo Immagine consentita mostra Sì o No per indicare se l'AMI sarà rilevabile e disponibile per gli utenti nell'account quando le AMI consentite sono abilitate.
- Nella riga del comando, la risposta all'operazione `describe-image` include `"ImageAllowed": true` o `"ImageAllowed": false` per indicare se l'AMI sarà rilevabile e disponibile per gli utenti nell'account quando le AMI consentite sono abilitate.

- Nella console EC2, nel catalogo AMI viene visualizzato il messaggio Non consentite accanto alle AMI che non saranno rilevabili o disponibili per gli utenti nell'account quando la funzionalità AMI consentite è abilitata.

Best practice per l'implementazione di AMI consentite

Quando implementi le AMI consentite, prendi in considerazione queste best practice per garantire una transizione senza intoppi e ridurre al minimo le potenziali interruzioni del tuo AWS ambiente.

1. Abilitare la modalità di controllo

   Iniziare abilitando le AMI consentite nella modalità di controllo. Questo stato consente di vedere quali AMI sarebbero interessate dai tuoi criteri senza limitare effettivamente l'accesso, garantendo un periodo di valutazione privo di rischi.

2. Impostare i criteri delle AMI consentite

   Stabilire con attenzione quali provider di AMI sono in linea con le politiche di sicurezza, i requisiti di conformità e le esigenze operative della tua organizzazione.

   > **Note**
   >
   > Quando si utilizzano servizi AWS gestiti, come Amazon ECS, Amazon EKS o AWS Lambda Managed Instances, consigliamo di specificare l'`amazon`alias per consentire le AMI create da. AWS Questi servizi dipendono dalle AMI per avviare le istanze. Amazon-published
   > Presta attenzione quando imposti restrizioni `CreationDateCondition` per qualsiasi AMI. L'impostazione di condizioni di data eccessivamente restrittive (ad esempio, le AMI devono avere meno di 5 giorni) può causare errori di avvio dell'istanza se le AMI, fornite AWS o da altri provider, non vengono aggiornate entro l'intervallo di tempo specificato. Consigliamo di abbinare `ImageNames` con `ImageProviders` per un controllo e una specificità migliori. Utilizzare `ImageNames` da solo potrebbe non identificare in modo univoco un'AMI.

3. Verificare l'impatto sui processi aziendali previsti

   Puoi utilizzare la console o la CLI per identificare le istanze avviate con AMI che non soddisfano i criteri specificati. Queste informazioni possono aiutarti a decidere se aggiornare le configurazioni

di avvio per utilizzare AMI conformi (ad esempio, specificando una AMI diversa in un modello di lancio) o modificare i criteri per consentire queste AMI.

Console: utilizza la AWS Config regola ec2-instance-launched-with-allowed-ami per verificare se le istanze in esecuzione o interrotte sono state avviate con AMI che soddisfano i criteri delle AMI consentite. La regola è NON_COMPLIANT se un'AMI non soddisfa i criteri delle AMI consentite e COMPLIANT se li soddisfa. La regola funziona solo quando l'impostazione AMI consentite è impostata su Abilitato o Modalità di controllo.

CLI: eseguire il comando describe-instance-image-metadata e filtrare la risposta per identificare le istanze avviate con AMI che non soddisfano i criteri specificati.

Per le istruzioni relative a console e CLI, consulta Trova le istanze avviate da AMI che non sono consentite.

4. Abilitare le AMI consentite

   Dopo aver verificato che i criteri non influiranno negativamente sui processi aziendali previsti, abilita le AMI consentite.

5. Monitorare gli avvii delle istanze

   Continua a monitorare i lanci di istanze dalle AMI nelle tue applicazioni e nei servizi AWS gestiti che utilizzi, come Amazon EMR, Amazon ECR, Amazon EKS e. AWS Elastic Beanstalk Verificare la presenza di eventuali problemi imprevisti e apportare le modifiche necessarie ai criteri delle AMI consentite.

6. Pilota nuove AMI

   Per testare le AMI di terze parti che non sono conformi alle attuali impostazioni delle AMI consentite, consiglia i seguenti approcci: AWS

   - Usa un altro Account AWS: crea un account senza accesso alle tue risorse aziendali critiche. Assicurati che l'impostazione AMI consentite non sia abilitata in questo account o che le AMI che vuoi testare siano esplicitamente consentite, in modo da poterle testare.
   - Effettua il test in un'altra regione Regione AWS: utilizza una regione in cui sono disponibili le AMI di terze parti, ma in cui non hai ancora abilitato le impostazioni delle AMI consentite.

   Questi approcci aiutano a garantire la sicurezza delle risorse aziendali critiche durante il test di nuove AMI.

Autorizzazioni IAM richieste

Per usare la funzionalità AMI consentite, sono necessarie le seguenti autorizzazioni relative a IAM:

- `GetAllowedImagesSettings`
- `EnableAllowedImagesSettings`
- `DisableAllowedImagesSettings`
- `ReplaceImageCriteriaInAllowedImagesSettings`

Gestisci le impostazioni per le AMI consentite

Puoi gestire le impostazioni per le AMI consentite. Queste impostazioni sono specifiche per ogni regione e per ogni account.

Processi

- Abilitare le AMI consentite
- Imposta i criteri delle AMI consentite
- Disabilitare le AMI consentite
- Ottieni i criteri delle AMI consentite
- Trova le AMI consentite
- Trova le istanze avviate da AMI che non sono consentite

Abilitare le AMI consentite

Puoi abilitare le AMI consentite e specificare i criteri delle AMI consentite. Consigliamo di iniziare in modalità di controllo, che mostra quali AMI sarebbero interessate dai criteri senza limitare effettivamente l'accesso.

Console

Per abilitare le AMI consentite

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione seleziona Pannello di controllo.
3. Nella scheda Attributi dell'account, in Impostazioni, scegli AMI consentite.

4. Nella scheda AMI consentite, seleziona Gestisci.
5. Per Impostazioni AMI consentite, seleziona Modalità di controllo o Abilitato. Consigliamo di iniziare in modalità di controllo, testare i criteri e poi tornare a questo passaggio per abilitare le AMI consentite.
6. (Facoltativo) Per i criteri delle AMI, inserisci i criteri in formato JSON.
7. Scegliere Aggiorna.

AWS CLI

Per abilitare le AMI consentite

Utilizza il comando enable-allowed-images-settings.

```
aws ec2 enable-allowed-images-settings --allowed-images-settings-state enabled
```

Per abilitare la modalità di controllo, invece, specifica `audit-mode` invece di `enabled`.

```
aws ec2 enable-allowed-images-settings --allowed-images-settings-state audit-mode
```

PowerShell

Per abilitare le AMI consentite

Utilizza il cmdlet Enable-EC2AllowedImagesSetting.

```
Enable-EC2AllowedImagesSetting -AllowedImagesSettingsState enabled
```

Per abilitare la modalità di controllo, invece, specifica `audit-mode` invece di `enabled`.

```
Enable-EC2AllowedImagesSetting -AllowedImagesSettingsState audit-mode
```

Imposta i criteri delle AMI consentite

Dopo aver abilitato le AMI consentite, puoi impostare o sostituire i criteri delle AMI consentite.

Per la corretta configurazione e i valori validi, consulta Configurazione delle AMI consentite e Parametri per le AMI consentite.

Console

Per impostare i criteri delle AMI consentite

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione seleziona Pannello di controllo.
3. Nella scheda Attributi dell'account, in Impostazioni, scegli AMI consentite.
4. Nella scheda AMI consentite, seleziona Gestisci.
5. Per i criteri delle AMI, inserisci i criteri in formato JSON.
6. Scegliere Aggiorna.

AWS CLI

Per impostare i criteri delle AMI consentite

Utilizza il comando replace-image-criteria-in-allowed-images-settings e specifica il file JSON che contiene i criteri delle AMI consentite.

```
aws ec2 replace-image-criteria-in-allowed-images-settings --cli-input-json
 file://file_name.json
```

PowerShell

Per impostare i criteri delle AMI consentite

Utilizza il Set-EC2ImageCriteriaInAllowedImagesSetting cmdlet e specifica il file JSON che contiene i criteri delle AMI consentite.

```
$imageCriteria = Get-Content -Path .\file_name.json | ConvertFrom-Json
Set-EC2ImageCriteriaInAllowedImagesSetting -ImageCriterion $imageCriteria
```

Disabilitare le AMI consentite

Puoi disabilitare le AMI consentite come segue.

Console

Per disabilitare le AMI consentite

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione seleziona Pannello di controllo.
3. Nella scheda Attributi dell'account, in Impostazioni, scegli AMI consentite.
4. Nella scheda AMI consentite, seleziona Gestisci.
5. Per le impostazioni delle AMI consentite, scegli Disabilitato.
6. Scegliere Aggiorna.

AWS CLI

Per disabilitare le AMI consentite

Utilizza il comando disable-allowed-images-settings.

```
aws ec2 disable-allowed-images-settings
```

PowerShell

Per disabilitare le AMI consentite

Utilizza il cmdlet Disable-EC2AllowedImagesSetting.

```
Disable-EC2AllowedImagesSetting
```

Ottieni i criteri delle AMI consentite

Puoi ottenere lo stato corrente dell'impostazione delle AMI consentite e dei criteri delle AMI consentite.

Console

Per ottenere lo stato e i criteri delle AMI consentite

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione seleziona Pannello di controllo.

3. Nella scheda Attributi dell'account, in Impostazioni, scegli AMI consentite.
4. Nella scheda AMI consentite, l'impostazione AMI consentite è impostata su Abilitato, Disabilitato o Modalità di controllo.
5. Se lo stato delle AMI consentite è Abilitato o Modalità di controllo, i criteri AMI visualizzano i criteri AMI in formato JSON.

AWS CLI

Per ottenere lo stato e i criteri delle AMI consentite

Utilizza il comando get-allowed-images-settings.

```
aws ec2 get-allowed-images-settings
```

Nell'output dell'esempio seguente, lo stato è `audit-mode` e i criteri per le immagini sono impostati nell'account.

```
{
    "State": "audit-mode",
    "ImageCriteria": [
        {
            "MarketplaceProductCodes": [
                "abcdefg1234567890"
            ]
        },
        {
            "ImageProviders": [
                "123456789012",
                "123456789013"
            ],
            "CreationDateCondition": {
                "MaximumDaysSinceCreated": 300
            }
        },
        {
            "ImageProviders": [
                "123456789014"
            ],
            "ImageNames": [
                "golden-ami-*"
```

```
            ]
        },
        {
            "ImageProviders": [
                "amazon"
            ],
            "DeprecationTimeCondition": {
                "MaximumDaysSinceDeprecated": 0
            }
        }
    ],
    "ManagedBy": "account"
}
```

PowerShell

Per ottenere lo stato e i criteri delle AMI consentite

Utilizza il cmdlet Get-EC2AllowedImagesSetting.

```
Get-EC2AllowedImagesSetting | Select-Object `
    State, `
    ManagedBy, `
    @{Name='ImageProviders'; Expression={($_.ImageCriteria.ImageProviders)}}, `
    @{Name='MarketplaceProductCodes';
 Expression={($_.ImageCriteria.MarketplaceProductCodes)}}, `
    @{Name='ImageNames'; Expression={($_.ImageCriteria.ImageNames)}}, `
    @{Name='MaximumDaysSinceCreated';
 Expression={($_.ImageCriteria.CreationDateCondition.MaximumDaysSinceCreated)}}, `
    @{Name='MaximumDaysSinceDeprecated';
 Expression={($_.ImageCriteria.DeprecationTimeCondition.MaximumDaysSinceDeprecated)}}
```

Nell'output dell'esempio seguente, lo stato è `audit-mode` e i criteri per le immagini sono impostati nell'account.

```
State      : audit-mode
ManagedBy  : account
ImageProviders            : {123456789012, 123456789013, 123456789014, amazon}
MarketplaceProductCodes   : {abcdefg1234567890}
ImageNames                : {golden-ami-*}
MaximumDaysSinceCreated   : 300
MaximumDaysSinceDeprecated: 0
```

Trova le AMI consentite

Puoi trovare le AMI consentite o non consentite in base ai criteri delle AMI consentite attuali.

> **Note**
>
> Abilita le AMI consentite nella modalità di controllo.

Console

Per controllare se un'AMI soddisfa i criteri delle AMI consentite

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI.
4. Nella scheda Dettagli (se hai selezionato la casella di spunta) o nell'area di riepilogo (se hai selezionato l'ID dell'AMI), trova il campo Immagine consentita.
   - Sì: l'AMI soddisfa i criteri per le AMI consentite. Questa AMI sarà disponibile per gli utenti del tuo account dopo aver abilitato le AMI consentite.
   - No: l'AMI non soddisfa i criteri per le AMI consentite.
5. Nel riquadro di navigazione seleziona AMI Catalog (catalogo AMI).

   Un'AMI contrassegnata come Non consentita indica un'AMI che non soddisfa i criteri delle AMI consentite. Questa AMI non sarà visibile o disponibile per gli utenti nel tuo account quando le AMI consentite sono abilitate.

AWS CLI

Per controllare se un'AMI soddisfa i criteri delle AMI consentite

Utilizzare il comando describe-images .

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query Images[].ImageAllowed \
    --output text
```

Di seguito è riportato un output di esempio.

```
True
```

Per trovare le AMI che soddisfano i criteri delle AMI consentite

Utilizzare il comando describe-images .

```
aws ec2 describe-images \
    --filters "Name=image-allowed,Values=true" \
    --max-items 10 \
    --query Images[].ImageId
```

Di seguito è riportato un output di esempio.

```
ami-000eaaa8be2fd162a
ami-000f82db25e50de8e
ami-000fc21eb34c7a9a6
ami-0010b876f1287d7be
ami-0010b929226fe8eba
ami-0010957836340aead
ami-00112c992a47ba871
ami-00111759e194abcc1
ami-001112565ffcafa5e
ami-0011e45aaee9fba88
```

PowerShell

Per controllare se un'AMI soddisfa i criteri delle AMI consentite

Utilizza il cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).ImageAllowed
```

Di seguito è riportato un output di esempio.

```
True
```

Per trovare le AMI che soddisfano i criteri delle AMI consentite

Utilizza il cmdlet Get-EC2Image.

```
Get-EC2Image `
    -Filter @{Name="image-allows";Values="true"} `
    -MaxResult 10 | `
    Select ImageId
```

Di seguito è riportato un output di esempio.

```
ami-000eaaa8be2fd162a
ami-000f82db25e50de8e
ami-000fc21eb34c7a9a6
ami-0010b876f1287d7be
ami-0010b929226fe8eba
ami-0010957836340aead
ami-00112c992a47ba871
ami-00111759e194abcc1
ami-001112565ffcafa5e
ami-0011e45aaee9fba88
```

Trova le istanze avviate da AMI che non sono consentite

Puoi identificare le istanze avviate utilizzando un'AMI che non soddisfa i criteri delle AMI consentite.

Console

Per verificare se un'istanza è stata avviata utilizzando un'AMI non consentita

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Nella scheda Dettagli, sotto Dettagli istanza, trova Immagine consentita.
   - Sì: l'AMI soddisfa i criteri per le AMI consentite.
   - No: l'AMI non soddisfa i criteri per le AMI consentite.

AWS CLI

Per trovare le istanze avviate utilizzando AMI non consentite

Utilizza il comando describe-instance-image-metadata con il filtro `image-allowed`.

```
aws ec2 describe-instance-image-metadata \
    --filters "Name=image-allowed,Values=false" \
    --query "InstanceImageMetadata[*].[InstanceId,ImageMetadata.ImageId]" \
    --output table
```

Di seguito è riportato un output di esempio.

```
-----------------------------------------------------
|          DescribeInstanceImageMetadata           |
+----------------------+--------------------------+
|  i-08fd74f3f1595fdbd |  ami-09245d5773578a1d6   |
|  i-0b1bf24fd4f297ab9 |  ami-07cccf2bd80ed467f   |
|  i-026a2eb590b4f7234 |  ami-0c0ec0a3a3a4c34c0   |
|  i-006a6a4e8870c828f |  ami-0a70b9d193ae8a799   |
|  i-0781e91cfeca3179d |  ami-00c257e12d6828491   |
|  i-02b631e2a6ae7c2d9 |  ami-0bfddf4206f1fa7b9   |
+----------------------+--------------------------+
```

PowerShell

Per trovare le istanze avviate utilizzando AMI non consentite

Utilizza il cmdlet Get-EC2InstanceImageMetadata.

```
Get-EC2InstanceImageMetadata `
    -Filter @{Name="image-allowed";Values="false"} | `
    Select InstanceId, @{Name='ImageId'; Expression={($_.ImageMetadata.ImageId)}}
```

Di seguito è riportato un output di esempio.

```
InstanceId          ImageId
----------          -------
i-08fd74f3f1595fdbd ami-09245d5773578a1d6
i-0b1bf24fd4f297ab9 ami-07cccf2bd80ed467f
i-026a2eb590b4f7234 ami-0c0ec0a3a3a4c34c0
i-006a6a4e8870c828f ami-0a70b9d193ae8a799
i-0781e91cfeca3179d ami-00c257e12d6828491
i-02b631e2a6ae7c2d9 ami-0bfddf4206f1fa7b9
```

AWS Config

Puoi aggiungere la AWS Config regola ec2-instance-launched-with-allowed-ami, configurarla in base alle tue esigenze e quindi utilizzarla per valutare le tue istanze.

Per ulteriori informazioni, consulta Adding rules e ec2-instance-launched-with-allowed-ami nella Developer Guide. AWS Config https://docs.aws.amazon.com/config/latest/developerguide/ec2-instance-launched-with-allowed-ami.html AWS Config

Rendi la tua AMI disponibile pubblicamente per l'utilizzo in Amazon EC2

Puoi rendere la tua AMI disponibile al pubblico condividendola con tutti Account AWS.

Se desideri impedire la condivisione pubblica delle tue AMI, puoi abilitare il blocco dell'accesso pubblico per le AMI. Ciò blocca qualsiasi tentativo di rendere pubblica un'AMI, contribuendo a prevenire l'accesso non autorizzato e il potenziale uso improprio dei dati dell'AMI. Tieni presente che l'abilitazione del blocco dell'accesso pubblico non influisce sulle AMI che sono già disponibili pubblicamente, che rimarranno disponibili al pubblico. Per ulteriori informazioni, consulta Capire il blocco dell'accesso pubblico per le AMI.

Per consentire a solo determinati account di utilizzare l'AMI per avviare le istanze, consulta Condividi un'AMI con uno specifico AWS account.

Indice

- Considerazioni
- Condividi un'AMI con tutti AWS account (condividi pubblicamente)

Considerazioni

Considera quanto segue prima di rendere pubblica un'AMI.

- Proprietà: per rendere pubblica un'AMI, Account AWS devi possederla.
- Regione: le AMI sono una risorsa basata sulla regione. Quando un'AMI viene condivisa, questa sarà disponibile solo nella Regione da cui viene condivisa. Per rendere un'AMI disponibile in un'altra regione, copiala nella regione desiderata e condividila. Per ulteriori informazioni, consulta Copiare un'AMI Amazon EC2.
- Blocca l'accesso pubblico: per condividere pubblicamente un'AMI, il blocco dell'accesso pubblico per le AMI deve essere disabilitato in ogni Regione in cui l'AMI verrà condivisa pubblicamente.

Dopo aver condiviso pubblicamente l'AMI, potrai riabilitare il blocco dell'accesso pubblico per le AMI e impedire un'ulteriore condivisione pubblica delle tue AMI.

- Alcune AMI non possono essere rese pubbliche: se l'AMI presenta una delle seguenti opzioni, non è possibile renderla pubblica (ma si può condividere l'AMI con Account AWS specifici):
  - Volumi crittografati
  - Snapshot di volumi crittografati
  - Codici di prodotto
- Evita di esporre dati sensibili: per evitare di esporre dati sensibili durante la condivisione di un'AMI, leggi le considerazioni di sicurezza in Consigli per creare AMI Linux condivise e segui le operazioni consigliate.
- Utilizzo: quando un'AMI viene condivisa, gli utenti possono soltanto avviare le istanze dall'AMI. Non possono eliminarle, condividerle o modificarle. Tuttavia, dopo l'avvio di un'istanza utilizzando l'AMI condivisa, potranno creare un'AMI dall'istanza di avvio.
- Obsolescenza automatica: per impostazione predefinita, la data di obsolescenza di tutte le AMI pubbliche è impostata a due anni dalla data di creazione dell'AMI. È possibile impostare la data di obsolescenza prima dei due anni. Per annullare la data di deprecazione o spostare la deprecazione a una data successiva, devi rendere privata l'AMI condividendola solo con specifici utenti. Account AWS
- Rimuovi le AMI obsolete: dopo che un'AMI pubblica raggiunge la data di deprecazione, se non vengono lanciate nuove istanze dall'AMI per sei o più mesi, AWS alla fine rimuove la proprietà di condivisione pubblica in modo che le AMI obsolete non compaiano negli elenchi delle AMI pubbliche.
- Fatturazione: non ti viene addebitato alcun costo quando l'AMI viene utilizzata da altri per avviare istanze. Account AWS Agli account che avviano le istanze tramite l'AMI saranno addebitate solo le istanze avviate.

Condividi un'AMI con tutti AWS account (condividi pubblicamente)

Una volta resa pubblica, un'AMI sarà disponibile nelle AMI della community nella console, a cui si può accedere dal catalogo AMI nel riquadro di navigazione sulla sinistra della console EC2 o quando si avvia un'istanza utilizzando la console. Tieni presente che, dopo averla resa pubblica, potrebbe essere necessario un po' di tempo prima che l'AMI venga visualizzata in Community AMIs (AMI della community).

Console

Per rendere un'AMI pubblica

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI nell'elenco e scegliere Actions (Operazioni), quindi Edit AMI permissions (Modifica autorizzazioni AMI).
4. In Disponibilità AMI, scegli Pubblica.
5. Scegli Save changes (Salva modifiche).

AWS CLI

Ogni AMI ha una `launchPermission` proprietà che controlla quali Account AWS, oltre a quella del proprietario, possono utilizzare quell'AMI per lanciare istanze. Modificando la `launchPermission` proprietà di un'AMI, puoi renderla pubblica (il che concede a tutti i permessi di lancio Account AWS) o condividerla solo con le Account AWS persone specificate.

Puoi aggiungere o rimuovere gli ID account dall'elenco degli account che dispongono dei permessi di avvio per l'AMI. Per rendere un'AMI pubblica, specifica il gruppo `all`. Puoi specificare i permessi di avvio sia espliciti che pubblici.

Per rendere un'AMI pubblica

1. Utilizza il comando modify-image-attribute come riportato di seguito per aggiungere il gruppo `all` all'elenco `launchPermission` dell'AMI specificata.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{Group=all}]"
```

2. Per verificare le autorizzazioni di avvio dell'AMI, utilizza il comando describe-image-attribute.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

3. (Facoltativo) Per rendere nuovamente privata l'AMI, rimuovere il gruppo `all` dai relativi permessi di avvio. Tenere presente che il proprietario dell'AMI dispone sempre dei permessi di avvio e, di conseguenza, non è interessato da questo comando.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{Group=all}]"
```

PowerShell

Ogni AMI ha una `launchPermission` proprietà che controlla che Account AWS, oltre a quella del proprietario, può utilizzare quell'AMI per avviare istanze. Modificando la `launchPermission` proprietà di un'AMI, puoi renderla pubblica (il che concede a tutti i permessi di lancio Account AWS) o condividerla solo con le Account AWS persone specificate.

Puoi aggiungere o rimuovere gli ID account dall'elenco degli account che dispongono dei permessi di avvio per l'AMI. Per rendere un'AMI pubblica, specifica il gruppo `all`. Puoi specificare i permessi di avvio sia espliciti che pubblici.

Per rendere un'AMI pubblica

1. Utilizza il comando Edit-EC2ImageAttribute come riportato di seguito per aggiungere il gruppo `all` all'elenco `launchPermission` dell'AMI specificata.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType add `
    -UserGroup all
```

2. Per verificare le autorizzazioni di avvio dell'AMI, utilizza il seguente comando Get-EC2ImageAttribute.

```
Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

3. (Facoltativo) Per rendere nuovamente privata l'AMI, rimuovere il gruppo `all` dai relativi permessi di avvio. Tenere presente che il proprietario dell'AMI dispone sempre dei permessi di avvio e, di conseguenza, non è interessato da questo comando.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType remove `
    -UserGroup all
```

Capire il blocco dell'accesso pubblico per le AMI

Per impedire la condivisione pubblica delle AMI, puoi abilitare il blocco dell'accesso pubblico per le AMI a livello di account.

Quando il blocco dell'accesso pubblico è abilitato, qualsiasi tentativo di rendere pubblica un'AMI viene automaticamente bloccato. Tuttavia, se si dispone già di AMI pubbliche, rimangono disponibili al pubblico.

Per condividere pubblicamente le AMI, devi disabilitare il blocco dell'accesso pubblico. Al termine della condivisione, è preferibile riabilitare il blocco dell'accesso pubblico per impedire la condivisione pubblica involontaria delle AMI.

> **Note**
>
> Questa impostazione è configurata a livello di account, direttamente nell'account o utilizzando una policy dichiarativa. Deve essere configurato in tutti i punti in Regione AWS cui desideri impedire la condivisione pubblica delle tue AMI. L'utilizzo di una policy dichiarativa consente di applicare l'impostazione contemporaneamente su più regioni, nonché su più account. Quando viene utilizzata una policy dichiarativa, non è possibile modificare l'impostazione direttamente all'interno di un account. Questo argomento illustra la modalità di configurazione dell'impostazione direttamente all'interno di un account. Per informazioni sull'utilizzo delle policy dichiarative, consulta Policy dichiarative nella Guida per l'utente di AWS Organizations .

È possibile limitare le autorizzazioni IAM a un utente amministratore in modo che solo lui possa abilitare o disabilitare il blocco dell'accesso pubblico per le AMI.

Argomenti

- Impostazioni predefinite

- Gestisci l'impostazione di blocco dell'accesso pubblico per le AMI

Impostazioni predefinite

L'impostazione Blocca l'accesso pubblico per le AMI è abilitata o disabilitata per impostazione predefinita a seconda che l'account sia nuovo o esistente e che disponga di AMI pubbliche. Nella tabella seguente vengono elencate le impostazioni predefinite:

AWS account	Blocco dell'accesso pubblico per le AMI per l'impostazione predefinita
Nuovi account	Abilitato
Account esistenti senza AMI pubbliche [1]	Abilitato
Account esistenti con una o più AMI pubbliche	Disabilitato

[1] Se il tuo account aveva una o più AMI pubbliche a partire dal 15 luglio 2023, l'opzione Blocca l'accesso pubblico alle AMI è disabilitata per impostazione predefinita per il tuo account, anche se successivamente hai reso private tutte le AMI.

Gestisci l'impostazione di blocco dell'accesso pubblico per le AMI

Puoi gestire l'impostazione di blocco dell'accesso pubblico per le tue AMI per controllare se possono essere condivise pubblicamente. Puoi abilitare, disabilitare o visualizzare lo stato attuale di blocco dell'accesso pubblico per le tue AMI utilizzando la console Amazon EC2 o AWS CLI.

Visualizzazione dello stato di blocco dell'accesso pubblico per le AMI

Per vedere se la condivisione pubblica delle tue AMI è bloccata nel tuo account, puoi visualizzare lo stato per bloccare l'accesso pubblico alle AMI. È necessario visualizzare lo stato in ogni Regione AWS in cui desideri verificare se la condivisione pubblica delle AMI è bloccata.

Autorizzazioni richieste

Per ottenere l'attuale impostazione di blocco dell'accesso pubblico per le AMI, devi avere l'autorizzazione IAM `GetImageBlockPublicAccessState`.

Console

Visualizzazione dello stato del blocco dell'accesso pubblico per le AMI nella Regione specificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, nella parte superiore della schermata, seleziona la Regione in cui visualizzare lo stato del blocco dell'accesso pubblico per le AMI.
3. Nel pannello di navigazione seleziona Pannello di controllo.
4. Nella scheda Attributi dell'account, in Impostazioni, scegli Protezione e sicurezza dei dati.
5. In Blocca l'accesso pubblico per le AMI, seleziona il campo Accesso pubblico. Il valore è Nuova condivisione pubblica bloccata o Nuova condivisione pubblica consentita.

AWS CLI

Per ottenere lo stato di blocco dell'accesso pubblico per le AMI

Utilizza il comando get-image-block-public-access-state. Il valore è `block-new-sharing` o `unblocked`.

Esempio: per una regione specifica

```
aws ec2 get-image-block-public-access-state --region us-east-1
```

Il campo `ManagedBy` indica l'entità che ha configurato l'impostazione. In questo esempio, `account` indica che l'impostazione è stata configurata direttamente nell'account. Il valore di `declarative-policy` indicherebbe che l'impostazione è stata configurata mediante una policy dichiarativa. Per ulteriori informazioni, consulta Policy dichiarative nella Guida per l'utente di AWS Organizations .

```
{
    "ImageBlockPublicAccessState": "block-new-sharing",
    "ManagedBy": "account"
}
```

Esempio: per tutte le regioni del tuo account

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
```

```
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-image-block-public-access-state \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Di seguito è riportato un output di esempio.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       unblocked
eu-west-3        block-new-sharing
...
```

PowerShell

Per ottenere lo stato di blocco dell'accesso pubblico per le AMI

Utilizza il cmdlet Get-EC2ImageBlockPublicAccessState. Il valore è `block-new-sharing` o `unblocked`.

Esempio: per una regione specifica

```
Get-EC2ImageBlockPublicAccessState -Region us-east-1
```

Di seguito è riportato un output di esempio.

```
block-new-sharing
```

Esempio: per tutte le regioni del tuo account

```
(Get-EC2Region).RegionName | `
```

```
    ForEach-Object {
        [PSCustomObject]@{
            Region   = $_
            PublicAccessState = (Get-EC2ImageBlockPublicAccessState -Region $_)
        }
} | `
Format-Table -AutoSize
```

Di seguito è riportato un output di esempio.

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
...
```

Abilitazione del blocco dell'accesso pubblico per le AMI

Per impedire la condivisione pubblica delle AMI, abilita il blocco dell'accesso pubblico per le AMI a livello di account. È necessario abilitare il blocco dell'accesso pubblico per le AMI in ogni Regione AWS in cui si desidera impedire la condivisione pubblica delle AMI. Se si dispone già di AMI pubbliche, rimarranno disponibili al pubblico.

Autorizzazioni richieste

Per abilitare l'impostazione di blocco dell'accesso pubblico per le AMI, devi avere l'autorizzazione IAM `EnableImageBlockPublicAccess`.

Considerazioni

- La configurazione di questa impostazione può richiedere fino a 10 minuti. Durante questo periodo, se descrivi lo stato di accesso pubblico, la risposta è `unblocked`. Quando la configurazione sarà completata, la risposta sarà `block-new-sharing`.

Console

Come abilitare il blocco dell'accesso pubblico per le AMI nella Regione specificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nella barra di navigazione, nella parte superiore della schermata, seleziona la regione in cui abilitare il blocco dell'accesso pubblico per le AMI.
3. Nel pannello di navigazione seleziona Pannello di controllo.
4. Nella scheda Attributi dell'account, in Impostazioni, scegli Protezione e sicurezza dei dati.
5. In Blocca l'accesso pubblico per le AMI, scegli Gestisci.
6. Seleziona la casella di spunta Blocca nuova condivisione pubblica quindi scegli Aggiorna.

AWS CLI

Per abilitare il blocco dell'accesso pubblico per le AMI

Utilizza il comando enable-image-block-public-access.

Esempio: per una regione specifica

```
aws ec2 enable-image-block-public-access \
--region us-east-1 \
--image-block-public-access-state block-new-sharing
```

Di seguito è riportato un output di esempio.

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

Esempio: per tutte le regioni del tuo account

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 enable-image-block-public-access \
            --region $region \
            --image-block-public-access-state block-new-sharing \
```

```
            --output text)
        echo -e "$region \t $output"
    );
done
```

Di seguito è riportato un output di esempio.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       block-new-sharing
eu-west-3        block-new-sharing
...
```

PowerShell

Per abilitare il blocco dell'accesso pubblico per le AMI

Utilizza il comando Enable-EC2ImageBlockPublicAccess.

Esempio: per una regione specifica

```
Enable-EC2ImageBlockPublicAccess `
    -Region us-east-1 `
    -ImageBlockPublicAccessState block-new-sharing
```

Di seguito è riportato un output di esempio.

```
Value
-----
block-new-sharing
```

Esempio: per tutte le regioni del tuo account

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (
        Enable-EC2ImageBlockPublicAccess `
         -Region $_ `
```

```
          -ImageBlockPublicAccessState block-new-sharing)
    }
} | `
Format-Table -AutoSize
```

Di seguito è riportato un output di esempio.

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
...
```

Disabilitazione del blocco dell'accesso pubblico per le AMI

Per consentire agli utenti del tuo account di condividere pubblicamente le tue AMI, disabilita il blocco dell'accesso pubblico a livello di account. È necessario disattivare il blocco dell'accesso pubblico per le AMI Regione AWS in ciascuna area in cui si desidera consentire la condivisione pubblica delle AMI.

Autorizzazioni richieste

Per disabilitare l'impostazione di blocco dell'accesso pubblico per le AMI, devi avere l'autorizzazione IAM `DisableImageBlockPublicAccess`.

Considerazioni

- La configurazione di questa impostazione può richiedere fino a 10 minuti. Durante questo periodo, se descrivi lo stato di accesso pubblico, la risposta è `block-new-sharing`. Quando la configurazione sarà completata, la risposta sarà `unblocked`.

Console

Come disabilitare il blocco dell'accesso pubblico per le AMI nella Regione specificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, nella parte superiore della schermata, seleziona la Regione in cui abilitare il blocco dell'accesso pubblico per le AMI.

3. Nel pannello di navigazione seleziona Pannello di controllo.
4. Nella scheda Attributi dell'account, in Impostazioni, scegli Protezione e sicurezza dei dati.
5. In Blocca l'accesso pubblico per le AMI, scegli Gestisci.
6. Deseleziona la casella di spunta Blocca nuova condivisione pubblica quindi scegli Aggiorna.
7. Quando viene richiesta la conferma, inserisci **`confirm`** e seleziona Consenti condivisione pubblica.

AWS CLI

Per disabilitare il blocco dell'accesso pubblico per le AMI

Utilizza il comando disable-image-block-public-access.

Esempio: per una regione specifica

```
aws ec2 disable-image-block-public-access --region us-east-1
```

Di seguito è riportato un output di esempio.

```
{
   "ImageBlockPublicAccessState": "unblocked"
}
```

Esempio: per tutte le regioni del tuo account

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 disable-image-block-public-access \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
```

```
done
```

Di seguito è riportato un output di esempio.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
...
```

PowerShell

Per disabilitare il blocco dell'accesso pubblico per le AMI

Utilizza il cmdlet Disable-EC2ImageBlockPublicAccess.

Esempio: per una regione specifica

```
Disable-EC2ImageBlockPublicAccess -Region us-east-1
```

Di seguito è riportato un output di esempio.

```
Value
-----
unblocked
```

Esempio: per tutte le regioni del tuo account

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (Disable-EC2ImageBlockPublicAccess -Region $_)
    }
} | `
Format-Table -AutoSize
```

Di seguito è riportato un output di esempio.

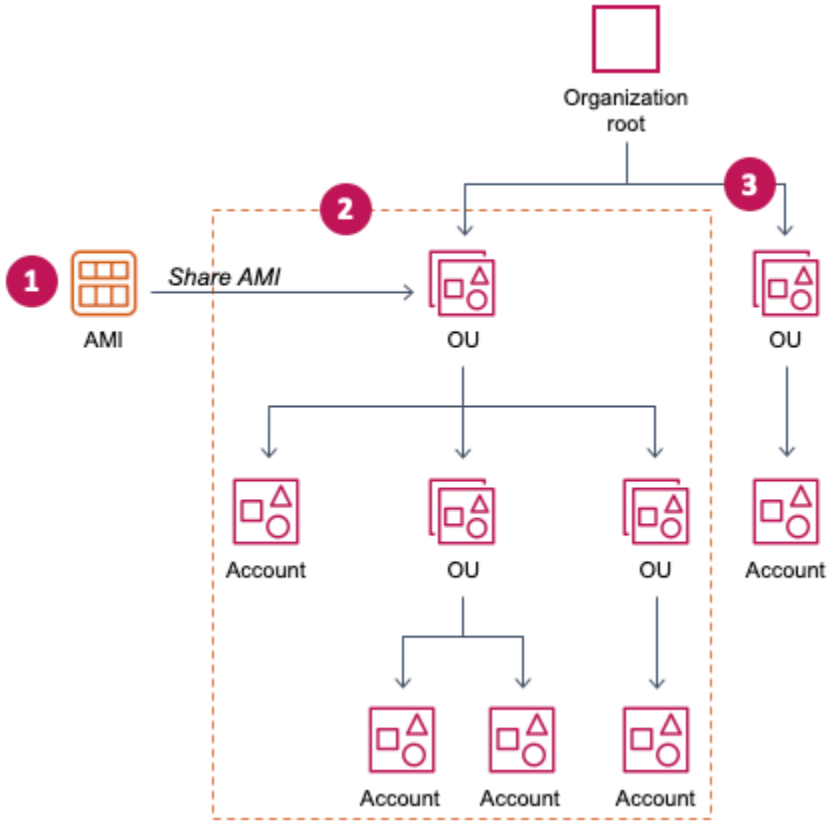
```
Region         PublicAccessState
------         -----------------
ap-south-1     unblocked
eu-north-1     unblocked
eu-west-3      unblocked
...
```

Condivisione di un'AMI con organizzazioni e unità organizzative

AWS Organizationsè un servizio di gestione degli account che consente di consolidare più account Account AWS in un'organizzazione creata e gestita centralmente. È possibile condividere un'AMI con un'organizzazione o un'unità organizzativa (UO) creata, oltre a condividerla con account specifici.

Un'organizzazione è un'entità che viene creata per consolidare e gestire centralmente i propri Account AWS. È possibile organizzare gli account in una struttura gerarchica strutturata ad albero con una radice nella parte superiore e unità organizzative sotto la radice dell'organizzazione. Ogni account può essere aggiunto direttamente alla radice o essere inserito in una delle UO nella gerarchia. Per ulteriori informazioni, consulta Concetti e terminologia di AWS nella Guida per l'utente di AWS Organizations .

Quando un'AMI viene condivisa con un'organizzazione o un'unità organizzativa, tutti gli account figlio hanno accesso all'AMI. Ad esempio, nel diagramma seguente, l'AMI viene condivisa con un'unità organizzativa di primo livello (indicata dalla freccia sul numero 1). Anche tutte le unità organizzative e gli account nidificati sotto l'unità organizzativa di primo livello (indicata dalla linea tratteggiata sul numero 2) avranno accesso all'AMI. Gli account dell'organizzazione e dell'unità organizzativa al di fuori della linea tratteggiata (indicati dal numero 3) non avranno accesso all'AMI perché non sono figli dell'UO con cui l'AMI è condivisa.



Argomenti

- Considerazioni
- Ottenere l'ARN di un'organizzazione o un'unità organizzativa
- Consentire a organizzazioni e unità organizzative di utilizzare una chiave KMS
- Gestire la condivisione di un'AMI con un'organizzazione o un'unità organizzativa

Considerazioni

Considera le informazioni seguenti durante la condivisione delle AMI con organizzazioni o unità organizzative specifiche.

- Proprietà: per condividere un'AMI, il tuo Account AWS deve essere proprietario dell'AMI.
- Limiti di condivisione: il proprietario dell'AMI può condividere un'AMI con qualsiasi organizzazione o unità organizzativa, incluse le organizzazioni e le unità organizzative di cui non è membro.

  Per il numero massimo di entità con cui un'AMI può essere condivisa all'interno di una regione, consulta le quote di servizio di Amazon EC2.

- Tag: non puoi condividere tag definiti dall'utente (tag che colleghi a un'AMI). Quando condividi un'AMI, i tag definiti dall'utente non sono disponibili per nessuna organizzazione o Account AWS unità organizzativa con cui l'AMI è condivisa.
- Formato ARN: quando si specifica un'organizzazione o un'unità organizzativa in un comando, assicurarsi di utilizzare il formato ARN corretto. Se si specifica solo l'ID, ad esempio se si specifica solo `o-123example` o `ou-1234-5example`, viene restituito un errore.

  Formati ARN corretti:

  - ARN dell'organizzazione: `arn:aws:organizations::111122223333:organization/organization-id`
  - ARN dell'unità organizzativa: `arn:aws:organizations::111122223333:ou/organization-id/ou-id`

  Dove:

  - *111122223333* è un esempio di ID account a 12 cifre per l'account di gestione. Se non si conosce il numero dell'account di gestione, è possibile descrivere l'organizzazione o l'unità organizzativa in modo da ottenere l'ARN, che include il numero dell'account di gestione. Per ulteriori informazioni, consulta Ottenere l'ARN di un'organizzazione o un'unità organizzativa.
  - *organization-id* è l'ID dell'organizzazione, ad esempio, `o-123example`.
  - *ou-id* è l'ID dell'unità organizzativa, ad esempio, `ou-1234-5example`.

  Per maggiori informazioni sul formato degli ARN, consulta Nomi della risorsa Amazon (ARN) nella Guida per l'utente IAM.
- Crittografia e chiavi: puoi condividere le AMI supportate da snapshot non crittografati e crittografati.
  - Gli snapshot crittografati devono essere crittografati con una chiave gestita dal cliente. Non puoi condividere le AMI supportate da istantanee crittografate con la chiave gestita predefinita AWS .
  - Se condividi un'AMI supportata da snapshot crittografati, è necessario consentire alle organizzazioni o alle unità organizzative di utilizzare le chiavi gestite dal cliente utilizzate per crittografare gli snapshot. Per ulteriori informazioni, consulta Consentire a organizzazioni e unità organizzative di utilizzare una chiave KMS.
- Regione: le AMI sono una risorsa basata sulla regione. Quando un'AMI viene condivisa, questa sarà disponibile solo nella Regione da cui viene condivisa. Per rendere un'AMI disponibile in un'altra regione, copiala nella regione desiderata e condividila. Per ulteriori informazioni, consulta Copiare un'AMI Amazon EC2.

- Utilizzo: quando un'AMI viene condivisa, gli utenti possono soltanto avviare le istanze dall'AMI. Non possono eliminarle, condividerle o modificarle. Tuttavia, dopo l'avvio di un'istanza utilizzando l'AMI condivisa, potranno creare un'AMI dall'istanza di avvio.
- Fatturazione: non ti viene addebitato alcun costo quando la tua AMI viene utilizzata da altri Account AWS per avviare istanze. Agli account che avviano le istanze tramite l'AMI saranno addebitate solo le istanze avviate.

Ottenere l'ARN di un'organizzazione o un'unità organizzativa

Gli ARN delle organizzazioni e delle unità organizzative contengono il numero di account di gestione a 12 cifre. Se non si conosce il numero dell'account di gestione, è possibile descrivere l'organizzazione e l'unità organizzativa in modo da ottenere l'ARN. Negli esempi seguenti, `123456789012` è l'ID dell'account di gestione.

Autorizzazioni richieste

Prima di poter ottenere gli ARN, occorre possedere l'autorizzazione per descrivere le organizzazioni e le unità organizzative. La seguente policy fornisce l'autorizzazione necessaria.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS CLI

Come ottenere l'ARN di un'organizzazione

Utilizza il comando describe-organization. Aggiungi l'opzione `--query` per restituire solo l'ARN dell'organizzazione.

```
aws organizations describe-organization --query 'Organization.Arn'
```

Di seguito è riportato un output di esempio.

```
"arn:aws:organizations::123456789012:organization/o-1234567abc"
```

Come ottenere l'ARN di una unità organizzativa

Utilizza il comando describe-organizational-unit. Utilizza il parametro `--query` per restituire solo l'ARN dell'unità organizzativa.

```
aws organizations describe-organizational-unit \
    --organizational-unit-id ou-a123-b4567890 \
    --query 'OrganizationalUnit.Arn'
```

Di seguito è riportato un output di esempio.

```
"arn:aws:organizations::123456789012:ou/o-1234567abc/ou-a123-b4567890"
```

PowerShell

Come ottenere l'ARN di un'organizzazione

Utilizza il cmdlet Get-ORGOrganization.

```
(Get-ORGOrganization).Arn
```

Di seguito è riportato un output di esempio.

```
arn:aws:organizations::123456789012:organization/o-1234567abc
```

Come ottenere l'ARN di una unità organizzativa

Utilizza il cmdlet Get-ORGOrganizationalUnit.

```
(Get-ORGOrganizationalUnit -OrganizationalUnitId "ou-a123-b4567890").Arn
```

Di seguito è riportato un output di esempio.

```
arn:aws:organizations::123456789012:ou/o-1234567abc/ou-a123-b4567890
```

Consentire a organizzazioni e unità organizzative di utilizzare una chiave KMS

Se condividi un'AMI supportata da snapshot crittografati, devi anche consentire alle organizzazioni o alle unità organizzative (OU) di utilizzare le chiavi KMS utilizzate per crittografare gli snapshot.

> **Note**
>
> Gli snapshot crittografati devono essere crittografati con una chiave gestita dal cliente. Non puoi condividere le AMI supportate da istantanee crittografate con la chiave gestita predefinita AWS .

Per controllare l'accesso alla chiave KMS, nella policy della chiave puoi utilizzare le chiavi di condizione `aws:PrincipalOrgID` e `aws:PrincipalOrgPaths` per consentire solo l'autorizzazione dei principali specifici alle azioni specificate. Un principale può essere un utente, un ruolo IAM, un utente federato o Account AWS un utente root.

Le chiavi di condizione vengono utilizzate nel modo seguente:

- `aws:PrincipalOrgID` – Consente qualsiasi principale appartenente all'organizzazione rappresentato dall'ID specificato.
- `aws:PrincipalOrgPaths` – Consente qualsiasi principale appartenente alle OU rappresentato dai percorsi specificati.

Per concedere a un'organizzazione (includendo le OU e gli account che le appartengono) l'autorizzazione a utilizzare una chiave KMS, aggiungi la seguente istruzione alla policy della chiave.

```
{
    "Sid": "Allow access for organization root",
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
        "kms:Describe*",
        "kms:List*",
        "kms:Get*",
        "kms:Encrypt",
```

```
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "o-123example"
        }
    }
}
```

Per concedere a unità organizzative specifiche (e agli account di loro appartenenza) l'autorizzazione a utilizzare una chiave KMS, puoi utilizzare una policy simile a quella riportata nell'esempio seguente.

```
{
        "Sid": "Allow access for specific OUs and their descendants",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "kms:Describe*",
            "kms:List*",
            "kms:Get*",
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*",
            "kms:CreateGrant"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "o-123example"
            },
            "ForAnyValue:StringLike": {
                "aws:PrincipalOrgPaths": [
                    "o-123example/r-ab12/ou-ab12-33333333/*",
                    "o-123example/r-ab12/ou-ab12-22222222/*"
                ]
            }
        }
}
```

Per altri esempi di istruzioni delle condizioni, consulta aws:PrincipalOrgID e aws:PrincipalOrgPaths nella Guida per l'utente di IAM.

Per informazioni sull'accesso multi-account, consulta Autorizzazione per gli utenti in altri account a utilizzare una chiave KMS nella Guida per gli sviluppatori di AWS Key Management Service .

Gestire la condivisione di un'AMI con un'organizzazione o un'unità organizzativa

Puoi gestire la condivisione di un'AMI con organizzazioni o unità organizzative (OU) per controllare se possono avviare istanze Amazon EC2.

Visualizzazione delle organizzazioni e delle unità organizzative con cui è condivisa un'AMI

Puoi trovare le organizzazioni e le unità organizzative con cui è stata condivisa l'AMI.

Console

Per verificare con quali organizzazioni e unità organizzative è stata condivisa l'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona la tua AMI nell'elenco, scegli la scheda Autorizzazioni e scorri verso il basso fino a Condivisa. organizations/OUs

   Per cercare le AMI che altri hanno condiviso con te, consulta Trova AMI condivise da usare per le istanze Amazon EC2.

AWS CLI

Per verificare con quali organizzazioni e unità organizzative è stata condivisa l'AMI

Utilizza il comando describe-image-attribute con l'attributo `launchPermission`.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

Di seguito è riportata una risposta di esempio.

```
{
    "ImageId": "ami-0abcdef1234567890",
```

```
    "LaunchPermissions": [
        {
            "OrganizationalUnitArn": "arn:aws:organizations::111122223333:ou/
o-123example/ou-1234-5example"
        }
    ]
}
```

PowerShell

Per verificare con quali organizzazioni e unità organizzative è stata condivisa l'AMI

Utilizza il cmdlet Get-EC2ImageAttribute.

```
Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

Condividere un'AMI con un'organizzazione o una unità organizzativa

Puoi condividere un'AMI con un'organizzazione o un'unità organizzativa.

> **Note**
>
> Non è necessario condividere gli snapshot di Amazon EBS a cui fa riferimento un'AMI per condividere l'AMI. Occorre condividere soltanto l'AMI; il sistema fornisce automaticamente all'istanza l'accesso agli snapshot EBS a cui viene fatto riferimento per l'avvio. Tuttavia, è necessario condividere le chiavi KMS utilizzate per crittografare snapshot a cui l'AMI fa riferimento. Per ulteriori informazioni, consulta Consentire a organizzazioni e unità organizzative di utilizzare una chiave KMS.

Console

Come condividere un'AMI con un'organizzazione o una unità organizzativa

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI nell'elenco e scegli Actions (Operazioni), quindi Edit AMI permissions (Modifica autorizzazioni AMI).

4. In AMI availability (Disponibilità AMI), scegliere Private (Privato).
5. Accanto a Condiviso organizations/OUs, scegli Aggiungi organization/OU ARN.
6. Per Organization/OU ARN, inserisci l'ARN o l'OU ARN dell'organizzazione con cui desideri condividere l'AMI, quindi scegli Condividi AMI. È necessario specificare l'ARN completo, non solo l'ID.

   Per condividere questa AMI con più utenti, ripetere questa fase fino a quando non sono stati aggiungere tutte le organizzazioni o unità organizzative (OU) desiderate.
7. Al termine, scegli Save changes (Salva modifiche).
8. (Facoltativo) Per visualizzare le organizzazioni o le unità organizzative con cui hai condiviso l'AMI, seleziona l'AMI nell'elenco, scegli la scheda Autorizzazioni e scorri verso il basso fino a Condiviso. organizations/OUs Per cercare le AMI che altri hanno condiviso con te, consulta Trova AMI condivise da usare per le istanze Amazon EC2.

AWS CLI

Per condividere un'AMI con un'organizzazione

Utilizza il comando modify-image-attribute per concedere all'organizzazione specificata le autorizzazioni di avvio per l'AMI selezionata.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Per condividere un'AMI con una unità organizzativa

Il comando modify-image-attribute concede all'unità organizzativa specificata le autorizzazioni di avvio per l'AMI specificata. È necessario specificare l'ARN completo, non solo l'ID.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationalUnitArn=arn:aws:organizations::123456789012:ou/o-123example/
ou-1234-5example}]"
```

PowerShell

Usa il Edit-EC2ImageAttribute comando (Strumenti per Windows PowerShell) per condividere un'AMI come mostrato negli esempi seguenti.

Come condividere un'AMI con un'organizzazione o una unità organizzativa

Il comando seguente concede all'organizzazione specificata le autorizzazioni di avvio per l'AMI selezionata.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType add `
    -OrganizationArn "arn:aws:organizations::123456789012:organization/o-123example"
```

Come interrompere la condivisione di un'AMI con un'organizzazione o una unità organizzativa

Il comando seguente rimuove le autorizzazioni di avvio per l'AMI specificata dall'organizzazione specificata:

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType remove `
    -OrganizationArn "arn:aws:organizations::123456789012:organization/o-123example"
```

Per interrompere la condivisione di un'AMI con tutte le organizzazioni, le unità organizzative e Account AWS

Il comando seguente consente di rimuovere dall'AMI specificata tutte le autorizzazioni di avvio esplicite e pubbliche. Considera che il proprietario dell'AMI dispone sempre delle autorizzazioni di avvio e, di conseguenza, questo comando non ha alcun effetto su di lui.

```
Reset-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

Interrompere la condivisione di un'AMI con un'organizzazione o una unità organizzativa

Puoi interrompere la condivisione di un'AMI con un'organizzazione o una unità organizzativa.

> **Note**
>
> Non è possibile interrompere la condivisione di un'AMI con un account specifico se si trova in un'organizzazione o in una unità organizzativa con cui è condivisa un'AMI. Se si prova a interrompere la condivisione dell'AMI rimuovendo le autorizzazioni di avvio per l'account, Amazon EC2 restituirà un messaggio di riuscita dell'operazione. Tuttavia, l'AMI continuerà a essere condivisa con l'account.

Console

Come interrompere la condivisione di un'AMI con un'organizzazione o una unità organizzativa

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI nell'elenco e scegli Actions (Operazioni), quindi Edit AMI permissions (Modifica autorizzazioni AMI).
4. In Condiviso organizations/OUs, seleziona le organizzazioni o le OU con cui desideri interrompere la condivisione dell'AMI, quindi scegli Rimuovi selezionati.
5. Al termine, scegli Save changes (Salva modifiche).
6. (Facoltativo) Per confermare di aver interrotto la condivisione dell'AMI con le organizzazioni o le OU, seleziona l'AMI nell'elenco, scegli la scheda Autorizzazioni e scorri verso il basso fino a Condivisa organizations/OUs.

AWS CLI

Come interrompere la condivisione di un'AMI con un'organizzazione o una unità organizzativa

Utilizza il comando modify-image-attribute. Questo esempio rimuove le autorizzazioni di avvio per l'AMI specificata dall'organizzazione specificata.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Remove=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Per interrompere la condivisione di un'AMI con tutte le organizzazioni, le OU e Account AWS

Utilizza il comando reset-image-attribute. Questo esempio rimuove tutte le autorizzazioni di avvio pubbliche ed esplicite dall'AMI specificata. Considera che il proprietario dell'AMI dispone sempre delle autorizzazioni di avvio e, di conseguenza, questo comando non ha alcun effetto su di lui.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

PowerShell

Come interrompere la condivisione di un'AMI con un'organizzazione o una unità organizzativa

Utilizza il cmdlet Edit-EC2ImageAttribute. Questo esempio rimuove le autorizzazioni di avvio per l'AMI specificata dall'organizzazione specificata.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType remove `
    -OrganizationArn "arn:aws:organizations::123456789012:organization/o-123example"
```

Per interrompere la condivisione di un'AMI con tutte le organizzazioni, le OU e Account AWS

Utilizza il cmdlet Reset-EC2ImageAttribute. Questo esempio rimuove tutte le autorizzazioni di avvio pubbliche ed esplicite dall'AMI specificata. Considera che il proprietario dell'AMI dispone sempre delle autorizzazioni di avvio e, di conseguenza, questo comando non ha alcun effetto su di lui.

```
Reset-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute LaunchPermission
```

Condividi un'AMI con uno specifico AWS account

Puoi condividere un'AMI con specifiche Account AWS senza renderla pubblica. Tutto ciò di cui hai bisogno sono gli Account AWS ID.

Un Account AWS ID è un numero di 12 cifre, ad esempio`012345678901`, che identifica in modo univoco un. Account AWS Per ulteriori informazioni, consulta la sezione View Account AWS identifiers nella Guida di riferimento di Gestione dell'account AWS .

Considerazioni

Considera quanto segue quando condividi le AMI con specifici. Account AWS

- Proprietà: per condividere un'AMI, il tuo Account AWS deve essere proprietario dell'AMI.
- Limiti di condivisione: per il numero massimo di entità con cui un'AMI può essere condivisa all'interno di una regione, consulta le quote di servizio di Amazon EC2.
- Tag: non puoi condividere tag definiti dall'utente (tag che colleghi a un'AMI). Quando condividi un'AMI, i tag definiti dall'utente non sono disponibili per nessuno con Account AWS cui l'AMI è condivisa.
- Snapshot: per condividere l'AMI, non è necessario condividere gli snapshot Amazon EBS a cui l'AMI fa riferimento. Puoi condividere solo l'AMI stessa; il sistema fornisce l'accesso dell'istanza agli snapshot EBS di riferimento per l'avvio. Tuttavia, devi condividere eventuali Chiavi KMS utilizzate per crittografare gli snapshot a cui l'AMI fa riferimento. Per ulteriori informazioni, consulta Condividi uno snapshot Amazon EBS nella Guida per l'utente di Amazon EBS.
- Crittografia e chiavi: puoi condividere le AMI supportate da snapshot non crittografati e crittografati.
  - Gli snapshot crittografati devono essere crittografati con una chiave KMS. Non è possibile condividere AMI supportate da snapshot crittografati con la chiave gestita da AWS di default.
  - Se condividi un'AMI supportata da istantanee crittografate, devi consentirle di Account AWS utilizzare le chiavi KMS utilizzate per crittografare le istantanee. Per ulteriori informazioni, consulta Consentire a organizzazioni e unità organizzative di utilizzare una chiave KMS. Per impostare la policy chiave necessaria per avviare le istanze di Auto Scaling quando utilizzi una chiave gestita dal cliente per la crittografia, consulta la AWS KMS key Politica richiesta per l'uso con volumi crittografati nella Amazon EC2 Auto Scaling User Guide.
- Regione: le AMI sono una risorsa basata sulla regione. Quando un'AMI viene condivisa, questa sarà disponibile solo in quella Regione. Per rendere un'AMI disponibile in un'altra regione, copiala nella regione desiderata e condividila. Per ulteriori informazioni, consulta Copiare un'AMI Amazon EC2.
- Utilizzo: quando un'AMI viene condivisa, gli utenti possono soltanto avviare le istanze dall'AMI. Non possono eliminarle, condividerle o modificarle. Tuttavia, dopo aver avviato un'istanza utilizzando l'AMI condivisa, potranno creare un'AMI dalla loro istanza.
- Copiare AMI condivise: Se gli utenti di un altro account vogliono copiare un'AMI condivisa, è necessario concedere loro le autorizzazioni di lettura per lo archiviazione che supporta l'AMI. Per ulteriori informazioni, consulta Cross-account copiando.

- Fatturazione: non ti viene addebitato alcun costo quando la tua AMI viene utilizzata da altri per avviare istanze. Account AWS Agli account che avviano le istanze tramite l'AMI saranno addebitate solo le istanze avviate.

Console

Per concedere i permessi di avvio espliciti

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Selezionare l'AMI nell'elenco e scegli Actions (Operazioni), quindi Edit AMI permissions (Modifica autorizzazioni AMI).
4. Scegli Private (Privato).
5. In Shared accounts (Account condivisi), scegliere Add account ID (Aggiungi ID account).
6. Per Account AWS ID, inserisci l' Account AWS ID con cui desideri condividere l'AMI, quindi scegli Condividi AMI.

   Per condividere questa AMI con più account, ripetere le fasi 5 e 6 fino a quando sono stati aggiunti tutti gli account richiesti.
7. Al termine, scegli Save changes (Salva modifiche).
8. (Facoltativo) Per visualizzare gli Account AWS ID con cui hai condiviso l'AMI, seleziona l'AMI nell'elenco e scegli la scheda Autorizzazioni. Per cercare le AMI che altri hanno condiviso con te, consulta Trova AMI condivise da usare per le istanze Amazon EC2.

AWS CLI

Utilizza il comando modify-image-attribute per condividere un'AMI come illustrato negli esempi seguenti.

Per concedere i permessi di avvio espliciti

L'esempio seguente concede all' Account AWS specificato le autorizzazioni di avvio per l'AMI specificata.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{UserId=123456789012}]"
```

Per rimuovere i permessi di avvio da un account

L'esempio seguente consente di rimuovere dall' Account AWS specificato le autorizzazioni di avvio per l'AMI specificata.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{UserId=123456789012}]"
```

Per rimuovere tutte le autorizzazioni di avvio

L'esempio seguente consente di rimuovere dall'AMI specificata tutte le autorizzazioni di avvio esplicite e pubbliche. Considera che il proprietario dell'AMI dispone sempre delle autorizzazioni di avvio e, di conseguenza, questo comando non ha alcun effetto su di lui.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

PowerShell

Usa il Edit-EC2ImageAttribute comando (Strumenti per Windows PowerShell) per condividere un'AMI come mostrato negli esempi seguenti.

Per concedere i permessi di avvio espliciti

L'esempio seguente concede all' Account AWS specificato le autorizzazioni di avvio per l'AMI specificata.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType add `
    -UserId "123456789012"
```

Per rimuovere i permessi di avvio da un account

L'esempio seguente consente di rimuovere dall' Account AWS specificato le autorizzazioni di avvio per l'AMI specificata.

```
Edit-EC2ImageAttribute `
```

```
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission -OperationType remove `
    -UserId "123456789012"
```

Per rimuovere tutte le autorizzazioni di avvio

L'esempio seguente consente di rimuovere dall'AMI specificata tutte le autorizzazioni di avvio esplicite e pubbliche. Considera che il proprietario dell'AMI dispone sempre delle autorizzazioni di avvio e, di conseguenza, questo comando non ha alcun effetto su di lui.

```
Reset-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

Annulla la condivisione di un'AMI con la tua Account AWS

Un'Amazon Machine Image (AMI) può essere condivisa con Account AWS specifici aggiungendo gli account alle sue autorizzazioni di avvio. Se un'AMI è stata condivisa con il tuo Account AWS e non desideri più condividerla con il tuo account, puoi rimuovere il tuo account dai permessi di avvio dell'AMI. Puoi farlo eseguendo il `cancel-image-launch-permission` AWS CLI comando. Quando si esegue questo comando, il tuo Account AWS viene rimosso dai permessi di avvio per l'AMI specificata. Per trovare le AMI condivise con te Account AWS, consulta. Trova AMI condivise da usare per le istanze Amazon EC2

Potresti annullare la condivisione di un'AMI con il tuo account, ad esempio, per ridurre la probabilità di avviare un'istanza con un'AMI inutilizzata o obsoleta che è stata condivisa con te. Quando annulli la condivisione di un'AMI con il tuo account, questa non viene più visualizzata in nessun elenco di AMI della console EC2 o nell'output per describe-images.

Argomenti

- Limitazioni
- Annullamento della condivisione di un'AMI con il tuo account

Limitazioni

- Puoi rimuovere il tuo account dai permessi di avvio di un'AMI condivisa solo con te Account AWS . Non puoi usare `cancel-image-launch-permission` per rimuovere il tuo account dalle

autorizzazioni di avvio di un'AMI condivisa con un'organizzazione o un'unità organizzativa (UO) o per rimuovere l'accesso alle AMI pubbliche.

- Non è possibile rimuovere definitivamente il tuo account dalle autorizzazioni di avvio di un'AMI. Il proprietario di un'AMI può condividerla nuovamente con il tuo account.
- Le AMI sono una risorsa basata sulla regione. Durante l'esecuzione di `cancel-image-launch-permission`, devi specificare la regione in cui si trova l'AMI. Specifica la regione nel comando o usa la variabile di AWS_DEFAULT_REGION ambiente.
- Solo gli SDK AWS CLI e gli SDK supportano la rimozione dell'account dai permessi di avvio di un'AMI. Al momento la console EC2 non supporta questa operazione.

Annullamento della condivisione di un'AMI con il tuo account

> **Note**
>
> L'annullamento della condivisione di un'AMI con il tuo account non è un'operazione annullabile. Per ottenere nuovamente l'accesso all'AMI, il proprietario dell'AMI dovrà condividerla con il tuo account.

AWS CLI

Per annullare la condivisione di un'AMI con il tuo account

Utilizza il comando cancel-image-launch-permission.

```
aws ec2 cancel-image-launch-permission \
    --image-id ami-0abcdef1234567890 \
    --region us-east-1
```

PowerShell

Per annullare la condivisione di un'AMI con il tuo account

Utilizza il cmdlet Stop-EC2ImageLaunchPermission.

```
Stop-EC2ImageLaunchPermission `
    -ImageId ami-0abcdef1234567890 `
```

```
    -Region us-east-1
```

Consigli per creare AMI Linux condivise

Utilizza le linee guida seguenti per ridurre la superficie di attacco e migliorare l'affidabilità delle AMI create.

> **Important**
>
> Nessun elenco delle linee guida di sicurezza può essere esaustivo. Crea le tue AMI condivise con attenzione considerando in quale posizione potresti esporre dati sensibili.

Indice

- Disabilitazione degli accessi remoti basati su password per l'utente root
- Disabilitazione dell'accesso root locale
- Rimozione delle coppie di chiavi dell'host SSH
- Installazione delle credenziali di chiave pubblica
- Disabilitare i controlli DNS sshd (facoltativo)
- Rimuovere i dati sensibili

Se stai creando AMI per Marketplace AWS, consulta le migliori pratiche per la creazione di AMI nella Guida per il Marketplace AWS venditore per linee guida, politiche e best practice.

Disabilitazione degli accessi remoti basati su password per l'utente root

L'uso di una password root fissa per le AMI pubbliche rappresenta un rischio per la sicurezza che può diventare noto rapidamente. Anche fare affidamento sul fatto che gli utenti modifichino la password dopo il primo accesso lascia aperta una piccola possibilità di potenziali usi illeciti.

Per risolvere questo problema, disabilita gli accessi remoti basati su password per l'utente root.

Per disabilitare gli accessi remoti basati su password per l'utente root

1. Aprire il file `/etc/ssh/sshd_config` con un editor di testo e individuare la riga seguente:

```
#PermitRootLogin yes
```

2. Modificare la riga in:

```
PermitRootLogin without-password
```

Il percorso di questo file di configurazione potrebbe essere diverso a seconda della distribuzione o se OpenSSH non è in esecuzione. In questo caso, consultare la relativa documentazione.

Disabilitazione dell'accesso root locale

Quando utilizzi AMI condivise, ti consigliamo, come best practice, di disabilitare gli accessi root diretti. Per farlo, accedi all'istanza in esecuzione ed esegui il comando seguente:

```
[ec2-user ~]$ sudo passwd -l root
```

> **Note**
>
> Questo comando non ha alcun impatto sull'uso di `sudo`.

Rimozione delle coppie di chiavi dell'host SSH

Se intendi condividere un'AMI derivata da un'AMI pubblica, rimuovi le coppie di chiavi dell'host SSH esistenti posizionate in `/etc/ssh`. Questa azione forza SSH a generare nuove coppie di chiavi SSH univoche quando un utente avvia un'istanza tramite l'AMI, migliorando la sicurezza e riducendo la possibilità di attacchi "man-in-the-middle".

Rimuovi tutti i file di chiave seguenti presenti sul sistema.

- ssh_host_dsa_key
- ssh_host_dsa_key.pub
- ssh_host_key
- ssh_host_key.pub
- ssh_host_rsa_key
- ssh_host_rsa_key.pub
- ssh_host_ecdsa_key

- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key
- ssh_host_ed25519_key.pub

Puoi rimuovere in sicurezza tutti questi file con il comando seguente.

```
[ec2-user ~]$ sudo shred -u /etc/ssh/*_key /etc/ssh/*_key.pub
```

> **Warning**
>
> Le utilità di eliminazione sicura, come shred, potrebbero non rimuovere tutte le copie di un file dai supporti di archiviazione. I file system di journaling (tra cui il file system ext4 predefinito di Amazon Linux), snapshot, backup, RAID e la cache temporanea potrebbero creare delle copie nascoste dei file. Per ulteriori informazioni, consulta la documentazione sull'eliminazione.

> **Important**
>
> Se dimentichi di rimuovere le coppie di chiavi dell'host SSH esistenti dall'AMI pubblica, il nostro processo di controllo di routine invia una notifica a te e a tutti gli utenti che eseguono le istanze della tua AMI informandovi del potenziale rischio per la sicurezza. Dopo un breve periodo di tolleranza, contrassegneremo l'AMI come privata.

Installazione delle credenziali di chiave pubblica

Dopo aver configurato l'AMI per impedire l'accesso tramite password, devi assicurarti che gli utenti possano accedervi mediante un altro meccanismo.

Amazon EC2 consente agli utenti di specificare un nome di coppia di chiavi pubblica-privata al momento dell'avvio dell'istanza. Se viene specificato un nome della coppia di chiavi valido alla chiamata API `RunInstances` (o tramite gli strumenti API della riga di comando), la chiave pubblica (la porzione della coppia di chiavi che Amazon EC2 conserva sul server in seguito alla chiamata a `CreateKeyPair` o a `ImportKeyPair`) viene resa disponibile per l'istanza tramite una query HTTP sui metadati dell'istanza.

Per accedere tramite SSH, l'AMI deve recuperare il valore di chiave al momento dell'avvio e aggiungerlo a `/root/.ssh/authorized_keys` (o all'equivalente per gli altri account utente sull'AMI). Gli utenti possono avviare le istanze dell'AMI con una coppia di chiavi e accedere senza bisogno di una password root.

Molte distribuzioni, tra cui Amazon Linux e Ubuntu, utilizzano il pacchetto `cloud-init` per inserire le credenziali di chiave pubblica per un utente configurato. Se la distribuzione in uso non supporta `cloud-init`, puoi aggiungere il codice seguente a uno script di avvio del sistema (come `/etc/rc.local`) per inserire la chiave pubblica specificata al momento dell'avvio per l'utente root.

> **Note**
>
> Nell'esempio seguente, l'indirizzo IP http://169.254.169.254/ è un indirizzo locale del collegamento ed è valido solo dall'istanza.

IMDSv2

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

IMDSv1

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
```

```
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

Questa procedura è applicabile a tutti gli utenti e non è necessario limitarla all'utente `root`.

> **Note**
>
> Il nuovo raggruppamento di un'istanza basata su tale AMI include la chiave con la quale è stata avviata. Per impedire l'inclusione della chiave, è necessario eliminare il file `authorized_keys` o escluderlo dal nuovo raggruppamento.

Disabilitare i controlli DNS sshd (facoltativo)

La disabilitazione dei controlli DNS sshd indebolisce leggermente la sicurezza sshd. Tuttavia, in caso di errori della risoluzione DNS, gli accessi SSH continueranno a funzionare. Se non disabiliti i controlli sshd, gli errori della risoluzione DNS impediranno tutti gli accessi.

Per disabilitare i controlli DNS sshd

1. Aprire il file `/etc/ssh/sshd_config` con un editor di testo e individuare la riga seguente:

   ```
   #UseDNS yes
   ```

2. Modificare la riga in:

   ```
   UseDNS no
   ```

> **Note**
>
> Il percorso di questo file di configurazione può essere diverso a seconda della distribuzione o se OpenSSH non è in esecuzione. In questo caso, consultare la relativa documentazione.

Rimuovere i dati sensibili

Ti sconsigliamo di archiviare dati sensibili o software sulle AMI che condividi. Gli utenti che avviano un'AMI condivisa potrebbero ricompilarla e registrarla come di loro proprietà. Segui queste linee guida per evitare rischi della sicurezza spesso sottovalutati:

- Ti consigliamo di utilizzare l'opzione `--exclude` *`directory`* su `ec2-bundle-vol` per saltare le directory e le sottodirectory contenenti informazioni segrete che non desideri includere nel bundle. In particolare, escludi tutte le coppie di public/private chiavi SSH e i `authorized_keys` file SSH di proprietà dell'utente quando raggruppi l'immagine. Le AMI pubbliche di Amazon archiviano questi elementi in `/root/.ssh` per l'utente root e in `/home/`*`user_name`*`/.ssh/` per gli utente normali. Per ulteriori informazioni, consulta ec2-bundle-vol.
- Elimina sempre la cronologia della shell prima di effettuare il raggruppamento. Se tenti di effettuare più di un caricamento del bundle nella stessa AMI, la cronologia di shell (interprete di comandi) conterrà la tua chiave di accesso. L'esempio seguente riporta l'ultimo comando eseguito prima del raggruppamento effettuato dall'istanza.

  ```
  [ec2-user ~]$ shred -u ~/.*history
  ```

  > **Warning**
  >
  > Le limitazioni dell'utilità shred descritte nell'avviso riportato sopra si applicano anche in questo caso.
  > Tieni presente che bash scrive la cronologia della sessione corrente sul disco al momento dell'uscita. Se ti disconnetti dall'istanza dopo avere eliminato `~/.bash_history` e ripeti l'accesso, scoprirai che `~/.bash_history` è stato ricreato e contiene tutti i comandi eseguiti durante la sessione precedente.
  > Oltre a bash, anche altri programmi scrivono la cronologia sul disco; presta attenzione e rimuovi o escludi i file e le directory dot non necessari.

- Il raggruppamento di un'istanza in esecuzione richiede la chiave privata e il certificato X.509. Inserisci queste e altre credenziali in un percorso non incluso nel bundle (come l'instance store).

Monitora gli eventi AMI utilizzando Amazon EventBridge

Quando lo stato di un'Amazon Machine Image (AMI) cambia, Amazon EC2 genera un evento che viene inviato ad Amazon EventBridge (precedentemente noto come Amazon Events). CloudWatch

Gli eventi vengono inviati al bus di EventBridge eventi predefinito in formato JSON. Puoi usare Amazon EventBridge per rilevare e reagire a questi eventi. Puoi farlo creando regole EventBridge che attivano un'azione in risposta a un evento. Ad esempio, puoi creare una EventBridge regola che rilevi quando il processo di creazione dell'AMI è stato completato e quindi richiami un argomento Amazon SNS per inviarti una notifica via email.

Amazon EC2 genera un evento `EC2 AMI State Change` quando un'AMI entra in uno dei seguenti stati:

- `available`
- `failed`
- `deregistered`
- `disabled`

Gli eventi vengono generati in base al miglior tentativo.

La tabella seguente elenca le operazioni AMI e gli stati che un'AMI può assumere. Nella tabella, Sì indica gli stati che l'AMI può assumere quando viene eseguita l'operazione corrispondente.

Operazioni AMI	available	failed	deregistered	disabled
CopyImage	Sì	Sì		
CreateImage	Sì	Sì		
CreateRestoreImageTask	Sì	Sì		
DeregisterImage			Sì	
DisableImage				Sì
EnableImage	Sì			
RegisterImage	Sì	Sì		

Eventi EC2 AMI State Change

- Dettagli dell'evento

- disponibile eventi
- Non riuscito eventi
- annullata la registrazione eventi
- disabled eventi

Dettagli dell'evento

Puoi utilizzare i campi seguenti dell'evento per creare regole che attivano un'operazione:

`"source": "aws.ec2"`

Identifica che l'evento proviene da Amazon EC2.

`"detail-type": "EC2 AMI State Change"`

Identifica il nome dell'evento.

`"detail": { "ImageId": "ami-0abcdef1234567890", "State": "available", }`

Fornisce l'ID dell'AMI e lo stato dell'AMI (`available`, `failed`, `deregistered`, o `disabled`).

Per ulteriori informazioni, consulta quanto segue nella Amazon EventBridge User Guide:

- EventBridge Eventi Amazon
- Modelli di EventBridge eventi Amazon
- EventBridge Regole di Amazon

Per un tutorial su come creare una funzione Lambda e una EventBridge regola che esegua la funzione Lambda, consulta Tutorial: Registra lo stato di un'istanza Amazon EC2 utilizzando EventBridge nella Developer Guide. AWS Lambda

disponibile eventi

Di seguito è illustrato un esempio di un evento generato da Amazon EC2 quando l'AMI assume lo stato `available` dopo un'operazione `CreateImage`, `CopyImage`, `RegisterImage`, `CreateRestoreImageTask` o `EnableImage` riuscita.

`"State": "available"` indica che l'operazione è riuscita.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "available",
        "ErrorMessage": ""
    }
}
```

Non riuscito eventi

Di seguito è illustrato un esempio di un evento generato da Amazon EC2 quando l'AMI assume lo stato `failed` dopo un'operazione `CreateImage`, `CopyImage`, `RegisterImage` o `CreateRestoreImageTask` non riuscita.

I campi seguenti forniscono informazioni pertinenti:

- `"State": "failed"`: indica che l'operazione non è riuscita.
- `"ErrorMessage": ""`: fornisce il motivo dell'operazione non riuscita.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "failed",
```

```
        "ErrorMessage": "Description of failure"
    }
}
```

annullata la registrazione eventi

Di seguito è illustrato un esempio di un evento generato da Amazon EC2 quando l'AMI assume lo stato `deregistered` dopo un'operazione `DeregisterImage` riuscita. Se l'operazione ha esito negativo, non viene generato alcun evento. Qualsiasi errore viene comunicato immediatamente perché `DeregisterImage` è un'operazione sincrona.

`"State": "deregistered"` indica che l'operazione `DeregisterImage` è riuscita.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "deregistered",
        "ErrorMessage": ""
    }
}
```

disabled eventi

Di seguito è illustrato un esempio di un evento generato da Amazon EC2 quando l'AMI assume lo stato `disabled` dopo un'operazione `DisableImage` riuscita. Se l'operazione ha esito negativo, non viene generato alcun evento. Qualsiasi errore viene comunicato immediatamente perché `DisableImage` è un'operazione sincrona.

`"State": "disabled"` indica che l'operazione `DisableImage` è riuscita.

```
{
```

```
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "disabled",
        "ErrorMessage": ""
    }
}
```

Comprendere le informazioni di fatturazione AMI

Quando lanci le istanze, puoi scegliere tra molte Amazon Machine Image (AMI) che supportano una varietà di piattaforme del sistema operativo e funzionalità. Per capire in che modo l'AMI scelta al momento dell'avvio dell'istanza influisce sui profitti della AWS fattura, puoi ricercare la piattaforma del sistema operativo associata e le informazioni di fatturazione. Esegui questa operazione prima di avviare una On-Demand o più istanze Spot o di acquistare un'istanza riservata.

Ecco due esempi di come ricercare la tua AMI in anticipo può aiutarti a scegliere l'AMI più adatta alle tue esigenze:

- Per Istanze spot, è possibile utilizzare i Dettagli della piattaforma per confermare che l'AMI è supportata per Istanze spot.
- Al momento dell'acquisto di una Istanza riservata, è possibile assicurarsi di selezionare la piattaforma del sistema operativo (Piattaforma) mappata ai Dettagli della piattaforma AMI.

Per ulteriori informazioni sui prezzi delle istanze, consulta Prezzi di Amazon EC2.

Indice

- Campi informativi di fatturazione AMI
- Ricerca dei dettagli di fatturazione e utilizzo dell'AMI
- Verificare gli addebiti AMI in fattura

Campi informativi di fatturazione AMI

I seguenti campi forniscono informazioni di fatturazione associate a un'AMI:

Dettagli della piattaforma

I dettagli della piattaforma associati al codice di fatturazione dell'AMI. Ad esempio, `Red Hat Enterprise Linux`.

Operazione di utilizzo

L'operazione dell'istanza Amazon EC2 e il codice di fatturazione associato all'AMI. Ad esempio, `RunInstances:0010`. L'operazione di utilizzo corrisponde alla lineitem/Operation colonna del Rapporto sui AWS costi e sull'utilizzo (CUR) e nell'API del AWS listino prezzi.

Puoi visualizzare questi campi nella pagina Istanze o AMI nella console Amazon EC2 o nella risposta restituita dal comando describe-images o dal comando. Get-EC2Image

Dati di esempio: operazione di utilizzo per piattaforma

La tabella seguente elenca alcuni dei dettagli della piattaforma e dei valori delle operazioni di utilizzo che possono essere visualizzati nelle pagine Instances o AMI nella console Amazon EC2 o nella risposta restituita dal comando describe-images o dal comando. https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-images.html Get-EC2Image

Dettagli della piattaforma	Operazione di utilizzo [2]
Linux/UNIX	RunInstances
Red Hat BYOL Linux	RunInstances:00g0[3]
Red Hat Enterprise Linux	RunInstances:0010
Red Hat Enterprise Linux with HA	RunInstances:1010
Red Hat Enterprise Linux with SQL Server Standard and HA	RunInstances:1014

Dettagli della piattaforma	Operazione di utilizzo [2]
Red Hat Enterprise Linux with SQL Server Enterprise and HA	RunInstances:1110
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110
SQL Server Enterprise	RunInstances:0100
SQL Server Standard	RunInstances:0004
SQL Server Web	RunInstances:0200
SUSE Linux	RunInstances:000g
Ubuntu Pro	RunInstances:0g00
Windows	RunInstances:0002
Windows BYOL	RunInstances:0800
Windows with SQL Server Enterprise[1]	RunInstances:0102
Windows with SQL Server Standard[1]	RunInstances:0006
Windows with SQL Server Web[1]	RunInstances:0202

[1] Se due licenze software sono associate a un'AMI, il campo Platform details (Dettagli della piattaforma) mostra entrambe le licenze.

[2] Se stai utilizzando istanze Spot, il valore riportato nel rapporto lineitem/Operation su AWS costi e utilizzo potrebbe essere diverso dal valore dell'operazione di utilizzo elencato qui. Ad esempio, se `lineitem/Operation` visualizzato`RunInstances:0010:SV006`, significa che Amazon EC2 esegue Red Hat Enterprise Linux Spot Instance-hour negli Stati Uniti orientali (Virginia settentrionale) nella Zona 6.

[3] Questo viene visualizzato come RunInstances (Linux/UNIX) nei report di utilizzo.

Ricerca dei dettagli di fatturazione e utilizzo dell'AMI

Le seguenti proprietà possono aiutarti a verificare gli addebiti AMI in fattura:

- Dettagli della piattaforma
- Operazione di utilizzo
- ID ISTANZA AMI

Console

Per trovare le informazioni di fatturazione per un'AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI.
4. Nella scheda Dettagli trova i Dettagli della piattaforma e Operazione di utilizzo.

Per trovare le informazioni di fatturazione per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Nella scheda Dettagli, espandi Dettagli dell'istanza e trova Dettagli della piattaforma e Operazione di utilizzo.

AWS CLI

Per trovare le informazioni di fatturazione per un'AMI

Utilizzare il comando describe-images .

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query "Images[].
{PlatformDetails:PlatformDetails,UsageOperation:UsageOperation}"
```

Di seguito è riportato un output di esempio per un'AMI Linux.

```
[
    {
        "PlatformDetails": "Linux/UNIX",
        "UsageOperation": "RunInstances"
    }
]
```

Per trovare le informazioni di fatturazione per un'istanza

Utilizzare il comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[].Instances[].
{PlatformDetails:PlatformDetails,UsageOperation:UsageOperation}"
```

Di seguito è riportato un esempio di istanza Windows.

```
[
    {
        "PlatformDetails": "Windows",
        "UsageOperation": "RunInstances:0002"
    }
]
```

PowerShell

Per trovare le informazioni di fatturazione per un'AMI

Utilizza il cmdlet Get-EC2Image.

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | `
    Format-List PlatformDetails, UsageOperation
```

Di seguito è riportato un output di esempio per un'AMI Linux.

```
PlatformDetails : Linux/UNIX
UsageOperation  : RunInstances
```

Per trovare le informazioni di fatturazione per un'istanza

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances | `
    Format-List PlatformDetails, UsageOperation
```

Di seguito è riportato un esempio di istanza Windows.

```
PlatformDetails : Windows
UsageOperation  : RunInstances:0002
```

Verificare gli addebiti AMI in fattura

Per assicurarti di non incorrere in costi non pianificati, puoi verificare che i dati di fatturazione di un'istanza contenuti nel tuo AWS Cost and Usage Report (CUR) corrispondano ai dati di fatturazione associati all'AMI che hai utilizzato per avviare l'istanza.

Per confermare le informazioni di fatturazione, trovare l'ID istanza nel CUR e controllare il valore corrispondente nella colonna `lineitem/Operation`. Il valore deve corrispondere al valore Operazione di utilizzo associato all'AMI.

Ad esempio, l'AMI `ami-0123456789EXAMPLE` dispone delle seguenti informazioni di fatturazione:

- Dettagli della piattaforma = `Red Hat Enterprise Linux`
- Operazione di utilizzo = `RunInstances:0010`

Se è stata avviata un'istanza utilizzando questa AMI, è possibile trovare l'ID istanza nel CUR e controllare il valore corrispondente nella colonna `lineitem/Operation`. In questo esempio, il valore dovrebbe essere `RunInstances:0010`.

Quote AMI in Amazon EC2

Le seguenti quote si applicano alla creazione e alla condivisione. AMIs Le quote si applicano per Regione AWS.

Nome quota	Description	Quota predefinita per regione
AMIs	Il numero massimo di risorse pubbliche e private AMIs consentite per regione. Questi includono quelli disponibili, in sospeso AMIs, disabilitati e AMIs nel Cestino.	50.000
Pubblica AMIs	Il numero massimo di elementi pubblici AMIs, compresi quelli pubblici AMIs presenti nel Cestino, consentito per regione.	5
Condivisione AMI	Il numero massimo di entità (organizzazioni, unità organizzative (OUs) e account) con cui è possibile condividere un AMI in una regione. Tieni presente che se condividi un'AMI con un'organizzazione o un'unità organizzativa, il numero di account nell'organizzazione o nell'unità organizzativa non viene conteggiato ai fini della quota.	1.000

Se superi le tue quote e desideri crearne o condividerne altre AMIs, puoi fare quanto segue:

- Se superi la AMIs quota totale AMIs o pubblica, valuta la possibilità di annullare la registrazione delle immagini non utilizzate.
- Se superi la tua AMIs quota pubblica, prendi in considerazione la possibilità di rendere private una o più di esse. AMIs
- Se superi la quota di condivisione AMI, valuta la possibilità di condividerla AMIs con un'organizzazione o un'unità organizzativa anziché con account separati.
- Richiedi un aumento della quota per AMIs.

Richiedi un aumento della quota per AMIs

Se hai bisogno di una quota superiore a quella predefinita AMIs, puoi richiedere un aumento della quota.

Per richiedere un aumento della quota per AMIs

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/.
2. Nel pannello di navigazione, scegliere servizi AWS .
3. Scegli Amazon Elastic Compute Cloud (Amazon EC2) dall'elenco o digita il nome del servizio nella casella di ricerca.
4. Scegli la quota delle AMI per richiedere un aumento. Puoi scegliere tra:
   - AMIs
   - Pubblico AMIs
   - Condivisione AMI
5. Scegliere Request quota increase (Richiedi aumento di quota).
6. Sotto Change quota value (Modifica il valore della quota), inserisci il nuovo valore della quota, quindi seleziona Request (Richiedi).

Per visualizzare eventuali richieste in sospeso o risolte di recente, scegliere Dashboard dal riquadro di navigazione. Per le richieste in sospeso, scegliere lo stato della richiesta per aprire la ricevuta della richiesta. Lo stato iniziale di una richiesta è Pending (In attesa). Quando la denominazione dello stato cambia in Quota requested (Quota richiesta), vedrai il numero della pratica al di sotto di Support

Center case number (Numero del caso assegnato dal centro di supporto). Scegli il numero del caso per aprire il ticket della tua richiesta.

Dopo aver risolto la richiesta, il valore della quota applicata per la quota viene impostato sul nuovo valore.

Per maggiori informazioni, consulta Guida per l'utente di Service Quotas.

Istanze Amazon EC2

Un'istanza Amazon EC2 è un server virtuale nell'ambiente AWS cloud. Hai il pieno controllo sulla tua istanza, dal momento in cui la avvii per la prima volta (indicato come avvio di un'istanza) fino alla sua eliminazione (indicato come interruzione di un'istanza). Puoi scegliere tra una varietà di sistemi operativi quando avvii la tua istanza. Puoi connetterti alla tua istanza e personalizzarla secondo le tue esigenze. Ad esempio, puoi configurare il sistema operativo, installare aggiornamenti del sistema operativo e installare applicazioni sull'istanza.

Amazon EC2 fornisce un'ampia gamma di tipi di istanza. Puoi scegliere un tipo di istanza che fornisce le risorse di calcolo, la memoria, l'archiviazione e le prestazioni di rete necessarie per eseguire le applicazioni.

I prezzi di Amazon EC2 vengono calcolati in base all'uso effettivo. La fatturazione dell'istanza inizia all'avvio dell'istanza e passa allo stato di esecuzione. La fatturazione si arresta quando interrompi l'istanza e riprende quando avvii l'istanza. Quando interrompi l'istanza, la fatturazione si arresta quando passa allo stato di chiusura.

Amazon EC2 fornisce funzionalità che puoi utilizzare per ottimizzare le prestazioni e il costo delle istanze. Ad esempio, puoi utilizzare Amazon EC2 Fleet o Amazon EC2 Auto Scaling per aumentare o ridurre la capacità al variare dell'utilizzo dell'istanza. Puoi ridurre i costi delle istanze utilizzando istanze spot o Savings Plans.

Un'istanza gestita è gestita da un fornitore di servizi, come Amazon EKS Auto Mode. Non è possibile modificare direttamente le impostazioni di un'istanza gestita. Le istanze gestite sono identificate da un valore true nel campo Gestite. Per ulteriori informazioni, consulta Istanze gestite di Amazon EC2.

Funzionalità e attività

- Tipi di istanza Amazon EC2
- Istanze gestite di Amazon EC2
- Usa la virtualizzazione annidata per eseguire hypervisor nelle istanze Amazon EC2
- Opzioni di fatturazione e acquisto di Amazon EC2
- Archivia i parametri di avvio dell'istanza nei modelli di avvio di Amazon EC2
- Avviare un'istanza Amazon EC2
- Connettiti all'istanza EC2
- Cambio di stato di un'istanza Amazon EC2

- Ripristino automatico dell'istanza
- Utilizzo dei metadati dell'istanza per gestire l'istanza EC2
- Individua se un host è un'istanza EC2
- Documenti di identità dell'istanza per le istanze Amazon EC2
- Conformità STIG per la tua istanza EC2
- Sincronizzazione precisa dell'orologio e dell'ora sull'istanza EC2
- EC2 Capacity Manager
- Gestione dei driver di dispositivo per l'istanza EC2
- Configurazione dell'istanza Amazon EC2 Windows
- Aggiornamento di un'istanza EC2 Windows a una versione più recente di Windows Server
- Tutorial: Connessione di un'istanza Amazon EC2 a un database Amazon RDS

Tipi di istanza Amazon EC2

Quando si avvia un'istanza, il tipo di istanza specificato determina l'hardware del computer host utilizzato per tale istanza. Ogni tipo di istanza è caratterizzato da diverse capacità di calcolo, memoria e archiviazione ed è raggruppato in famiglie di istanze basate su tali capacità. Seleziona un tipo di istanza in base ai requisiti dell'applicazione o del software che intendi eseguire sull'istanza. Per ulteriori informazioni sulle funzionalità e i casi d'uso, consulta Tipi di istanze Amazon EC2.

Amazon EC2 dedica alcune risorse del computer host, come CPU, memoria e archiviazione dell'istanza, a un'istanza specifica. Amazon EC2 condivide altre risorse del computer host, ad esempio la rete e il sottosistema del disco, tra le istanze. Se ogni istanza in un computer host cerca di utilizzare la maggior quantità possibile di queste risorse condivise, a ciascuna istanza viene assegnata la stessa quantità di una risorsa. Tuttavia, quando viene utilizzata una quantità inferiore di una risorsa, un'istanza potrà utilizzare una quantità maggiore di tale risorsa in base alla sua disponibilità.

Ogni tipo di istanza fornisce prestazioni minime inferiori o superiori in base a una risorsa condivisa. Ad esempio, i tipi di istanza ad alte I/O prestazioni hanno un'allocazione maggiore di risorse condivise. L'allocazione di una quota maggiore di risorse condivise riduce anche la varianza delle prestazioni. I/O Per la maggior parte delle applicazioni, I/O prestazioni moderate sono più che sufficienti. Tuttavia, per le applicazioni che richiedono I/O prestazioni maggiori o più costanti, considera un tipo di istanza con I/O prestazioni più elevate.

Indice

- Tipi di istanza disponibili
- Specifiche dell'hardware
- Tipi di hypervisor
- Tipi di virtualizzazione dell'AMI
- Processori
- Individuazione di un tipo di istanza Amazon EC2
- Ottieni consigli dallo strumento di ricerca del tipo di istanza EC2
- Ottieni suggerimenti sulle istanze EC2 proposti da Compute Optimizer
- Modifiche del tipo di istanza Amazon EC2
- Istanze a prestazioni espandibili
- Accelerazione delle prestazioni con istanze GPU
- Istanze Amazon EC2 Mac
- Tipi di istanze Amazon EBS-optimized
- Opzioni della CPU per le istanze Amazon EC2
- Istanze AMD SEV-SNP per Amazon EC2
- Controllo degli stati del processore delle istanze Linux Amazon EC2

Tipi di istanza disponibili

Amazon EC2 offre un'ampia selezione di tipi di istanza ottimizzati per adattarsi a diversi casi d'uso. I tipi di istanza comprendono diverse combinazioni di CPU, memoria, archiviazione e capacità di rete, inoltre offrono la flessibilità necessaria per scegliere la combinazione di risorse appropriata per le applicazioni. Ogni tipo di istanza include una o più dimensioni di istanza, consentendo di ridimensionare le risorse in base ai requisiti del carico di lavoro di destinazione.

Convenzioni di denominazione dei tipi di istanza

I nomi sono basati sulla famiglia, sulla generazione, sulla famiglia del processore, sulle funzionalità e sulle dimensioni dell'istanza. Per ulteriori informazioni, consulta Convenzioni di denominazione nella Guida ai tipi di istanza Amazon EC2.

Individuazione di un tipo di istanza

Per determinare quali tipi di istanza soddisfano i requisiti, ad esempio le regioni supportate, le risorse di calcolo o le risorse di archiviazione, consultare Individuazione di un tipo di istanza Amazon EC2 e le Specifiche dei tipi di istanza Amazon EC2 nella Guida ai tipi di istanza Amazon EC2.

Specifiche dell'hardware

Per specifiche dettagliate, consultare Specifiche nella Guida ai tipi di istanza Amazon EC2. Per informazioni sui prezzi, consulta i On-Demand prezzi di Amazon EC2.

Per determinare il tipo di istanza più idoneo alle specifiche esigenze, ti consigliamo di avviare un'istanza e utilizzare la tua applicazione per il benchmark. Dal momento che l'addebito dei costi viene calcolato al secondo, è più conveniente eseguire il test di più tipi di istanza prima di prendere una decisione. Se le esigenze cambiano nel tempo dopo una decisione specifica, si potrà sempre ridimensionare l'istanza in un secondo momento. Per ulteriori informazioni, consulta Modifiche del tipo di istanza Amazon EC2.

Tipi di hypervisor

Amazon EC2 supporta i seguenti hypervisor: Xen e Nitro.

Nitro-based istanze

- Uso generico: M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6a | M6g | M6gd | M6i | M6id | M6idn | M6in | M7a | M7g | M7gd | M7i | | M8a | M8a | M8aZn | M8g | M8gb | M8gd | M8Gn | M8i | M8id | | M8in | M8idn | M8ine | M8iN | M8ib | M8idb | M9g | M9gd | T3 | T3a | M7i-flex T4g M8i-flex
- Ottimizzato per il calcolo: C5 | C5a | C5ad | C5d | C5n | C6a | C6g | C6gd | C6gn | C6i | C6id | C6in | C7a | C7g | C7gd | C7gn | C7i C7i-flex | | C8a | C8g | C8gb | C8gd | C8gn | C8i | C8id | C8i-flex | C8in | C8ine | C8ib | C9g | C9gd
- Memoria ottimizzata: R5 | R5a | R5ad | R5b | R5d | R5dn | R5n | R6a | R6g | R6gd | R6i | R6id | R6idn | R6in | R7a | R7g | R7gd | R7i | R7iz | R8a | R8g | R8gb | R8gb | R8gb Gd | R8gn | R8i | R8id | | | | R8in | R8idn | R8ib | R8idb R8i-flex | R9g | | | | | | | | | | | | X2gd | X2idn | X2iedn | X2iEdn U-3tb1 U-6tb1 U-9tb1 U-12tb1 U-18tb1 | X2iezn U-24tb1 U7i-6tb U7i-8tb U7i-12tb | X8g U7in-16tb U7in-24tb U7in-32tb U7inh-32tb | X8aedz | X8i | z1d
- Ottimizzate per l'archiviazione: D3 | D3en | I3en | I4g | I4i | I7i | I7ie | I8g | I8ge | Im4gn | Is4gen
- Calcolo accelerato: DL1 | DL2q | F2 | G4ad | G4dn | G5 | G5g | G6 | G6e | G6f | Gr6 | Gr6f | G7 | G7e | Inf1 | Inf2 | P4d | P4de | P5 | P5e | P5en | | | Trn1 P6-B200 P6-B300 P6e-GB200 | Trn1n | Trn2 | Trn2 | Trn2 N2u | VT1

- High-performance elaborazione: HPC6a | HPC6id | HPC7a | HPC7g | HPC8a
- Generazione precedente: A1 | P3dn

Per ulteriori informazioni sulle versioni supportate dell'hypervisor Nitro, consultare Supporto delle funzionalità di rete nella Guida ai tipi di istanza Amazon EC2.

Xen-based istanze

- Uso generico: M1 | M2 | M3 | M4 | T1 | T2
- Ottimizzate per il calcolo: C1 | C3 | C4
- Ottimizzate per la memoria: R3 | R4 | X1 | X1e
- Ottimizzate per l'archiviazione: D2 | H1 | I2 | I3
- Calcolo accelerato: G3 | P3

Tipi di virtualizzazione dell'AMI

Il tipo di virtualizzazione dell'istanza viene determinato dall'AMI utilizzata per avviarla. I tipi di istanza della generazione corrente supportano solo la tipologia HVM (Hardware Virtual Machine). Alcuni tipi di istanze di generazione precedente supportano le istanze paravirtuali (PV) e alcune regioni supportano le istanze PV. AWS Per ulteriori informazioni, consulta Tipi di virtualizzazione.

Per ottenere prestazioni migliori, ti consigliamo di usare un'AMI HVM. Inoltre, è consigliabile utilizzare le AMI HVM se desideri sfruttare le funzionalità avanzate di rete. La virtualizzazione HVM utilizza la tecnologia di assistenza hardware fornita dalla piattaforma. AWS Con la virtualizzazione HVM, la VM guest viene eseguita come se si trovasse su una piattaforma di hardware nativo, con la differenza che utilizza comunque driver di archiviazione e una rete PV per migliorare le prestazioni.

Processori

Le istanze EC2 supportano diversi processori.

Processori

- Processori Intel
- Processori AMD
- AWS Processori Graviton
- AWS Trainium

- AWS Inferentia

Processori Intel

Le istanze Amazon EC2 eseguite su processori Intel possono includere le seguenti funzionalità. Non tutte le istanze eseguite su processori Intel supportano tutte le funzionalità. Per informazioni sulle funzionalità disponibili per ciascun tipo di istanza, consultare Tipi di istanza Amazon EC2.

- Intel AES New Instructions (AES-NI): il set di istruzioni di AES-NI crittografia Intel migliora l'algoritmo originale Advanced Encryption Standard (AES) per fornire una protezione dei dati più rapida e una maggiore sicurezza. Tutte le istanze EC2 di attuale generazione supportano questa caratteristica del processore.
- Intel Advanced Vector Extensions (Intel AVX, Intel AVX2 e IntelAVX-512): Intel AVX e Intel AVX2 sono a 256 bit e Intel AVX-512 è un'estensione del set di istruzioni a 512 bit progettata per applicazioni che richiedono un uso intensivo di Floating Point (FP). Le istruzioni Intel AVX migliorano le prestazioni per applicazioni quali immagini ed audio/video elaborazione, simulazioni scientifiche, analisi finanziarie e modellazione e analisi 3D. Queste funzionalità sono disponibili solo su istanze avviate con AMI HVM.
- Tecnologia Intel Turbo Boost — I processori Intel Turbo Boost eseguono automaticamente i core più velocemente della frequenza operativa di base.
- Intel Deep Learning Boost (Intel DL Boost) — Accelera i casi d'uso di deep learning AI. I processori scalabili Intel Xeon di seconda generazione ampliano Intel AVX-512 con una nuova Vector Neural Network Instruction (VNNI/INT8) che aumenta significativamente le prestazioni di inferenza del deep learning rispetto ai processori scalabili Intel Xeon della generazione precedente (con FP32) per immagini recognition/segmentation, rilevamento di oggetti, riconoscimento vocale, traduzione linguistica, sistemi di raccomandazione, apprendimento per rinforzo e altro ancora. VNNI potrebbe non essere compatibile con tutte le distribuzioni di Linux.

  Le istanze seguenti supportano VNNI: `M5n`, `R5n`, `M5dn`, `M5zn`, `R5b`, `R5dn`, `D3`, `D3en` e `C6i`. Le istanze `C5` e `C5d` supportano VNNI solo per le istanze `12xlarge`, `24xlarge` e `metal`.

Tuttavia, potrebbe sorgere un certo livello di confusione per via delle convenzioni di denominazione standard per le CPU a 64 bit. Il produttore di chip Advanced Micro Devices (AMD) ha introdotto la prima architettura a 64 bit di successo basata sul set di istruzioni Intel x86. Di conseguenza, a questo tipo di architettura viene in genere fatto riferimento con AMD64, indipendentemente dal produttore. Windows e numerose distribuzioni Linux si conformano a questo standard. Ciò spiega il motivo per

cui nelle informazioni sul sistema esterno in un'istanza EC2 in Ubuntu o Windows l'architettura della CPU viene definita come AMD64, anche se le istanze vengono eseguite su hardware Intel.

Processori AMD

Le istanze Amazon EC2 eseguite su processori AMD EPYC possono aiutare a ottimizzare sia i costi che le prestazioni dei carichi di lavoro. Queste istanze potrebbero supportare le funzionalità del processore riportate di seguito. Non tutte le istanze eseguite su processori AMD supportano tutte le funzionalità. Per informazioni sulle funzionalità disponibili per ciascun tipo di istanza, consultare Tipi di istanza Amazon EC2.

- AMD Secure Memory Encryption (SME)
- AMD Transparent Single Key Memory Encryption (TSME)
- Estensioni AMD Advanced Vector (AVX)
- SEV-SNPAMD Secure Encrypted Nested Paging () Virtualization-Secure
- Istruzioni di rete neurale vettoriale (VNNI)
- BFloat16

AWS Processori Graviton

AWS Graviton è una famiglia di processori progettata per offrire il miglior rapporto prezzo/prestazioni per i carichi di lavoro in esecuzione su istanze Amazon EC2.

Per ulteriori informazioni, consulta Nozioni di base di Graviton.

AWS Trainium

Le istanze basate su AWS Trainium sono progettate appositamente per l'addestramento ad alte prestazioni e conveniente di modelli di deep learning. È possibile utilizzare queste istanze per addestrare modelli per l'elaborazione del linguaggio naturale, la visione artificiale e la funzione di suggerimento utilizzati in un'ampia gamma di applicazioni, ad esempio riconoscimento vocale, suggerimenti, rilevamento di frodi e classificazione di immagini e video. Usa i flussi di lavoro esistenti nei framework ML più diffusi, come e. PyTorch TensorFlow

AWS Inferentia

Le istanze basate su AWS Inferentia sono progettate per accelerare il machine learning. Offrono inferenza di machine learning con elevate prestazioni e bassa latenza. Queste istanze sono

ottimizzate per la distribuzione di modelli di Deep Learning (DL) per applicazioni, quali l'elaborazione del linguaggio naturale, il rilevamento e la classificazione degli oggetti, la personalizzazione e il filtro dei contenuti e il riconoscimento vocale.

È possibile iniziare in diversi modi:

- Usa l' SageMaker intelligenza artificiale, un servizio completamente gestito che è il modo più semplice per iniziare con i modelli di machine learning. Per ulteriori informazioni, consulta Get Started with SageMaker AI nella Amazon SageMaker AI Developer Guide.
- Avvia un'istanza Inf1 o Inf2 utilizzando l'AMI Deep Learning. Per ulteriori informazioni, consulta AWS Inferentia con DLAMI nella Guida per gli sviluppatori di AWS Deep Learning AMIs .
- Avvia un'istanza Inf1 o Inf2 utilizzando la tua AMI e installa l'SDK AWS Neuron, che consente di compilare, eseguire e profilare modelli di deep learning per AWS Inferentia.
- Avvia un'istanza container utilizzando un'istanza Inf1 o Inf2 e un'Amazon ECS-optimized AMI. Per ulteriori informazioni, consulta AMI Amazon Linux 2 (Inferentia) in Amazon Elastic Container Service Developer Guide.
- Creare un cluster Amazon EKS con nodi che eseguono istanze Inf1. Per maggiori informazioni, consulta Supporto Inferentia nella Guida per l'utente di Amazon EKS.

Individuazione di un tipo di istanza Amazon EC2

Prima di poter avviare un'istanza, devi selezionare un tipo di istanza da utilizzare. Il tipo di istanza scelto può dipendere dalle risorse richieste dal carico di lavoro, ad esempio risorse di elaborazione, memoria o archiviazione. Può essere utile identificare diversi tipi di istanze che potrebbero adattarsi al carico di lavoro e valutarne le prestazioni in un ambiente di test. Non ci sono alternative per misurare le prestazioni dell'applicazione sotto carico.

Puoi ottenere suggerimenti e indicazioni per i tipi di istanza EC2 tramite lo strumento di ricerca del tipo di istanza EC2. Per ulteriori informazioni, consulta the section called “Strumento di ricerca del tipo di istanza EC2”.

Se disponi già di istanze EC2 in esecuzione, puoi utilizzarle AWS Compute Optimizer per ottenere consigli sui tipi di istanze da utilizzare per migliorare le prestazioni, risparmiare denaro o entrambi. Per ulteriori informazioni, consulta the section called “Suggerimenti sul Compute Optimizer”.

Processi

- Individuazione di un tipo di istanza mediante la console

- Descrivi un tipo di istanza utilizzando AWS CLI
- Trova un tipo di istanza usando AWS CLI
- Trova un tipo di istanza utilizzando gli strumenti per PowerShell

Individuazione di un tipo di istanza mediante la console

Puoi individuare un tipo di istanza che soddisfa le esigenze utilizzando la console Amazon EC2.

Per individuare un tipo di istanza mediante la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dalla barra di navigazione selezionare la regione in cui avviare le istanze. È possibile selezionare qualsiasi regione disponibile, indipendentemente dalla posizione.
3. Nel riquadro di navigazione, scegliere Instance Types (Tipi di istanza).
4. (Facoltativo) Scegli l'icona delle preferenze (ingranaggio) per selezionare gli attributi del tipo di istanza da visualizzare, ad esempio i prezzi di On-Demand Linux, quindi scegli Conferma. In alternativa, seleziona il nome di un tipo di istanza per aprire la pagina dei dettagli e visualizzare tutti gli attributi disponibili tramite la console. La console non visualizza tutti gli attributi disponibili tramite l'API o la riga di comando.
5. Utilizzare gli attributi del tipo di istanza per filtrare l'elenco dei tipi di istanza visualizzati ai soli tipi di istanza che soddisfano le proprie esigenze. Ad esempio, è possibile applicare un filtro ai seguenti attributi:

   - Zone di disponibilità: il nome della zona di disponibilità, della zona locale o della zona Wavelength. Per ulteriori informazioni, consulta the section called "Regioni e zone".
   - vCPU o Core: il numero di vCPU o core.
   - Memoria (GiB): la dimensione della memoria in GiB.
   - Prestazioni di rete: le prestazioni di rete, in Gigabit.
   - Storage dell'istanza locale: indica se il tipo di istanza dispone di archiviazione dell'istanza locale (`true` | `false`).
6. (Facoltativo) Per visualizzare un confronto affiancato, seleziona la casella di controllo per più tipi di istanza. Il confronto viene visualizzato nella parte inferiore dello schermo.
7. (Facoltativo) Per salvare l'elenco di tipi di istanza in un file di valori separati da virgola (.csv) per ulteriore analisi, scegliere Actions (Operazioni), Download list CSV (Scarica elenco CSV). Il file include tutti i tipi di istanza che corrispondono ai filtri impostati.

8. (Facoltativo) Per avviare istanze utilizzando un tipo di istanza che soddisfa le proprie esigenze, selezionare la casella di controllo per il tipo di istanza e scegliere Actions (Operazioni), Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

Descrivi un tipo di istanza utilizzando AWS CLI

Puoi usare il comando describe-instance-types per descrivere un tipo di istanza specifico.

Per descrivere in modo completo un tipo di istanza

Il seguente comando visualizza tutti i dettagli disponibili per il tipo di istanza specificato. L'output è lungo, quindi viene omesso qui.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2
```

Descrivono un tipo di istanza e filtrano l'output

Il seguente comando visualizza i dettagli di rete per il tipo di istanza specificato.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2 \
    --query "InstanceTypes[].NetworkInfo"
```

Di seguito è riportato un output di esempio.

```
[
    {
        "NetworkPerformance": "Low to Moderate",
        "MaximumNetworkInterfaces": 2,
        "MaximumNetworkCards": 1,
        "DefaultNetworkCardIndex": 0,
        "NetworkCards": [
            {
                "NetworkCardIndex": 0,
                "NetworkPerformance": "Low to Moderate",
                "MaximumNetworkInterfaces": 2,
```

```
                "BaselineBandwidthInGbps": 0.064,
                "PeakBandwidthInGbps": 1.024
            }
        ],
        "Ipv4AddressesPerInterface": 2,
        "Ipv6AddressesPerInterface": 2,
        "Ipv6Supported": true,
        "EnaSupport": "unsupported",
        "EfaSupported": false,
        "EncryptionInTransitSupported": false,
        "EnaSrdSupported": false
    }
]
```

Il seguente comando visualizza la memoria disponibile per il tipo di istanza specificato.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2 \
    --query "InstanceTypes[].MemoryInfo"
```

Di seguito è riportato un output di esempio.

```
[
    {
        "SizeInMiB": 1024
    }
]
```

Trova un tipo di istanza usando AWS CLI

Puoi utilizzare i comandi describe-instance-types e describe-instance-type-offerings per trovare i tipi di istanza che soddisfano le tue esigenze.

Esempi

- Esempio 1: Trova un tipo di istanza in base alla zona di disponibilità
- Esempio 2: Trova un tipo di istanza in base alla dimensione della memoria disponibile
- Esempio 3: Trova un tipo di istanza in base all'archiviazione di istanza disponibile
- Esempio 4: Trova un tipo di istanza che supporti l'ibernazione

Esempio 1: Trova un tipo di istanza in base alla zona di disponibilità

Il seguente esempio visualizza solo i tipi di istanza offerti nella zona di disponibilità specificata.

```
aws ec2 describe-instance-type-offerings \
    --location-type "availability-zone" \
    --filters "Name=location,Values=us-east-2a" \
    --region us-east-2 \
    --query "InstanceTypeOfferings[*].[InstanceType]" --output text | sort
```

L'output è un elenco di tipi di istanze, in ordine alfabetico. Di seguito è riportato solo l'inizio dell'output.

```
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge
c4.2xlarge
   ...
```

Esempio 2: Trova un tipo di istanza in base alla dimensione della memoria disponibile

Il comando seguente visualizza solo i tipi di istanza della generazione attuale con 64 GiB (65.536 MiB) di memoria.

```
aws ec2 describe-instance-types \
    --filters "Name=current-generation,Values=true" "Name=memory-info.size-in-
mib,Values=65536" \
    --region us-east-2 \
    --query "InstanceTypes[*].[InstanceType]" --output text | sort
```

L'output è un elenco di tipi di istanze, in ordine alfabetico. Di seguito è riportato solo l'inizio dell'output.

```
c5a.8xlarge
c5ad.8xlarge
c6a.8xlarge
c6g.8xlarge
c6gd.8xlarge
c6gn.8xlarge
c6i.8xlarge
```

```
c6id.8xlarge
c6in.8xlarge
   ...
```

Esempio 3: Trova un tipo di istanza in base all'archiviazione di istanza disponibile

Nell'esempio seguente viene visualizzata la dimensione totale dell'archiviazione dell'istanza per tutte le istanze R7 con volumi dell'archivio dell'istanza.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r7*" "Name=instance-storage-
supported,Values=true" \
    --region us-east-2 \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

Di seguito è riportato un output di esempio.

```
---------------------------
|  DescribeInstanceTypes  |
+----------------+--------+
|  r7gd.xlarge   |  237   |
|  r7gd.8xlarge  |  1900  |
|  r7gd.16xlarge |  3800  |
|  r7gd.medium   |  59    |
|  r7gd.4xlarge  |  950   |
|  r7gd.2xlarge  |  474   |
|  r7gd.metal    |  3800  |
|  r7gd.large    |  118   |
|  r7gd.12xlarge |  2850  |
+----------------+--------+
```

Esempio 4: Trova un tipo di istanza che supporti l'ibernazione

Il seguente esempio visualizza i tipi di istanza che supportano l'ibernazione.

```
aws ec2 describe-instance-types \
    --filters "Name=hibernation-supported,Values=true" \
    --region us-east-2 \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

L'output è un elenco di tipi di istanze, in ordine alfabetico. Di seguito è riportato solo l'inizio dell'output.

```
c4.2xlarge
c4.4xlarge
c4.8xlarge
c4.large
c4.xlarge
c5.12xlarge
c5.18xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
...
```

Trova un tipo di istanza utilizzando gli strumenti per PowerShell

È possibile utilizzare i Get-EC2InstanceTypeOffering cmdlet Get-EC2InstanceType and per trovare i tipi di istanza che soddisfano le proprie esigenze.

Esempi

- Trova un tipo di istanza in base alla zona di disponibilità
- Trova un tipo di istanza in base alla dimensione della memoria disponibile
- Trova un tipo di istanza in base all'archiviazione di istanza disponibile
- Trova un tipo di istanza che supporti l'ibernazione

Trova un tipo di istanza in base alla zona di disponibilità

Il seguente esempio visualizza solo i tipi di istanza offerti nella zona di disponibilità specificata.

```
(Get-EC2InstanceTypeOffering `
    -LocationType "availability-zone" `
    -Region us-east-2 `
    -Filter @{Name="location"; Values="us-east-2a"}).InstanceType | Sort-Object `
```

Trova un tipo di istanza in base alla dimensione della memoria disponibile

Il comando seguente visualizza solo i tipi di istanza della generazione attuale con 64 GiB (65.536 MiB) di memoria.

```
(Get-EC2InstanceType `
```

```
    -Filter @{Name="current-generation"; Values="true"},
            @{Name="memory-info.size-in-mib"; Values="65536"}).InstanceType | Sort-
Object
```

Trova un tipo di istanza in base all'archiviazione di istanza disponibile

Nell'esempio seguente viene visualizzata la dimensione totale dell'archiviazione dell'istanza per tutte le istanze R7 con volumi dell'archivio dell'istanza.

```
Get-EC2InstanceType `
    -Filter @{Name="instance-type"; Values="r7*"},
            @{Name="instance-storage-supported"; Values="true"} | `
     Select InstanceType, @{Name="TotalSizeInGB";
 Expression={($_.InstanceStorageInfo.TotalSizeInGB)}}
```

Di seguito è riportato un output di esempio.

```
InstanceType  TotalSizeInGB
------------  -------------
r7gd.8xlarge           1900
r7gd.16xlarge          3800
r7gd.xlarge             237
r7gd.4xlarge            950
r7gd.medium              59
r7gd.2xlarge            474
r7gd.large              118
r7gd.metal             3800
r7gd.12xlarge          2850
```

Trova un tipo di istanza che supporti l'ibernazione

Il seguente esempio visualizza i tipi di istanza che supportano l'ibernazione.

```
(Get-EC2InstanceType `
    -Filter @{Name="hibernation-supported"; Values="true"}).InstanceType | Sort-Object
```

Ottieni consigli dallo strumento di ricerca del tipo di istanza EC2

Lo strumento di ricerca del tipo di istanza EC2 considera il caso d'uso, il tipo di carico di lavoro, le preferenze del produttore della CPU e il modo in cui dai priorità a prezzo e prestazioni, nonché

i parametri aggiuntivi che puoi specificare. Utilizza quindi questi dati per fornire indicazioni e suggerimenti per i tipi di istanze Amazon EC2 più adatti ai nuovi carichi di lavoro.

Con un numero così elevato di tipi di istanza disponibili, trovare i tipi di istanza adatti per il proprio carico di lavoro può essere complesso e richiedere molto tempo. Utilizzando lo strumento di ricerca dei tipi di istanze EC2, puoi rimanere aggiornato sui tipi di istanze più recenti e ottenere il miglior rapporto prezzo/prestazioni per i tuoi carichi di lavoro.

Puoi ottenere suggerimenti e indicazioni per i tipi di istanza EC2 tramite la console Amazon EC2. Puoi anche passare direttamente ad Amazon Q per chiedere, ad esempio, consigli sul tipo di istanza. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon Q Developer.

Se stai cercando, ad esempio, consigli di tipo di istanza per un carico di lavoro esistente, usa AWS Compute Optimizer. Per ulteriori informazioni, consulta Ottieni suggerimenti sulle istanze EC2 proposti da Compute Optimizer.

Utilizzo dello strumento di ricerca del tipo di istanza EC2

Nella console Amazon EC2 puoi ottenere suggerimenti sul tipo di istanza dallo strumento di ricerca del tipo di istanza EC2 nella procedura guidata di avvio dell'istanza, durante la creazione di un modello di avvio o nella pagina Tipi di istanza.

Utilizza le seguenti istruzioni per ottenere indicazioni e suggerimenti per i tipi di istanza EC2 utilizzando lo strumento di ricerca del tipo di istanza EC2 nella console Amazon EC2. Per visualizzare un'animazione di questi passaggi, consulta Visualizza un'animazione: ottieni suggerimenti sul tipo di istanza utilizzando lo strumento di ricerca del tipo di istanza EC2.

Per ottenere suggerimenti sul tipo di istanza tramite lo strumento di ricerca del tipo di istanza EC2

1. Puoi avviare il processo utilizzando una delle seguenti opzioni:
   - Segui la procedura per avviare un'istanza. Accanto a Tipo di istanza, scegli il link Fatti consigliare.
   - Segui questa procedura per creare un modello di avvio. Accanto a Tipo di istanza, scegli il link Fatti consigliare.
   - Nel riquadro di navigazione, scegli Tipi di istanza, quindi scegli il pulsante Ricerca tipo di istanza.
2. Nella schermata Ottieni consigli sulla selezione del tipo di istanza, procedi come segue:

a. Specifica i requisiti del tipo di istanza selezionando le opzioni relative a Tipo di carico di lavoro, Caso d'uso, Priorità e Produttori della CPU.

b. (Facoltativo) Per specificare requisiti più dettagliati per il carico di lavoro, procedi come segue:

   i. Espandi Parametri avanzati.

   ii. Per aggiungere un parametro, selezionane uno, scegli Aggiungi e specifica un valore per il parametro. Ripeti la procedura per ogni altro parametro che desideri aggiungere. Se non desideri indicare alcun valore minimo o massimo, lascia vuoto il campo.

   iii. Per rimuovere un parametro dopo averlo aggiunto, scegli la X accanto al parametro.

c. Scegli Ricevi consigli sul tipo di istanza.

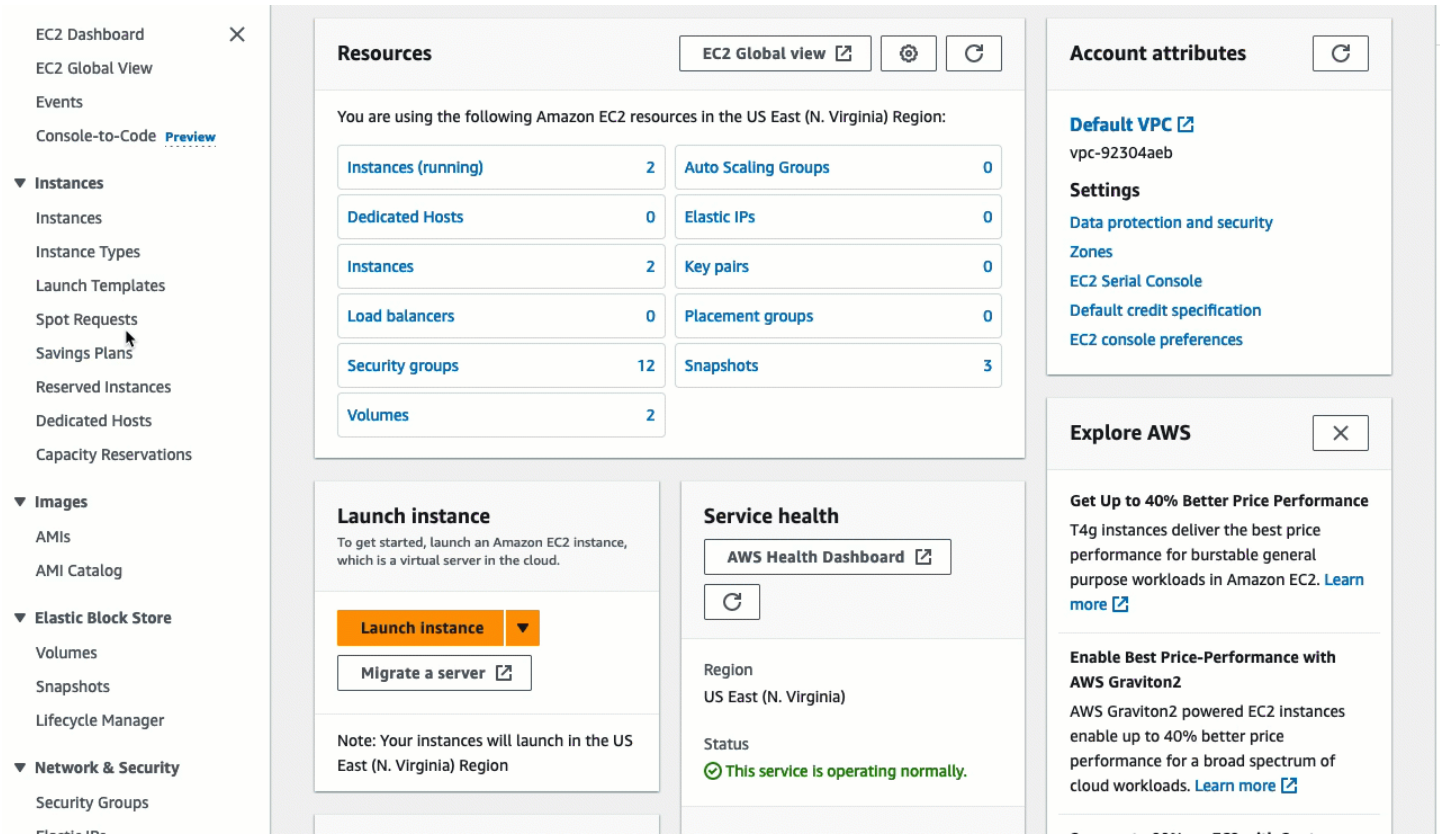
   Amazon EC2 ti fornisce suggerimenti per le famiglie di istanza che soddisfano i requisiti da te specificati.

3. Per visualizzare i dettagli di ciascun tipo di istanza all'interno delle famiglie di istanza suggerite, scegli Visualizza i dettagli della famiglia di istanza consigliata.

4. Seleziona un tipo di istanza che soddisfi i tuoi requisiti, quindi scegli Azioni, Avvia istanza o Azioni, Crea modello di avvio.

   In alternativa, se hai avviato il processo nella procedura guidata di avvio dell'istanza o nella pagina del modello di avvio e preferisci tornare al flusso originale, prendi nota del tipo di istanza che desideri utilizzare. Quindi, nella procedura guidata di avvio dell'istanza o nel modello di avvio, per Tipo di istanza scegli il tipo di istanza e completa la procedura per avviare un'istanza o creare un modello di avvio.

Visualizza un'animazione: ottieni suggerimenti sul tipo di istanza utilizzando lo strumento di ricerca del tipo di istanza EC2



Ottieni suggerimenti sulle istanze EC2 proposti da Compute Optimizer

AWS Compute Optimizer fornisce consigli su Amazon EC2 per aiutarti a migliorare le prestazioni, risparmiare denaro o entrambe le cose. Puoi utilizzare questi suggerimenti per decidere se passare o meno a un nuovo tipo di istanza.

Per fornire le raccomandazioni, Compute Optimizer analizza le specifiche delle istanze esistenti e i parametri di utilizzo. I dati compilati vengono quindi utilizzati per raccomandare i tipi di istanza Amazon EC2 più adatti per gestire il carico di lavoro esistente. Le raccomandazioni vengono restituite insieme ai prezzi delle istanze per ora. Per ulteriori informazioni, consulta Parametri di istanza Amazon EC2 nella Guida per l'utente di AWS Compute Optimizer .

Indice

- Requisiti
- Individuazione delle classificazioni
- Visualizzare le raccomandazioni

- Considerazioni sulla valutazione delle raccomandazioni

Requisiti

Per ricevere suggerimenti da Compute Optimizer, devi prima scegliere Compute Optimizer. Per ulteriori informazioni, consulta Nozioni di base su AWS Compute Optimizer nella Guida per l'utente di AWS Compute Optimizer .

Compute Optimizer genera suggerimenti per alcuni tipi di istanza, ma non per tutti i tipi di istanza. Se utilizzi un tipo di istanza non supportato, Compute Optimizer non genererà suggerimenti. Per l'elenco dei tipi di istanza supportati, consulta i Requisiti delle istanze Amazon EC2 nella Guida per l'utente di AWS Compute Optimizer .

Individuazione delle classificazioni

Compute Optimizer classifica le sue conclusioni per le istanze EC2 come segue:

- Under-provisioned— Un'istanza EC2 è considerata insufficiente quando almeno una specifica dell'istanza, ad esempio CPU, memoria o rete, non soddisfa i requisiti prestazionali del carico di lavoro. Under-provisioned Le istanze EC2 potrebbero portare a prestazioni scadenti delle applicazioni.
- Over-provisioned— Un'istanza EC2 è considerata sovra-provisioning quando almeno una specifica dell'istanza, ad esempio CPU, memoria o rete, può essere ridotta pur soddisfacendo i requisiti prestazionali del carico di lavoro e quando nessuna specifica è sottoposta a provisioning insufficiente. Over-provisioned Le istanze EC2 potrebbero comportare costi di infrastruttura non necessari.
- Optimized (Ottimizzata)– Un'istanza EC2 viene considerata ottimizzata quando tutte le specifiche dell'istanza, ad esempio CPU, memoria e rete, soddisfano i requisiti di prestazioni del carico di lavoro e l'istanza non presenta provisioning eccessivo. Un'istanza EC2 ottimizzata esegue i carichi di lavoro con prestazioni e costi di infrastruttura ottimali. Per le istanze ottimizzate, Compute Optimizer può talvolta raccomandare un tipo di istanza di nuova generazione.
- None (Nessuna) – Non ci sono raccomandazioni per questa istanza. Ciò potrebbe verificarsi se Compute Optimizer è stato attivato da meno di 12 ore o quando l'istanza è in esecuzione da meno di 30 ore o quando il tipo di istanza non è supportato da Ottimizzatore di calcolo.

Visualizzare le raccomandazioni

Dopo aver effettuato l'accesso su Compute Optimizer, puoi visualizzare i risultati generati da Compute Optimizer per le istanze EC2 nella console Amazon EC2. Puoi quindi accedere alla console Compute Optimizer per visualizzare i suggerimenti. Se hai aderito di recente, i risultati potrebbero non essere visualizzati nella console EC2 per un massimo di 12 ore.

Per visualizzare suggerimenti per un'istanza tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Scegli l'ID dell'istanza per aprire la relativa pagina dei dettagli.
4. Nella pagina dei dettagli dell'istanza, nella sezione di riepilogo superiore, trova Individua AWS Compute Optimizer . Se c'è un risultato, visualizziamo la classificazione del risultato e un link per visualizzarne i dettagli. In caso contrario, viene visualizzato Nessun suggerimento disponibile per questa istanza.
5. Se c'è un risultato, scegli Visualizza dettagli. Si apre la pagina Suggerimenti per istanze EC2 nella console di Compute Optimizer. Il tipo di istanza attuale è denominato Attuale. Vi sono anche fino a tre suggerimenti per il tipo di istanza, denominate come Opzione 1, Opzione 2 e Opzione 3. Questa pagina mostra anche i dati CloudWatch metrici recenti per l'istanza.

Per visualizzare i suggerimenti per tutte le istanze in tutte le regioni

Puoi visualizzare i suggerimenti per tutte le tue istanze Amazon EC2 in tutte le regioni utilizzando la console di Compute Optimizer. Per ulteriori informazioni, consulta Visualizzazione di suggerimenti sulle istanze EC2 e Visualizzazione dei dettagli delle istanze EC2 nella Guida per l'utente di AWS Compute Optimizer .

Considerazioni sulla valutazione delle raccomandazioni

Quando ricevi un suggerimento, devi decidere se agire di conseguenza. Prima di modificare un tipo di istanza, considera quanto segue:

- Le raccomandazioni non prevedono l'utilizzo. Le raccomandazioni si basano sull'utilizzo cronologico dell'ultimo periodo di 14 giorni. Assicurati di scegliere un tipo di istanza che soddisfi le tue esigenze future in termini di risorse.
- Concentrati sui parametri dei grafici per determinare se l'utilizzo effettivo è inferiore alla capacità dell'istanza. Puoi anche visualizzare i dati delle metriche (media, picco, percentile) CloudWatch

per valutare ulteriormente i consigli sulle istanze EC2. Ad esempio, verifica se i parametri in percentuale della CPU durante il giorno cambiano e se si verifichino picchi che devono essere gestiti. Per ulteriori informazioni, consulta Visualizzare le metriche disponibili nella Amazon User Guide. CloudWatch

- Compute Optimizer può fornire raccomandazioni per le istanze a prestazioni espandibili, ossia le istanze T3, T3a e T2. Se periodicamente ti espandi oltre la linea di base, assicurati di poterlo continuare a fare in base alle vCPU del nuovo tipo di istanza. Per ulteriori informazioni, consulta Concetti chiave per istanze a prestazioni espandibili.
- Se hai acquistato un'istanza riservata, la tua On-Demand istanza potrebbe essere fatturata come istanza riservata. Prima di modificare il tipo di istanza corrente, valuta innanzitutto l'impatto sull'utilizzo e sulla copertura dell'Istanza riservata.
- Laddove possibile, valuta il passaggio a istanze di ultima generazione.
- Quando esegui la migrazione a una famiglia di istanze diversa, assicurati che il tipo di istanza corrente e il nuovo tipo di istanza siano compatibili, ad esempio in termini di virtualizzazione, architettura o tipo di rete. Per ulteriori informazioni, consulta Compatibilità per la modifica del tipo di istanza.
- Infine, prendi in considerazione la valutazione del rischio delle prestazioni fornita per ogni raccomandazione. Il rischio prestazionale indica l'impegno che potresti dover dedicare per verificare se il tipo di istanza consigliato soddisfa i requisiti prestazionali del tuo carico di lavoro. Ti suggeriamo, inoltre, di eseguire test rigorosi per il carico e le prestazioni prima e dopo aver apportato eventuali modifiche.

Modifiche del tipo di istanza Amazon EC2

Man mano che le tue esigenze cambiano, potresti scoprire che la tua istanza Amazon EC2 è troppo grande o troppo piccola per il suo carico di lavoro. In questo caso, è possibile ridimensionare l'istanza modificandone il tipo di istanza. Ad esempio, se la propria istanza `t2.micro` è troppo piccola per il suo carico di lavoro, è possibile aumentarne le dimensioni modificandola in un tipo di istanza T2 più grande, ad esempio una `t2.large`. In alternativa, è possibile cambiarla in un altro tipo di istanza, ad esempio una `m5.large`. Potrebbe inoltre essere necessario passare sda un tipo di istanza della generazione precedente a uno della generazione corrente per avvalersi di alcune caratteristiche, ad esempio il supporto per IPv6.

Se si desidera un suggerimento per un tipo di istanza che sia in grado di gestire al meglio il carico di lavoro esistente, è possibile utilizzare AWS Compute Optimizer. Per ulteriori informazioni, consulta Ottieni suggerimenti sulle istanze EC2 proposti da Compute Optimizer.

Se modifichi il tipo di istanza, inizierai a pagare la tariffa per il nuovo tipo di istanza. Per le tariffe on demand di tutti i tipi di istanze, consulta i prezzi di Amazon EC2. On-Demand

Per aggiungere ulteriore spazio di archiviazione all'istanza senza modificare il tipo di istanza, aggiungi un volume EBS a quest'ultima. Per ulteriori informazioni, consulta Attach an Amazon EBS volume to an instance nella Guida per l'utente di Amazon EBS.

Quali istruzioni seguire?

Esistono diverse istruzioni per modificare il tipo di istanza. Le istruzioni da usare dipendono dal volume root dell'istanza e dal fatto che il tipo di istanza sia compatibile con la configurazione corrente dell'istanza. Per informazioni su come viene determinata la compatibilità, consultare Compatibilità per la modifica del tipo di istanza.

Utilizzare la tabella seguente per determinare quali istruzioni seguire.

Volume root	Compatibilità	Seguire le seguenti istruzioni
EBS	Compatible	Cambiare il tipo di istanza
EBS	Non compatibile	Esecuzione della migrazione a un nuovo tipo di istanza
Instance store	Non applicabile	Esecuzione della migrazione a un nuovo tipo di istanza

Compatibilità per la modifica del tipo di istanza

È possibile modificare il tipo di un'istanza solo se la configurazione corrente dell'istanza è compatibile con il tipo di istanza desiderato. Se il tipo di istanza desiderato non è compatibile con la configurazione corrente dell'istanza, si dovrà avviare una nuova istanza con una configurazione compatibile con il tipo di istanza e migrare quindi l'applicazione alla nuova istanza.

La compatibilità è determinata nei seguenti modi:

Tipo di virtualizzazione

Le AMI Linux utilizzano uno dei due tipi di virtualizzazione disponibili: paravirtuale (PV) o macchina virtuale hardware (HVM). Non è possibile passare a un'istanza avviata da un'AMI PV

a un tipo di istanza solo HVM. Per ulteriori informazioni, consulta Tipi di virtualizzazione. Per verificare il tipo di virtualizzazione dell'istanza, si faccia riferimento al valore di Virtualizzazione nel riquadro dei dettagli della schermata Istanze nella console Amazon EC2.

Architecture

Le AMI sono specifiche per l'architettura del processore, per cui è necessario selezionare un tipo di istanza con la stessa architettura del processore del tipo di istanza corrente. Ad esempio:

- Se il tipo di istanza corrente ha un processore basato sull'architettura Arm, si è limitati ai tipi di istanze che supportano un processore basato sull'architettura Arm, ad esempio C6g e M6g.
- I seguenti tipi di istanza sono gli unici tipi di istanza che supportano le AMIs a 32-bit: `t2.nano`, `t2.micro`, `t2.small`, `t2.medium`, `c3.large`, `t1.micro`, `m1.small`, `m1.medium` e `c1.medium`. Se si stai modificando il tipo di istanza di un'istanza a 32 bit, si è limitati a questi tipi di istanza.

Schede di rete

Se si passa da un driver per una scheda di rete a un altro, le impostazioni della scheda di rete vengono reimpostate quando il sistema operativo crea la nuova scheda. Per riconfigurare le impostazioni, potrebbe essere necessario accedere a un account locale con autorizzazioni di amministratore. Di seguito sono riportati alcuni esempi di spostamento da una scheda di rete a un'altra:

- AWS Da PV (istanze T2) a Intel 82599 VF (istanze M4)
- Da Intel 82599 VF (la maggior parte delle istanze M4) a ENA (istanze M5)
- Da ENA (istanze M5) a ENA ad elevata larghezza di banda (istanze M5n)

Reti avanzate

I tipi di istanza che supportano la connettività di rete migliorata richiedono l'installazione dei driver necessari. Ad esempio, le Nitro-based istanze richiedono EBS-backed AMI con i driver Elastic Network Adapter (ENA) installati. Per passare da un tipo di istanza che non supporta la rete avanzata a un tipo che la supporta, è necessario installare i driver ENA o i driver ixgbevf sull'istanza, a seconda dei casi.

> **Note**
>
> Quando ridimensioni un'istanza con ENA Express abilitato, anche il nuovo tipo di istanza deve supportare ENA Express. Per un elenco dei tipi di istanza che supportano ENA Express, consulta la pagina Tipi di istanza supportati per ENA Express.

Per passare da un tipo di istanza che supporta ENA Express a un tipo di istanza che non lo supporta, assicurati che ENA Express non sia abilitato prima di ridimensionare l'istanza.

NVMe

I volumi EBS sono esposti come dispositivi a blocchi NVMe sulle istanze. Nitro-based Se si passa da un tipo di istanza che non supporta NVMe a un tipo di istanza che lo supporta, è necessario prima installare i driver NVMe sull'istanza. Inoltre, i nomi dei dispositivi specificati nella mappatura dei dispositivi a blocchi vengono sostituiti dai nomi dei dispositivi NVMe (`/dev/nvme[0-26]n1`).

[Istanze Linux] Pertanto, per montare i file system all'avvio utilizzando`/etc/fstab`, è necessario utilizzare UUID/Label al posto dei nomi dei dispositivi.

Limite di volumi

Il numero massimo di volumi Amazon EBS che puoi collegare a un'istanza dipende dal tipo e dalle dimensioni dell'istanza. Per ulteriori informazioni, consulta Limiti di volume di Amazon EBS per le istanze Amazon EC2.

È possibile passare solo a un'istanza di tipo e dimensione che supporti lo stesso numero o un numero maggiore di volumi rispetto a quello attualmente collegato all'istanza. Se si passa a un'istanza di tipo e dimensioni che non supporta il numero di volumi attualmente collegati, la richiesta ha esito negativo. Ad esempio, se passi da un'istanza `m7i.4xlarge` con 32 volumi allegati a un`m6i.4xlarge` che supporta massimo 27 volumi, la richiesta ha esito negativo.

NitroTPM

Se hai avviato l'istanza utilizzando un'AMI con NitroTPM abilitato e un tipo di istanza che supporta NitroTPM, l'istanza viene avviata con NitroTPM abilitato. Puoi passare solo a un tipo di istanza che supporti anche NitroTPM.

Modifica del tipo di istanza per l'istanza Amazon EC2

Usa le seguenti istruzioni per modificare il tipo di istanza di un' EBS-backed istanza Amazon se il tipo di istanza di cui hai bisogno è compatibile con la configurazione corrente della tua istanza. Per ulteriori informazioni, consulta the section called "Compatibilità".

Considerazioni

- Per poter modificare il tipo di un'istanza, devi arrestarla. Assicurati di prevedere i tempi di inattività durante l'arresto dell'istanza. L'arresto dell'istanza e il cambio del suo tipo di istanza potrebbero richiedere alcuni minuti, mentre il riavvio può richiedere un intervallo variabile di tempo, a seconda degli script di startup dell'applicazione. Per ulteriori informazioni, consulta Avvio e arresto di un'istanza Amazon EC2.
- Quando si interrompe e si avvia un'istanza, spostiamo l'istanza su un nuovo hardware. Se l'istanza ha un indirizzo IPv4 pubblico, che non è un IP elastico, l'indirizzo viene rilasciato e viene assegnato un nuovo indirizzo IPv4 pubblico. Per ulteriori informazioni sul comportamento degli indirizzi IP durante l'intero ciclo di vita di un'istanza, consulta Differenze tra gli stati dell'istanza.
- Non puoi modificare il tipo di istanza di un'istanza spot.
- [Istanze Windows] Ti consigliamo di aggiornare il pacchetto driver AWS PV prima di modificare il tipo di istanza. Per ulteriori informazioni, consulta the section called “Aggiornamento dei driver PV”.
- Se l'istanza è inclusa in un gruppo Auto Scaling, il servizio Amazon EC2 Auto Scaling contrassegna l'istanza interrotta come non integra e pertanto può arrestarla e avviarne una sostitutiva. Per evitare questa situazione, si può sospendere il processo di dimensionamento per il gruppo mentre si cambia il tipo di istanza. Per ulteriori informazioni, consulta Sospensione e ripresa di un processo per un gruppo Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.
- Quando modifichi il tipo di istanza di un'istanza con volumi dell'archivio istanza NVMe, l'istanza aggiornata potrebbe presentare volumi dell'archivio istanza aggiuntivi, in quanto tutti i volumi dell'archivio istanza NVMe sono disponibili, anche se non sono specificati nella mappatura dei dispositivi a blocchi dell'AMI o delle istanze. Altrimenti, l'istanza aggiornata ha lo stesso numero di volumi dell'archivio istanza specificato quando hai avviato l'istanza originale.
- Il numero massimo di volumi Amazon EBS che puoi collegare a un'istanza dipende dal tipo e dalle dimensioni dell'istanza. Non puoi passare a un'istanza di tipo e dimensione che non supporti il numero di volumi già collegati all'istanza. Per ulteriori informazioni, consulta Limiti di volume di Amazon EBS per le istanze Amazon EC2.
- [Istanze Linux] Puoi utilizzare il runbook `AWSSupport-MigrateXenToNitroLinux` per migrare istanze Linux compatibili da un tipo di istanza Xen a un tipo di istanza Nitro. Per ulteriori informazioni, consulta AWSSupport-MigrateXenToNitroLinux runbook nella Documentazione di riferimento del runbook di Automazione AWS Systems Manager .
- [Istanze Windows] Per ulteriori indicazioni sulla migrazione delle istanze Windows compatibili da un tipo di istanza Xen a un tipo di istanza Nitro, consulta Migrate to latest generation instance types.

Per modificare il tipo di istanza di un'istanza Amazon EBS-backed

1. (Facoltativo) Se il nuovo tipo di istanza richiede driver che non sono installati sull'istanza esistente, devi prima connetterti all'istanza e installare i driver. Per ulteriori informazioni, consulta Compatibilità per la modifica del tipo di istanza.
2. [Istanze Windows] Se hai configurato l'istanza Windows per l'uso di indirizzi IP statici e si passa da un tipo di istanza che non supporta le reti avanzate a un tipo di istanza che invece le supporta, potresti visualizzare un avviso relativo a un potenziale conflitto di indirizzi IP durante la riconfigurazione degli indirizzi IP statici. Per evitare questo problema, abilita il protocollo DHCP sull'interfaccia di rete per l'istanza in uso prima di modificare il tipo di istanza. Dalla tua istanza, apri il Network and Sharing Center, apri le proprietà del protocollo Internet versione 4 (TCP/IPv4) per l'interfaccia di rete e scegli Ottieni automaticamente un indirizzo IP. Modifica il tipo di istanza e riconfigura l'indirizzo IP statico sull'interfaccia di rete.
3. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
4. Nel riquadro di navigazione, scegliere Instances (Istanze).
5. Seleziona l'istanza e scegli Instance state (Stato istanza), Stop instance (Arresta istanza). Quando viene richiesta la conferma, selezionare Stop (Arresta). Possono essere necessari alcuni minuti per arrestare l'istanza.
6. Con l'istanza ancora selezionata, scegliere Actions (Operazioni), Instance settings (Impostazioni istanza), Change instance type (Cambia tipo di istanza). Questa opzione è disabilitata se lo stato dell'istanza non è `stopped`.
7. Per Change Instance Type (Cambia tipo di istanza), effettuare le seguenti operazioni:

   a. In Tipo di istanza, selezionare il tipo di istanza desiderato.

      Se il tipo di istanza non è nell'elenco, non è compatibile con la configurazione dell'istanza. Utilizzare invece le seguenti istruzioni: Migrazione a un nuovo tipo di istanza avviando una nuova istanza EC2.

   b. (Facoltativo) Se il tipo di istanza selezionato supporta l'ottimizzazione EBS, seleziona EBS-optimized per abilitare l'ottimizzazione EBS o deseleziona EBS-optimized per disabilitare l'ottimizzazione EBS.

      Se il tipo di istanza selezionato è ottimizzato per EBS per impostazione predefinita, EBS-optimized è selezionato e non è possibile deselezionarlo.

   c. (Facoltativo) Configura le opzioni vCPU sul nuovo tipo di istanza.

Quando modifichi il tipo di un'istanza esistente, Amazon EC2 applica le impostazioni di opzioni CPU dall'istanza esistente a quella nuova, se possibile. Se il nuovo tipo di istanza non supporta tali impostazioni, le opzioni CPU vengono ripristinate a Nessuna. Questa opzione utilizza il numero predefinito di vCPU per il nuovo tipo di istanza.

Se il tipo di istanza selezionato supporta la configurazione vCPU, seleziona Specifica le opzioni CPU nel pannello Dettagli avanzati per configurare le vCPU per il nuovo tipo di istanza.

d. Scegli Applica per accettare le nuove impostazioni.

8. Per avviare l'istanza, selezionare l'istanza e scegli Stato istanza, Avvia istanza. Possono essere necessari alcuni minuti affinché l'istanza entri nello stato `running`. Se l'istanza non si avvia, consulta Risoluzione dei problemi relativi alla modifica del tipo di istanza.
9. [Istanze Windows] Se l'istanza esegue Windows Server 2016 o Windows Server 2019 con EC2Launch v1, connettiti all'istanza di Windows ed esegui il seguente PowerShell script EC2Launch per configurare l'istanza dopo la modifica del tipo di istanza.

> **Important**
>
> La password amministratore verrà reimpostata quando abiliti lo script EC2 Launch dell'istanza di inizializzazione. Puoi modificare il file di configurazione per disattivare la reimpostazione della password amministratore specificandolo nelle impostazioni delle attività di inizializzazione. Per istruzioni su come disabilitare la reimpostazione della password, consulta Configure initialization tasks (EC2Launch) o Change settings (EC2Launch v2).

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Migrazione a un nuovo tipo di istanza avviando una nuova istanza EC2

È possibile modificare il tipo di istanza di un'istanza EC2 solo se si tratta di un' EBS-backed istanza con una configurazione compatibile con il nuovo tipo di istanza desiderato. Altrimenti, se la configurazione o l'istanza non è compatibile con il nuovo tipo di istanza o si tratta di un'istanza basata sull'archivio dell'istanza, dovrai avviare un'istanza sostitutiva compatibile con il tipo desiderato. Per

informazioni su come viene determinata la compatibilità, consulta Compatibilità per la modifica del tipo di istanza.

Panoramica del processo di migrazione

- Esegui il backup dei dati sull'istanza originale.
- Avvia una nuova istanza con una configurazione compatibile con il nuovo tipo di istanza desiderato, collegando tutti i volumi EBS che erano collegati all'istanza originale.
- Installa la tua applicazione sulla nuova istanza.
- Ripristinare tutti i dati.
- Se l'istanza originale ha un indirizzo IP elastico devi associare l'indirizzo IP elastico alla nuova istanza per assicurarti che gli utenti possano continuare a utilizzare le applicazioni senza interruzioni.

Esecuzione della migrazione di un'istanza verso una nuova istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Esegui il backup dei dati di cui hai bisogno come riportato di seguito:
   - Collegati all'istanza e copia i dati dei volumi dell'archivio dell'istanza in un'archiviazione persistente.
   - Crea uno snapshot dei volumi EBS per produrre nuovi volumi con gli stessi dati o scollega i volumi dall'istanza originale in modo da poterli collegare alla nuova.
3. Nel riquadro di navigazione, scegliere Instances (Istanze).
4. Scegliere Launch Instances (Avvia istanze). Quando si configura l'istanza, effettuare le seguenti operazioni:
   a. Seleziona un'AMI che supporta il tipo di istanza desiderato. Ad esempio, puoi selezionare un'AMI che supporta il tipo di processore del nuovo tipo di istanza. Inoltre, i tipi di istanza della generazione corrente richiedono un'AMI HVM.
   b. Selezionare il nuovo tipo di istanza. Se il tipo di istanza desiderato non è disponibile, significa che non è compatibile con la configurazione dell'AMI selezionata.
   c. Se desideri consentire allo stesso traffico di raggiungere la nuova istanza, seleziona il VPC e il gruppo di sicurezza utilizzati nell'istanza originale.

d. Al termine della configurazione della nuova istanza, completare i passaggi per selezionare una coppia di chiavi e avviare l'istanza. Possono essere necessari alcuni minuti affinché l'istanza entri nello stato `running`.

5. Se hai eseguito il backup dei dati su uno snapshot EBS, crea un volume dallo snapshot e collega il volume alla nuova istanza.

   Per spostare un volume EBS dall'istanza originale alla nuova, scollega il volume dall'istanza originale e collegalo alla nuova.

6. Installare l'applicazione e tutto il software richiesto sulla nuova istanza.
7. Ripristina i dati di cui è stato creato il backup dai volumi di instance store dell'istanza originale.
8. Se l'istanza originale dispone di un indirizzo IP elastico, assegnalo alla nuova istanza nel seguente modo:

   a. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).

   b. Seleziona l'indirizzo IP elastico associato all'istanza originale e scegli Actions (Operazioni), Disassociate Elastic IP address (Dissocia indirizzo IP elastico). Quando viene richiesta la conferma, seleziona Disassociate (Dissocia).

   c. Con l'indirizzo IP elastico ancora selezionato, scegli Actions (Operazioni), quindi seleziona Associate Elastic IP address (Associa indirizzo IP elastico).

   d. Per Resource type (Tipo di risorsa), scegliere Instance (Istanza).

   e. In Istanza, scegli la nuova istanza.

   f. (Facoltativo) Per Private IP address (Indirizzo IP privato), specificare un indirizzo IP privato a cui associare l'indirizzo IP elastico.

   g. Seleziona Associate (Associa).

9. (Facoltativo) È possibile terminare l'istanza originale se non è più necessaria. Selezionare l'istanza e verificare che si stia terminando l'istanza originale e non la nuova istanza, ad esempio controllando il nome o l'ora di avvio, quindi scegliere Stato istanza, Termina istanza.

Risoluzione dei problemi relativi alla modifica del tipo di istanza

Utilizzare le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante il cambio del tipo di istanza.

L'istanza non viene avviata dopo aver modificato il tipo di istanza

Possibile causa: requisiti per il nuovo tipo di istanza non soddisfatti

Se l'istanza non viene avviata, è possibile che uno dei requisiti per il nuovo tipo di istanza non sia stato soddisfatto. Per ulteriori informazioni, consulta Perché la mia istanza Linux non si avvia dopo che ne ho modificato il tipo?

Possibile causa: l'AMI non supporta il tipo di istanza

Se si utilizza la console EC2 per modificare il tipo di istanza, sono disponibili solo i tipi di istanza supportati dall'AMI selezionata. Tuttavia, se si utilizza il AWS CLI per avviare un'istanza, è possibile specificare un'AMI e un tipo di istanza incompatibili. Se l'AMI e il tipo di istanza sono incompatibili, l'istanza non può essere avviata. Per ulteriori informazioni, consulta Compatibilità per la modifica del tipo di istanza.

Possibile causa: l'istanza si trova nel gruppo di collocazione cluster

Se la propria istanza si trova in un gruppo di collocazione cluster e, dopo aver modificato il tipo di istanza, l'istanza non viene avviata, provare quanto segue:

1. Arrestare tutte le istanze nel gruppo di collocazione cluster.
2. Cambiare il tipo di istanza dell'istanza interessata.
3. Avviare tutte le istanze nel gruppo di collocazione cluster.

Applicazione o sito Web non raggiungibile da Internet dopo aver modificato il tipo di istanza

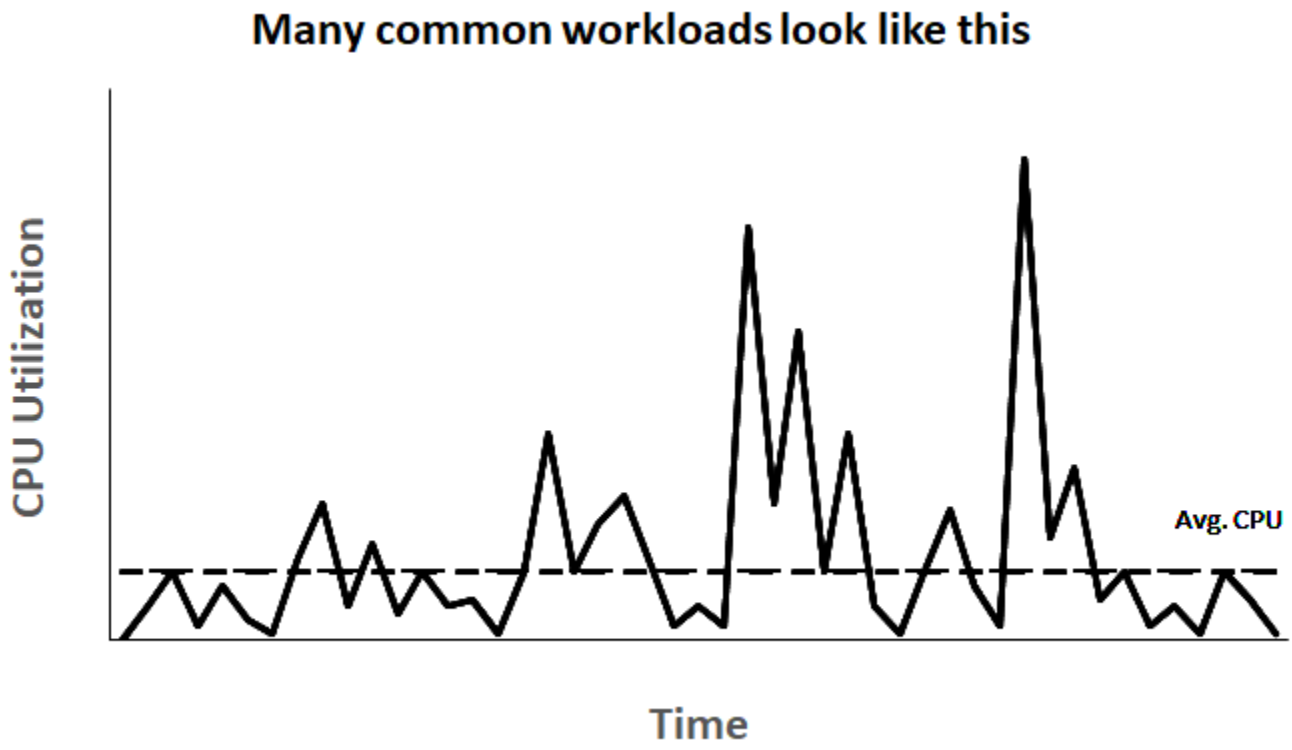
Possibile causa: viene rilasciato un indirizzo IPv4 pubblico

Quando si modifica il tipo di istanza, è prima necessario arrestare l'istanza. Quando si arresta un'istanza, viene rilasciato l'indirizzo IPv4 pubblico e ne viene assegnato uno nuovo.

Per mantenere l'indirizzo IPv4 pubblico tra gli arresti e gli avvii dell'istanza, ti consigliamo di utilizzare un indirizzo IP elastico. Per ulteriori informazioni, consulta Indirizzi IP elastici.

Istanze a prestazioni espandibili

Molti carichi di lavoro generici non sono in media occupati e non richiedono un elevato livello di prestazioni della CPU sostenute. Il grafico seguente illustra l'utilizzo della CPU per molti carichi di lavoro comuni che i clienti eseguono oggi nel cloud. AWS



Questi carichi di lavoro di utilizzo della CPU da basso a moderato comportano uno spreco di cicli della CPU e, di conseguenza, si paga più di quanto si utilizza. Per superare questo problema, è possibile sfruttare le istanze generiche a basso costo espandibili, che sono le istanze T.

La famiglia di istanze T fornisce prestazioni CPU base con la possibilità di superare la baseline in qualsiasi momento per tutto il tempo necessario. La CPU di base è definita per soddisfare le esigenze della maggior parte dei carichi di lavoro generici, inclusi microservizi su larga scala, server Web, database di piccole e medie dimensioni, registrazione dei dati, repository di codice, desktop virtuali, ambienti di sviluppo e test e applicazioni business-critical. Le istanze T offrono un equilibrio tra risorse di elaborazione, memoria e rete e offrono il modo più conveniente per eseguire un'ampia gamma di applicazioni generiche con un utilizzo della CPU da basso a moderato. Possono risparmiare fino al 15% in termini di costi rispetto alle istanze M e portare a risparmi ancora maggiori sui costi con dimensioni di istanza più piccole ed economiche, offrendo fino a 2 vCPU e 0,5 GiB di memoria. Le dimensioni delle istanze T più piccole, come nano, micro, small e medium, sono adatte per carichi di lavoro che richiedono una piccola quantità di memoria e non prevedono un utilizzo elevato della CPU.

> **Note**
>
> In questo argomento sono descritte le CPU espandibili. Per informazioni sulle prestazioni delle reti espandibili, consulta Larghezza di banda di rete dell'istanza Amazon EC2.

Tipi di istanze espandibili EC2

Le istanze EC2 espandibili sono costituite da tipi di istanze T4g, T3a e T3 e i tipi di istanza T2 della generazione precedente.

I tipi di istanza T4g sono l'ultima generazione di istanze espandibili. Offrono il miglior prezzo per le prestazioni e offrono il costo più basso di tutti i tipi di istanza EC2. I tipi di istanze T4g sono alimentati da processori Arm-based AWS Graviton2 con un ampio supporto ecosistemico da parte di fornitori di sistemi operativi, fornitori di software indipendenti e servizi e applicazioni popolari. AWS

Nella tabella seguente vengono riepilogate le principali differenze tra i tipi di istanza espandibili.

Tipo	Descrizione	Famiglia di processori
Generazione più recente		
T4g	Il tipo di istanza EC2 dal costo più basso, con costi fino al 40% superiori e inferiori del 20% rispetto a T3 price/per formance	AWS Processori Graviton2 con core Arm Neoverse N1
T3a	Istanze basate su x86 a basso costo con costi inferiori del 10% rispetto alle istanze T3	Processori EPYC di prima generazione AMD
T3	Miglior picco price/per formance per i carichi di lavoro x86 con una riduzione fino al 30% rispetto alle istanze T2 della generazione precedente price/performance	Intel Xeon scalabile (processo ri Skylake, Cascade Lake)

Tipo	Descrizione	Famiglia di processori
Generazione precedente		
T2	Istanze espandibili di generazioni precedenti	Processori Intel Xeon

Per ulteriori informazioni sui prezzi delle istanze e per specifiche aggiuntive, consulta Amazon EC2 Pricing (Prezzi di Amazon EC2) e Amazon EC2 Instance Types (Tipi di istanza Amazon EC2). Per informazioni sulle prestazioni delle reti espandibili, consulta Larghezza di banda di rete dell'istanza Amazon EC2.

Se l'hai creata Account AWS prima del 15 luglio 2025 e ha meno di 12 mesi, puoi utilizzare un'`t2.micro`istanza gratuitamente (o un'`t3.micro`istanza nelle regioni in cui non `t2.micro` è disponibile) entro determinati limiti di utilizzo. Se hai creato la tua Account AWS istanza il 15 luglio 2025 o dopo tale data, puoi utilizzare `t3.micro` i tipi di `t4g.small` istanza `t3.small``t4g.micro`,, per 6 mesi o fino a esaurimento dei crediti. Per ulteriori informazioni, consulta Piano gratuito di AWS.

Opzioni di acquisto supportate per istanze T

- On-Demand Istanze
- Istanze riservate
- Istanze dedicate (solo T3)
- Host dedicati (solo T3, esclusivamente in modalità `standard`)
- Spot Instances

Per ulteriori informazioni, consulta Opzioni di fatturazione e acquisto di Amazon EC2.

Indice

- Best practice
- Concetti chiave per istanze a prestazioni espandibili
- Modalità illimitata per istanze a prestazioni espandibili
- Modalità standard per istanze a prestazioni espandibili
- Configurazione delle istanze a prestazioni espandibili
- Monitoraggio dei crediti CPU per istanze espandibili

Best practice

Queste best practice consentono di sfruttare al meglio i vantaggi delle istanze a prestazioni espandibili.

- Assicurarsi che le dimensioni dell'istanza scelte rispettino i requisiti minimi di memoria del sistema operativo e delle applicazioni. I sistemi operativi con interfacce utente grafiche che consumano notevoli quantità di risorse di memoria e CPU (ad esempio, Windows) potrebbero richiedere una dimensione dell'istanza `t3.micro` o più grande per molti casi d'uso. Man mano che i requisiti di memoria e CPU del carico di lavoro aumentano nel tempo, con le istanze T è possibile passare a dimensioni maggiori dello stesso tipo di istanza o selezionare un altro tipo di istanza.
- Abilita AWS Compute Optimizer per il tuo account ed esamina i suggerimenti di Compute Optimizer per il tuo carico di lavoro. Compute Optimizer può aiutare a valutare se le istanze devono essere aumentate per migliorare le prestazioni o ridimensionate per risparmiare sui costi. L'ottimizzatore di calcolo può anche consigliare un tipo di istanza diverso in base allo scenario. Per ulteriori informazioni, consulta Visualizzazione dei suggerimenti sulle istanze EC2 nella sezione Guida per l'utente di AWS Compute Optimizer .

Concetti chiave per istanze a prestazioni espandibili

I tradizionali tipi di istanze Amazon EC2 forniscono risorse CPU fisse, mentre le istanze espandibili forniscono un livello di baseline di utilizzo della CPU con la possibilità di aumentare l'utilizzo della CPU al di sopra della baseline. In questo modo si garantisce il pagamento solo per la CPU della baseline e per qualsiasi utilizzo aggiuntivo della CPU con conseguente riduzione dei costi di calcolo. Le prestazioni di base e la capacità di espansione sono governate dai crediti CPU. Le istanze a prestazioni espandibili sono gli unici tipi di istanza che utilizzano i crediti per l'utilizzo della CPU.

Ogni istanza espandibile guadagna continuamente credito quando rimane al di sotto della baseline della CPU e spende crediti quando sfora al di sopra della baseline. La quantità di crediti guadagnati o spesi dipende dall'utilizzo della CPU dell'istanza:

- Se l'utilizzo della CPU è inferiore alla baseline, i crediti guadagnati sono superiori ai crediti spesi.
- Se l'utilizzo della CPU è uguale alla baseline, i crediti guadagnati sono uguali ai crediti spesi.
- Se l'utilizzo della CPU è superiore alla baseline, i crediti spesi sono superiori ai crediti guadagnati.

Quando i crediti guadagnati sono superiori ai crediti spesi, la differenza viene chiamata crediti accumulati, crediti che possono essere utilizzati in seguito per andare oltre l'utilizzo della CPU di

base. Allo stesso modo, quando i crediti spesi sono superiori ai crediti guadagnati, il comportamento dell'istanza dipende dalla modalità di configurazione del credito: modalità Standard o modalità Illimitato.

In modalità Standard, quando i crediti spesi sono superiori ai crediti guadagnati, l'istanza utilizza i crediti accumulati per andare oltre l'utilizzo della CPU di base. Se non ci sono crediti accumulati rimanenti, l'istanza si riduce gradualmente all'utilizzo della CPU baseline e non può superare la baseline fino a quando non accumula altri crediti.

In modalità illimitata, se l'istanza supera l'utilizzo della CPU di base, l'istanza utilizza prima i crediti accumulati. Se non ci sono crediti accumulati rimanenti, l'istanza spende i crediti eccedenti. Quando l'utilizzo della CPU è inferiore alla baseline, utilizza i crediti CPU che guadagna per pagare i crediti extra spesi in precedenza. La possibilità di guadagnare crediti CPU per pagare i crediti extra consente ad Amazon EC2 di calcolare una media dell'utilizzo della CPU di un'istanza in un periodo di 24 ore. Se l'utilizzo medio della CPU in un periodo di 24 ore supera il valore di base, all'istanza viene fatturato l'utilizzo aggiuntivo a una tariffa aggiuntiva fissa (tariffa aggiuntiva CPU-hour

Indice

- Concetti e definizioni chiave
- Guadagno di crediti CPU
- Tasso di guadagno di crediti CPU
- Limite di accumulo di crediti CPU
- Durata dei crediti CPU accumulati
- Utilizzo di base

Concetti e definizioni chiave

I seguenti concetti e definizioni chiave sono applicabili alle istanze espandibili.

Utilizzo CPU

> L'utilizzo della CPU è la percentuale delle unità di elaborazione EC2 assegnate attualmente in uso nell'istanza. Questa metrica misura la percentuale di cicli di CPU allocati utilizzati su un'istanza. La CloudWatch metrica sull'utilizzo della CPU mostra l'utilizzo della CPU per istanza e non l'utilizzo della CPU per core. La specifica della CPU di base di un'istanza si basa anche sull'utilizzo della CPU per istanza. Per misurare l'utilizzo della CPU utilizzando Console di gestione AWS o the AWS CLI, vedere. Ottenere le statistiche su un'istanza specifica

Credito CPU

Un'unità di vCPU-time.

Esempi:

1 credito CPU = 1 vCPU * 100% di utilizzo * 1 minuto.

1 credito CPU = 1 vCPU * 50% di utilizzo * 2 minuti.

1 credito CPU = 2 vCPU * 25% di utilizzo * 2 minuti.

Utilizzo di base

L'utilizzo di base è il livello al quale la CPU può essere utilizzata per un saldo netto pari a zero, quando il numero di crediti CPU guadagnati corrisponde al numero di crediti CPU utilizzati. L'utilizzo di base è noto anche come linea di base. L'utilizzo di base è espresso come percentuale di utilizzo della vCPU, calcolata come segue: Utilizzo basale% = (numero di crediti di vCPU) /60 minuti. earned/number

Per l'utilizzo della base di confronto di ogni tipo di istanza a prestazioni espandibili, consulta la tabella del credito.

Crediti guadagnati

I crediti guadagnati continuamente da un'istanza quando è in esecuzione.

Numero di crediti guadagnati per ora = % utilizzo di base * numero di vCPU * 60 minuti

Esempio:

Un t3.nano con 2 vCPU e un utilizzo di base del 5% guadagna 6 crediti all'ora, calcolati come segue:

2 vCPU * 5% di base * 60 minuti = 6 crediti all'ora

Crediti spesi o usati

I crediti utilizzati continuamente da un'istanza quando è in esecuzione.

I crediti CPU spesi al minuto = Numero di vCPU * Utilizzo della CPU * 1 minuto

Crediti accumulati

I crediti CPU non spesi quando un'istanza utilizza un numero di crediti inferiore a quello richiesto per l'utilizzo di base. In altre parole, crediti maturati = (Crediti guadagnati - Crediti usati) sotto la linea di base.

Esempio:

Se un t3.nano è in esecuzione al 2% di utilizzo della CPU, che è al di sotto della sua linea di base del 5% per un'ora, i crediti accumulati vengono calcolati come segue:

Crediti CPU accumulati = (Crediti guadagnati all'ora - Crediti usati all'ora) = 6 - 2 vCPU * 2% utilizzo CPU * 60 minuti = 6 - 2,4 = 3,6 crediti accumulati all'ora

Limite di accumulo di crediti

Dipende dalla dimensione dell'istanza, ma in generale è uguale al numero massimo di crediti guadagnati in 24 ore.

Esempio:

Per t3.nano, il limite di accumulo del credito = 24 * 6 = 144 crediti

Crediti di lancio

Applicabile solo per le istanze T2 configurate per la modalità Standard. I crediti di avvio sono un numero limitato di crediti CPU che vengono allocati a una nuova istanza T2 in modo che, quando viene avviata in modalità Standard, possa superare la linea di base.

Crediti in eccedenza

I crediti che vengono spesi da un'istanza dopo che ha esaurito il suo saldo di credito accumulato. I crediti in eccedenza sono progettati per le istanze espandibili per sostenere prestazioni elevate per un periodo di tempo prolungato e sono utilizzati solo in modalità Illimitato. Il saldo dei crediti in eccedenza viene utilizzato per determinare quanti crediti sono stati utilizzati dall'istanza per l'espansione in modalità Illimitato.

Modalità Standard

Modalità di configurazione del credito, che consente a un'istanza di superare la linea di base spendendo i crediti accumulati nel suo saldo.

Modalità illimitata

Modalità di configurazione del credito, che consente a un'istanza di superare la baseline sostenendo un utilizzo elevato della CPU per tutto il tempo necessario per qualsiasi periodo di tempo. Il prezzo orario copre automaticamente tutti i picchi di utilizzo della CPU se l'utilizzo medio della CPU dell'istanza corrisponde o è inferiore alla baseline per un periodo di 24 ore o la durata dell'istanza, a seconda di quale dei due è inferiore. Se l'istanza viene eseguita con un utilizzo della

CPU più elevato per un periodo prolungato, può farlo con una tariffa aggiuntiva fissa, una tariffa aggiuntiva fissa, una tariffa aggiuntiva fissa per v. CPU-hour

Nella tabella seguente vengono riepilogate le principali differenze di credito tra i tipi di istanza espandibili.

Tipo	Tipo di crediti CPU supportato	Modalità di configura zione crediti	Durata dei crediti CPU accumulati tra l'avvio e l'arresto dell'istanza
Generazione più recente			
T4g	Crediti guadagnati, Crediti accumulati, Crediti spesi, Crediti in eccedenza (solo modalità Illimitato)	Standard, Illimitato (predefinito)	7 giorni (i crediti persistono per 7 giorni dopo l'interruzione di un'istanza)
T3a	Crediti guadagnati, Crediti accumulati, Crediti spesi, Crediti in eccedenza (solo modalità Illimitato)	Standard, Illimitato (predefinito)	7 giorni (i crediti persistono per 7 giorni dopo l'interruzione di un'istanza)
T3	Crediti guadagnati, Crediti accumulati, Crediti spesi, Crediti in eccedenza (solo modalità Illimitato)	Standard, Illimitato (predefinito)	7 giorni (i crediti persistono per 7 giorni dopo l'interruzione di un'istanza)
Generazione precedente			
T2	Crediti guadagnati, Crediti accumulati, Crediti spesi, Crediti di avvio (solo modalità Standard), Crediti	Standard (predefinito), Illimitato	0 giorni (i crediti vengono persi quando un'istanza viene interrotta)

Tipo	Tipo di crediti CPU supportato	Modalità di configurazione crediti	Durata dei crediti CPU accumulati tra l'avvio e l'arresto dell'istanza
	in eccedenza (solo modalità Illimitato)		

> **Note**
>
> La modalità illimitata non è supportata per le istanze T3 avviate su un host dedicato.

Guadagno di crediti CPU

Ogni istanza a prestazioni espandibili guadagna continuamente (a una risoluzione a livello di millisecondo) un tasso fisso di crediti CPU all'ora, a seconda delle dimensioni dell'istanza. Il processo contabile per l'accumulo o la spesa dei crediti avviene anche a una risoluzione a livello di millisecondo, quindi non devi preoccuparti di spendere troppo i crediti CPU; una breve ottimizzazione della CPU utilizza una piccola frazione del credito CPU.

Se un'istanza a prestazioni espandibili utilizza una quantità inferiore di risorse CPU rispetto a quella necessaria per l'utilizzo di base (ad esempio quando è inattiva), i crediti CPU non spesi vengono accumulati nel saldo del credito CPU. Se un'istanza a prestazioni espandibili deve superare il livello di utilizzo di base, spende i crediti accumulati. Maggiore è il numero di crediti accumulato da un'istanza a prestazioni espandibili, maggiore è il tempo in cui può far aumentare le prestazioni al di là della sua baseline quando è necessario un utilizzo maggiore della CPU.

La seguente tabella elenca i tipi di istanze a prestazioni espandibili, la frequenza a cui i crediti CPU vengono guadagnati all'ora, il numero massimo di crediti CPU guadagnati che un'istanza può accumulare, il numero di vCPU per istanza e il livello di utilizzo di base come percentuale di un full core (utilizzando una singola vCPU).

Tipo di istanza	Crediti CPU guadagnati all'ora	Quantità massima di crediti guadagnati che può essere accumulata*	vCPU***	Utilizzo di base per vCPU
T2				
t2.nano	3	72	1	5%
t2.micro	6	144	1	10%
t2.small	12	288	1	20%
t2.medium	24	576	2	20%**
t2.large	36	864	2	30%**
t2.xlarge	54	1296	4	22,5%**
t2.2xlarge	81,6	1958,4	8	17%**
T3				
t3.nano	6	144	2	5%**
t3.micro	12	288	2	10%**
t3.small	24	576	2	20%**
t3.medium	24	576	2	20%**
t3.large	36	864	2	30%**
t3.xlarge	96	2304	4	40%**
t3.2xlarge	192	4608	8	40%**
T3a				
t3a.nano	6	144	2	5%**

Tipo di istanza	Crediti CPU guadagnati all'ora	Quantità massima di crediti guadagnati che può essere accumulata*	vCPU***	Utilizzo di base per vCPU
t3a.micro	12	288	2	10%**
t3a.small	24	576	2	20%**
t3a.medium	24	576	2	20%**
t3a.large	36	864	2	30%**
t3a.xlarge	96	2304	4	40%**
t3a.2xlarge	192	4608	8	40%**
T4g				
t4g.nano	6	144	2	5%**
t4g.micro	12	288	2	10%**
t4g.small	24	576	2	20%**
t4g.medium	24	576	2	20%**
t4g.large	36	864	2	30%**
t4g.xlarge	96	2304	4	40%**
t4g.2xlarge	192	4608	8	40%**

Note

* Il numero di crediti che possono essere accumulati è equivalente al numero di crediti che possono essere guadagnati in un periodo di 24 ore.

Note

** La percentuale di utilizzo di base nella tabella è per vCPU. In CloudWatch, l'utilizzo della CPU viene mostrato per vCPU. Ad esempio, l'utilizzo della CPU per un'`t3.large`istanza che opera al livello di base è indicato come 30% nelle CloudWatch metriche della CPU. Per informazioni su come calcolare l'utilizzo di base, consulta Utilizzo di base.

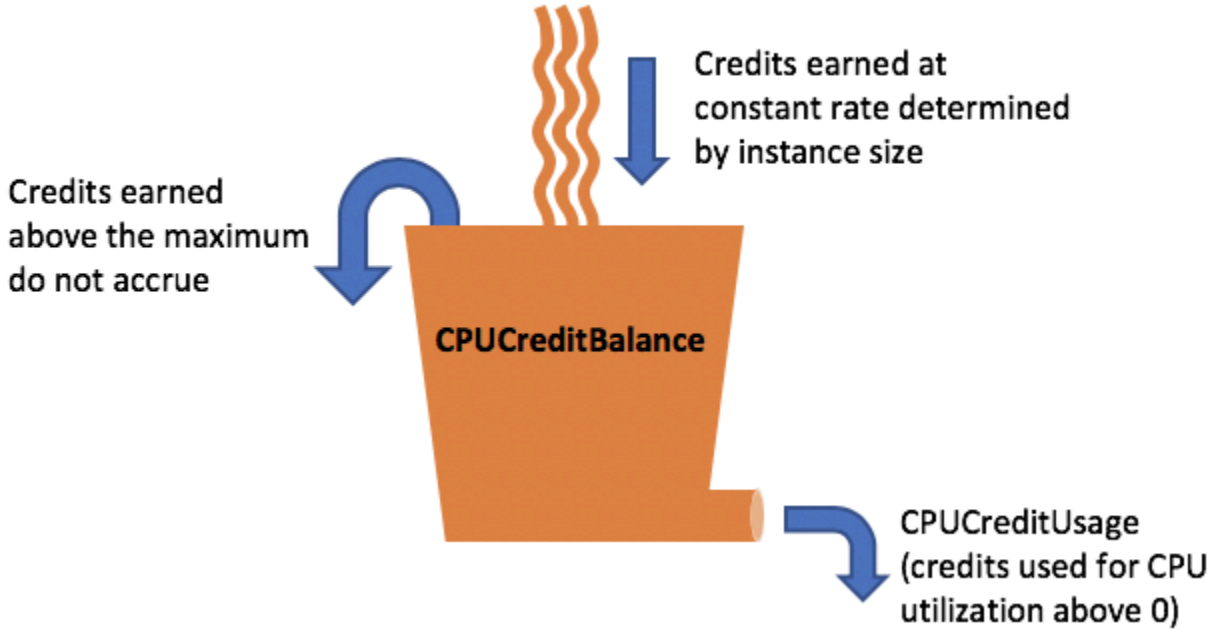
*** Ogni vCPU è un thread di un core Intel Xeon o un core AMD EPYC, ad eccezione delle istanze T2 e T4g.

Tasso di guadagno di crediti CPU

Il numero di crediti CPU guadagnati all'ora è determinato dalle dimensioni dell'istanza. Ad esempio, un'istanza `t3.nano` guadagna sei crediti all'ora, mentre una `t3.small` guadagna 24 crediti all'ora. La tabella precedente elenca il tasso di guadagno di crediti per tutte le istanze.

Limite di accumulo di crediti CPU

Sebbene i crediti guadagnati non scadano mai su un'istanza in esecuzione, esiste un limite al numero di crediti guadagnati che un'istanza può accumulare. Il limite è determinato dal limite del saldo del credito CPU. Una volta raggiunto il limite, tutti i nuovi crediti guadagnati vengono scartati, come indicato nell'immagine seguente. Il bucket pieno indica il limite di saldo del credito CPU e lo spillover indica i crediti appena guadagnati che superano il limite.



Il limite di saldo del credito CPU è diverso per ciascuna dimensione dell'istanza Ad esempio, un'istanza `t3.micro` può accumulare un massimo di 288 crediti CPU guadagnati nel saldo del credito CPU. La tabella precedente elenca il numero massimo di crediti guadagnati che ciascuna istanza di può accumulare.

Anche le istanze T2 Standard guadagnano crediti di lancio. I crediti di lancio non contano per il limite del saldo del credito CPU. Se un'istanza T2 non ha speso i suoi crediti di avvio e rimane inattiva per un periodo di 24 ore mentre accumula crediti guadagnati, il suo saldo del credito CPU appare oltre il limite. Per ulteriori informazioni, consulta Crediti di lancio.

Le istanze T4g, T3a e T3 non guadagnano crediti di avvio. Queste istanze vengono avviate come `unlimited` per impostazione predefinita, pertanto possono espandersi immediatamente all'avvio senza crediti di lancio. Le istanze T3 vengono avviate su host dedicato in modalità `standard` per impostazione predefinita; la modalità `unlimited` non è supportata per le istanze T3 su un host dedicato.

Durata dei crediti CPU accumulati

I crediti CPU su un'istanza in esecuzione non scadono.

Per T2, il saldo del credito CPU non persiste tra le interruzioni e gli avvii dell'istanza. Se interrompi un'istanza T2, l'istanza perde tutti i crediti accumulati.

Per T4g, T3a e T3, il saldo di crediti CPU viene conservato per sette giorni dopo l'arresto di un'istanza, trascorsi i quali i crediti vengono persi. Se avvii l'istanza entro sette giorni, non viene perso alcun credito.

Per ulteriori informazioni, consulta `CPUCreditBalance` nella tabella dei parametri CloudWatch .

Utilizzo di base

L'utilizzo di base è il livello al quale la CPU può essere utilizzata per un saldo netto pari a zero, quando il numero di crediti CPU guadagnati corrisponde al numero di crediti CPU utilizzati. L'utilizzo di base è noto anche come linea di base.

L'utilizzo di base è espresso come percentuale di utilizzo della vCPU, calcolata come segue:

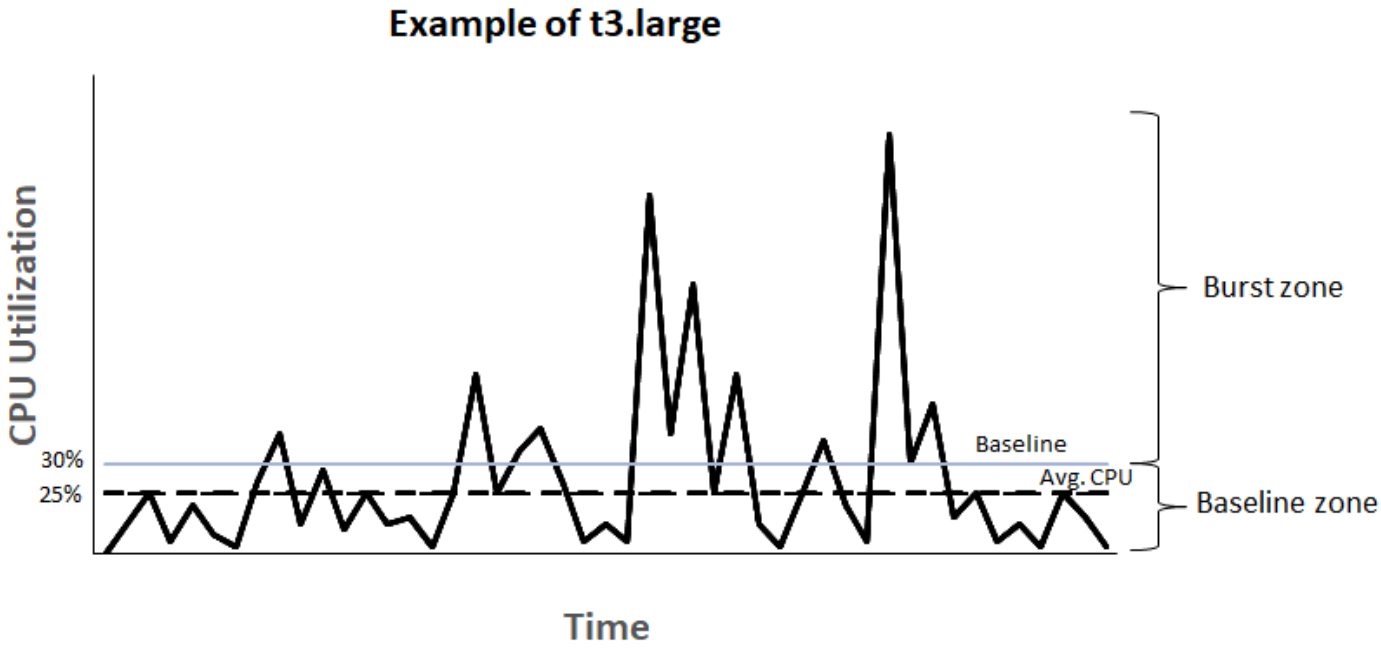
```
(number of credits earned/number of vCPUs)/60 minutes = % baseline
utilization
```

Ad esempio, un'istanza `t3.nano`, con 2 vCPU, guadagna 6 crediti all'ora, con un utilizzo di base del 5%, calcolato come segue:

```
(6 credits earned/2 vCPUs)/60 minutes = 5% baseline utilization
```

Un'istanza `t3.large`, con 2 vCPU, guadagna 36 crediti all'ora, con un utilizzo di base del 30% (`(36/2)/60`).

Il grafico seguente fornisce un esempio di `t3.large` con un utilizzo medio della CPU al di sotto della baseline.



Modalità illimitata per istanze a prestazioni espandibili

Un'istanza a prestazioni espandibili configurata come `unlimited` può sostenere un utilizzo elevato della CPU per tutto il tempo necessario in qualsiasi momento. Il prezzo orario copre automaticamente tutti i picchi di utilizzo della CPU se l'utilizzo medio della CPU dell'istanza corrisponde o è inferiore alla baseline per un periodo di 24 ore o la durata dell'istanza, a seconda di quale dei due è inferiore.

Per la grande maggioranza dei carichi di lavoro per scopi generici, le istanze configurate come `unlimited` offrono prestazioni elevate senza addebiti aggiuntivi. Se l'istanza viene eseguita con un maggiore utilizzo della CPU per un periodo prolungato, può farlo a una tariffa fissa aggiuntiva per v. CPU-hour Per informazioni sui prezzi, consulta i prezzi di Amazon EC2 e i prezzi della modalità T2/T3/T4 illimitata Prezzi della modalità

Se l'hai creata Account AWS prima del 15 luglio 2025 e utilizzi un'`t3.micro`istanza `t2.micro` or nell'ambito dell'Piano gratuito di AWSofferta e la usi in `unlimited` modalità, potrebbero essere

applicati dei costi se l'utilizzo medio su un periodo consecutivo di 24 ore supera l'utilizzo di base dell'istanza.

Le istanze T4g, T3a e T3 vengono avviate come `unlimited` per impostazione predefinita (a meno che non si modifichi l'impostazione predefinita). Se l'utilizzo medio della CPU per un periodo di 24 ore supera la baseline, vengono addebitati i costi per i crediti in eccedenza. Se avvii le Istanze spot come `unlimited` e prevedi di utilizzarle immediatamente e per un breve periodo, senza tempo di inattività per accumulare crediti CPU, vengono addebitati i costi per i crediti in eccedenza. Consigliamo di avviare le Istanze spot in modalità standard per evitare di pagare costi più elevati. Per ulteriori informazioni, consulta Possibilità di addebito dei costi per i crediti extra e Avvio di istanze a prestazioni espandibili.

> **Note**
>
> Le istanze T3 vengono avviate su host dedicato in modalità `standard` per impostazione predefinita; la modalità `unlimited` non è supportata per le istanze T3 su un host dedicato.

Indice

- Concetti di modalità illimitata per istanze espandibili
  - Come funzionano le istanze a prestazioni espandibili illimitata
  - Quando utilizzare la modalità illimitata rispetto alla CPU fissa
  - Possibilità di addebito dei costi per i crediti extra
  - Quanto costano le prestazioni illimitate ed espandibili?
  - Assenza di crediti di lancio per istanze T2 in modalità illimitata
  - Abilitazione della modalità illimitata
  - Cosa succede ai crediti quando si passa dalla modalità illimitata a Standard e viceversa
  - Monitoraggio dell'utilizzo del credito
- Esempi di modalità illimitata per istanze espandibili
  - Esempio 1: spiegazione dell'uso del credito con T3 in modalità illimitata
  - Esempio 2: spiegazione dell'uso del credito con T2 in modalità illimitata

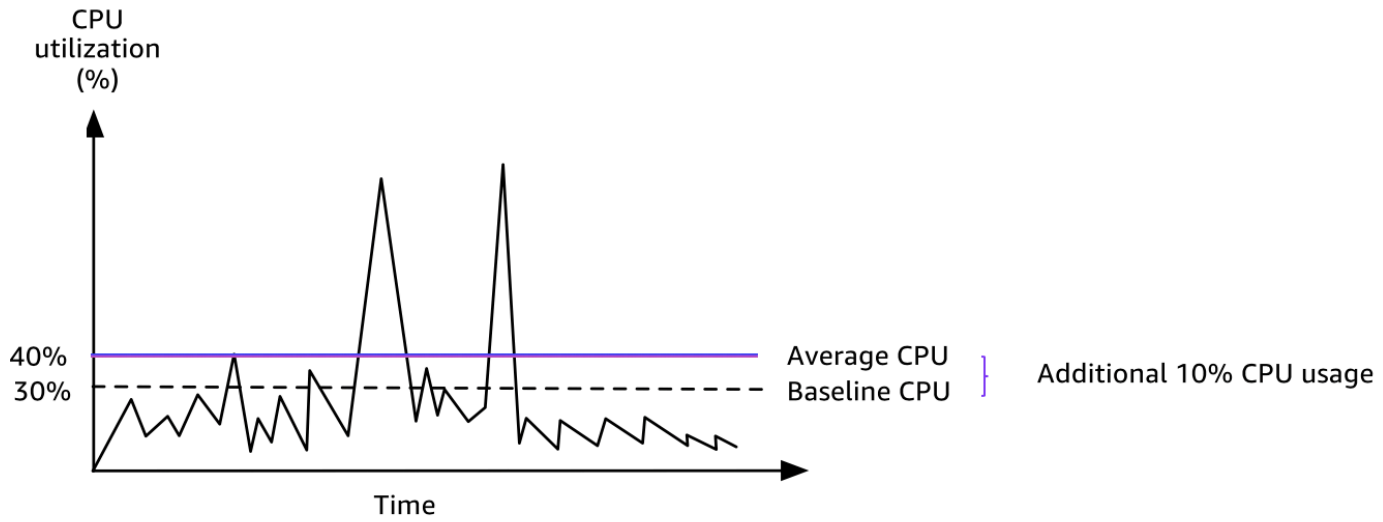
Concetti di modalità illimitata per istanze espandibili

La modalità `unlimited` è un'opzione di configurazione del credito per le istanze a prestazioni espandibili. Può essere abilitata o disabilitata in qualsiasi momento per un'istanza in esecuzione o arrestata. Puoi impostare `unlimited` come opzione di credito predefinita a livello di account per AWS regione, per famiglia di istanze Burstable Performance, in modo che tutte le nuove istanze Burstable Performance presenti nell'account vengano lanciate utilizzando l'opzione di credito predefinita.

Come funzionano le istanze a prestazioni espandibili illimitata

Se un'istanza a prestazioni espandibili configurata come `unlimited` esaurisce il suo saldo del credito CPU, può spendere crediti extra per superare la linea di base. Quando l'utilizzo della CPU è inferiore alla baseline, utilizza i crediti CPU che guadagna per pagare i crediti extra spesi in precedenza. La possibilità di guadagnare crediti CPU per pagare i crediti extra consente ad Amazon EC2 di calcolare una media dell'utilizzo della CPU di un'istanza in un periodo di 24 ore. Se l'utilizzo medio della CPU in un periodo di 24 ore supera la previsione, all'istanza viene fatturato l'utilizzo aggiuntivo a una tariffa aggiuntiva fissa (tariffa aggiuntiva fissa, tariffa fissa per v). CPU-hour

Il seguente grafico mostra l'utilizzo della CPU di un `t3.large`. L'utilizzo di base della CPU per un `t3.large` è 30%. Se l'istanza viene eseguita al 30% di utilizzo medio della CPU o meno in un periodo di 24 ore, non sono previsti costi aggiuntivi perché i costi sono già coperti dal prezzo orario dell'istanza. Tuttavia, se l'istanza viene eseguita in media con un utilizzo della CPU del 40% su un periodo di 24 ore, come mostrato nel grafico, all'istanza viene fatturato il 10% aggiuntivo di utilizzo della CPU a una tariffa aggiuntiva fissa (tariffa fissa fissa per v). CPU-hour



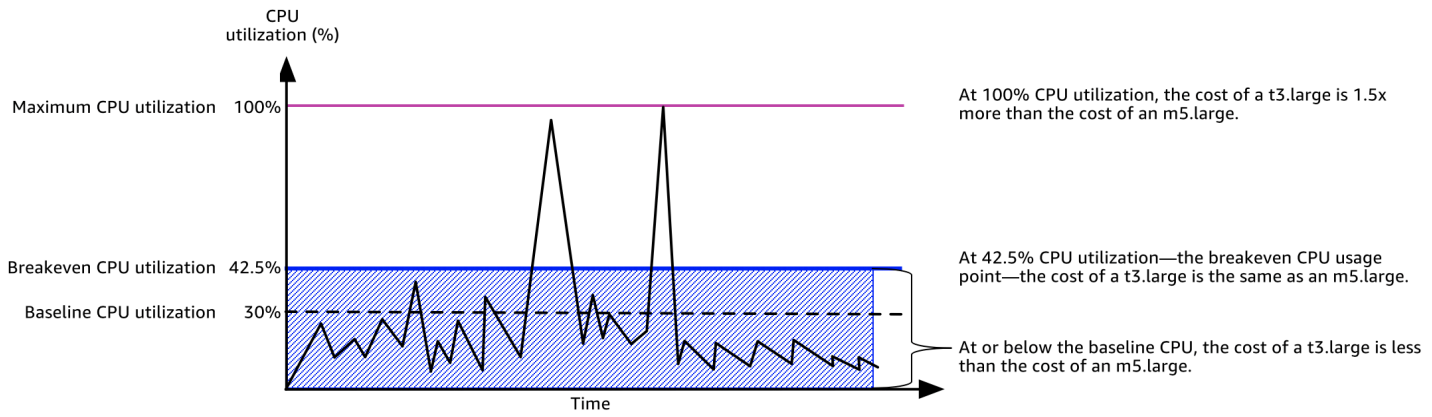
Per ulteriori informazioni sull'utilizzo di base per vCPU per ogni tipo di istanza e sul numero di crediti guadagnati da ogni tipo di istanza, consulta la tabella dei crediti.

Quando utilizzare la modalità illimitata rispetto alla CPU fissa

Nel determinare se utilizzare un'istanza a prestazioni espandibili in modalità `unlimited`, ad esempio T3 o un'istanza a prestazioni fisse, ad esempio M5, è necessario determinare il punto di utilizzo della CPU di break even. L'utilizzo della CPU di break even per un'istanza a prestazioni espandibili è il punto in cui il costo di un'istanza a prestazioni espandibili è identico a quello di un'istanza a prestazioni fisse. L'utilizzo della CPU di break even consente di determinare quanto segue:

- Se l'utilizzo medio della CPU in un periodo di 24 ore corrisponde o è inferiore all'utilizzo della CPU di break even, utilizza un'istanza a prestazioni espandibili in modalità `unlimited` per trarre vantaggio dal prezzo inferiore di un'istanza a prestazioni espandibili pur ottenendo le stesse prestazioni di un'istanza a prestazioni fisse.
- Se l'utilizzo medio della CPU in un periodo di 24 ore è superiore all'utilizzo della CPU di break even, l'istanza a prestazioni espandibili costerà di più rispetto all'istanza a prestazioni fisse di dimensioni equivalenti. Se un'istanza T3 emette continuamente picchi al 100% CPU, si pagherà all'incirca 1,5 volte il prezzo di un'istanza M5 di dimensioni equivalenti.

Il grafico seguente mostra il punto di utilizzo della CPU di break even in cui il costo di un `t3.large` è identico a quello di un `m5.large`. Il punto di utilizzo della CPU di break even per un `t3.large` è 42,5%. Se l'utilizzo medio della CPU è al 42,5%, il costo dell'esecuzione di `t3.large` è identico a quello di un `m5.large` ed è più costoso se l'utilizzo medio della CPU è superiore a 42,5%. Se il carico di lavoro richiede meno del 42,5% di utilizzo medio della CPU, puoi trarre vantaggio dal prezzo inferiore del `t3.large` pur ottenendo le stesse prestazioni di un`m5.large`.



La seguente tabella mostra come calcolare la soglia di utilizzo della CPU di break even in modo da determinare quando è meno costoso utilizzare un'istanza a prestazioni espandibili in modalità `unlimited` o un'istanza a prestazioni fisse. Le colonne nella tabella sono etichettate da A a K.

Tipo di istanza	vCPU	T3 prezzo*/ ora	M5 prezzo*/ ora	Differenza prezzo	Utilizzo di base T3 per vCPU (%)	Costo per vCPU/ ora per crediti extra	Costo per vCPU/ minuto	Minuti di burst aggiuntivi disponibili per vCPU	% CPU aggiuntiva disponibile	% CPU di break even
A	B	C	D	E = D - C	F	G	H = G / 60	I = E / H	J = (I / 60) / B	K = F + J
t3.large	2	0,0835 USD	0,096 USD	0,0125 USD	30%	0,05 $	0,000833 USD	15	12,5%	42,5%

Note

* Prezzo basato su us-east-1 e sistema operativo Linux.

La tabella fornisce le informazioni seguenti:

- La colonna A mostra il tipo di istanza, `t3.large`.
- La colonna B mostra il numero di vCPU per `t3.large`.
- La colonna C mostra il prezzo di un `t3.large` per ora.
- La colonna D mostra il prezzo di un `m5.large` per ora.
- La colonna E mostra la differenza di prezzo tra `t3.large` e `m5.large`.
- La colonna F mostra l'utilizzo di base per vCPU di `t3.large`, che è del 30%. Al livello base, il costo orario dell'istanza copre il costo di utilizzo della CPU.

- La colonna G mostra la tariffa forfettaria aggiuntiva per v CPU-hour che viene addebitata a un'istanza se raggiunge il 100% della CPU dopo aver esaurito i crediti guadagnati.
- La colonna H mostra la tariffa forfettaria aggiuntiva per v CPU-minute che viene addebitata a un'istanza se raggiunge il 100% della CPU dopo aver esaurito i crediti guadagnati.
- La colonna I mostra il numero di minuti aggiuntivi in cui `t3.large` può emettere picchi all'ora al 100% CPU pagando lo stesso prezzo orario di un `m5.large`.
- La colonna J mostra l'utilizzo aggiuntivo della CPU (in %) rispetto alla baseline in cui l'istanza può emettere picchi pagando lo stesso prezzo orario di un `m5.large`.
- La colonna K mostra l'utilizzo della CPU di break even (in %) in cui `t3.large` può emettere picchi senza pagare più di `m5.large`. In caso di superamento, il costo di `t3.large` è maggiore di quello di `m5.large`.

La tabella seguente mostra l'utilizzo della CPU di break even (in %) per tipi di istanza T3 in confronto ai tipi di istanza M5 di dimensioni simili.

Tipo di istanza T3	Utilizzo della CPU di break even (in %) per T3 in confronto a M5
`t3.large`	42,5%
`t3.xlarge`	52,5%
`t3.2xlarge`	52,5%

Possibilità di addebito dei costi per i crediti extra

Se l'utilizzo medio della CPU di un'istanza corrisponde o è inferiore alla baseline, non vengono addebitati costi aggiuntivi per l'istanza. Dato che un'istanza guadagna un numero massimo di crediti in un periodo di 24 ore (ad esempio, un'istanza `t3.micro` può guadagnare un massimo di 288 crediti in un periodo di 24 ore), può spendere crediti extra fino a quel massimo senza alcun addebito.

Tuttavia, se l'utilizzo della CPU rimane al di sopra della baseline, l'istanza non può guadagnare abbastanza crediti per pagare i crediti extra spesi. I crediti in eccesso non rimborsati vengono addebitati con una tariffa aggiuntiva fissa per v. CPU-hour Per informazioni sulla tariffa, consulta Prezzi per la modalità T2/T3/T4g illimitata Prezzi per la modalità

I crediti extra spesi in precedenza subiscono costi aggiuntivi quando si verifica uno dei seguenti casi:

- I crediti extra spesi vanno oltre il numero massimo di crediti che un'istanza può ottenere in un periodo di 24 ore. I crediti extra spesi, che eccedono il limite, subiscono costi aggiuntivi alla fine dell'ora;
- l'istanza viene arrestata o terminata;
- l'istanza passa da `unlimited` a `standard`.

I crediti in eccedenza spesi vengono tracciati in base alla CloudWatch metrica. `CPUSurplusCreditBalance` I crediti eccedenti addebitati vengono tracciati in base alla metrica. CloudWatch `CPUSurplusCreditsCharged` Per ulteriori informazioni, consulta Metriche aggiuntive per istanze con prestazioni straordinarie CloudWatch.

Quanto costano le prestazioni illimitate ed espandibili?

Se utilizzi i crediti in eccesso e questi non vengono ripagati dai crediti guadagnati (vediPossibilità di addebito dei costi per i crediti extra), paghi una tariffa aggiuntiva fissa per v CPU-hour per i crediti in eccesso. La tariffa è elencata nella T2/T3/T4g T2/T3 illimitata nella pagina dei prezzi di Amazon EC2 On-Demand.

Assenza di crediti di lancio per istanze T2 in modalità illimitata

Le istanze T2 Standard ricevono crediti di lancio, mentre le istanze T2 Unlimited non li ricevono. Un'istanza T2 Unlimited può superare la baseline in qualsiasi momento senza alcun addebito fino a quando l'utilizzo medio della CPU dell'istanza corrisponde o è inferiore alla baseline per un periodo continuo di 24 ore o per la sua durata, a seconda di quale dei due è inferiore. Pertanto, le istanze T2 Unlimited non richiedono crediti di lancio per ottenere prestazioni elevate immediatamente dopo l'avvio.

Se un'istanza T2 passa da `standard` a `unlimited`, tutti i crediti di lancio accumulati vengono rimossi da `CPUCreditBalance` prima di trasferire il `CPUCreditBalance` restante.

Le istanze T4g, T3a e T3 non ricevono mai crediti di avvio perché vengono avviate in modalità illimitata per impostazione predefinita e possono pertanto interrompersi immediatamente all'avvio. La configurazione del credito in modalità illimitata consente alle istanze T4g, T3a e T3 di utilizzare tutta la CPU necessaria per superare la baseline e per tutto il tempo necessario.

Abilitazione della modalità illimitata

È possibile passare da `unlimited` a `standard` e da `standard` a `unlimited` in qualsiasi momento su un'istanza in esecuzione o interrotta. Per ulteriori informazioni, consulta Configurazione

delle specifiche del credito al momento dell'avvio e Gestione della specifica del credito di un'istanza a prestazioni espandibili.

Puoi impostare `unlimited` come opzione di credito predefinita a livello di account per AWS regione, per famiglia di istanze Burstable Performance, in modo che tutte le nuove istanze Burstable Performance presenti nell'account vengano lanciate utilizzando l'opzione di credito predefinita. Per ulteriori informazioni, consulta Gestione della specifica del credito predefinita per un account.

Puoi verificare se l'istanza espandibile è configurata come `unlimited` o `standard` utilizzando la console Amazon EC2 o AWS CLI. Per ulteriori informazioni, consulta Configurazione delle istanze a prestazioni espandibili.

Cosa succede ai crediti quando si passa dalla modalità illimitata a Standard e viceversa

`CPUCreditBalance`è una CloudWatch metrica che tiene traccia del numero di crediti maturati da un'istanza. `CPUSurplusCreditBalance`è una CloudWatch metrica che tiene traccia del numero di crediti in eccesso spesi da un'istanza.

Quando si modifica un'istanza configurata come `unlimited` in `standard`, si verifica quanto segue:

- Il valore `CPUCreditBalance` rimane invariato e viene trasferito.
- Il valore `CPUSurplusCreditBalance` viene immediatamente addebitato.

Quando un'istanza `standard` passa a `unlimited`, si verifica quanto segue:

- Il valore `CPUCreditBalance` contenente i crediti guadagnati accumulati viene trasferito.
- Per le istanze T2 Standard, tutti i crediti di lancio accumulati vengono rimossi dal valore `CPUCreditBalance`, mentre il valore `CPUCreditBalance` residuo, contenente i crediti guadagnati accumulati, viene trasferito.

Monitoraggio dell'utilizzo del credito

Per vedere se la tua istanza spende più crediti di quelli forniti dalla baseline, puoi utilizzare le CloudWatch metriche per monitorare l'utilizzo e puoi impostare allarmi orari per ricevere notifiche sull'utilizzo del credito. Per ulteriori informazioni, consulta Monitoraggio dei crediti CPU per istanze espandibili.

Esempi di modalità illimitata per istanze espandibili

Di seguito vengono forniti esempi che spiegano l'utilizzo del credito per le istanze configurate come `unlimited`.

Esempi

- Esempio 1: spiegazione dell'uso del credito con T3 in modalità illimitata
- Esempio 2: spiegazione dell'uso del credito con T2 in modalità illimitata

Esempio 1: spiegazione dell'uso del credito con T3 in modalità illimitata

Questo esempio illustra l'utilizzo della CPU di un'istanza `t3.nano` avviata come `unlimited` e in che modo spende i crediti guadagnati ed extra per sostenere l'utilizzo della CPU.

Un'istanza `t3.nano` guadagna 144 crediti CPU in un periodo continuo di 24 ore, che può utilizzare per 144 minuti di utilizzo di vCPU. Quando esaurisce il saldo di crediti della CPU (rappresentato dalla CloudWatch metrica`CPUCreditBalance`), può spendere i crediti CPU in eccesso, che non ha ancora guadagnato, per esaurirli per tutto il tempo necessario. Dato che un'istanza `t3.nano` guadagna un massimo di 144 crediti in un periodo di 24 ore, può spendere crediti extra fino a quel valore massimo senza alcun addebito immediato. Se spende più di 144 crediti CPU, viene addebitata la differenza alla fine dell'ora.

L'intento dell'esempio, illustrato dal seguente grafico, è quello di mostrare come un'istanza possa ottimizzare le prestazioni utilizzando i crediti extra anche dopo aver esaurito il suo `CPUCreditBalance`. l seguente flusso di lavoro fa riferimento ai punti numerati sul grafico:

P1 - All'ora– 0 sul grafico l'istanza viene avviata come `unlimited` e inizia immediatamente a guadagnare crediti. L'istanza rimane inattiva dal momento in cui viene avviata —(l'utilizzo della CPU è pari allo 0%)— e non vengono spesi crediti. Tutti i crediti non spesi vengono accumulati nel saldo del credito. Per le prime 24 ore, `CPUCreditUsage` è a 0 e il valore `CPUCreditBalance` raggiunge il suo massimo di 144.

P2 – per le 12 ore successive, l'utilizzo della CPU è al 2,5%, ovvero inferiore al 5% della baseline. L'istanza guadagna più crediti di quanti ne spende, ma il valore `CPUCreditBalance` non può superare il suo massimo di 144 crediti.

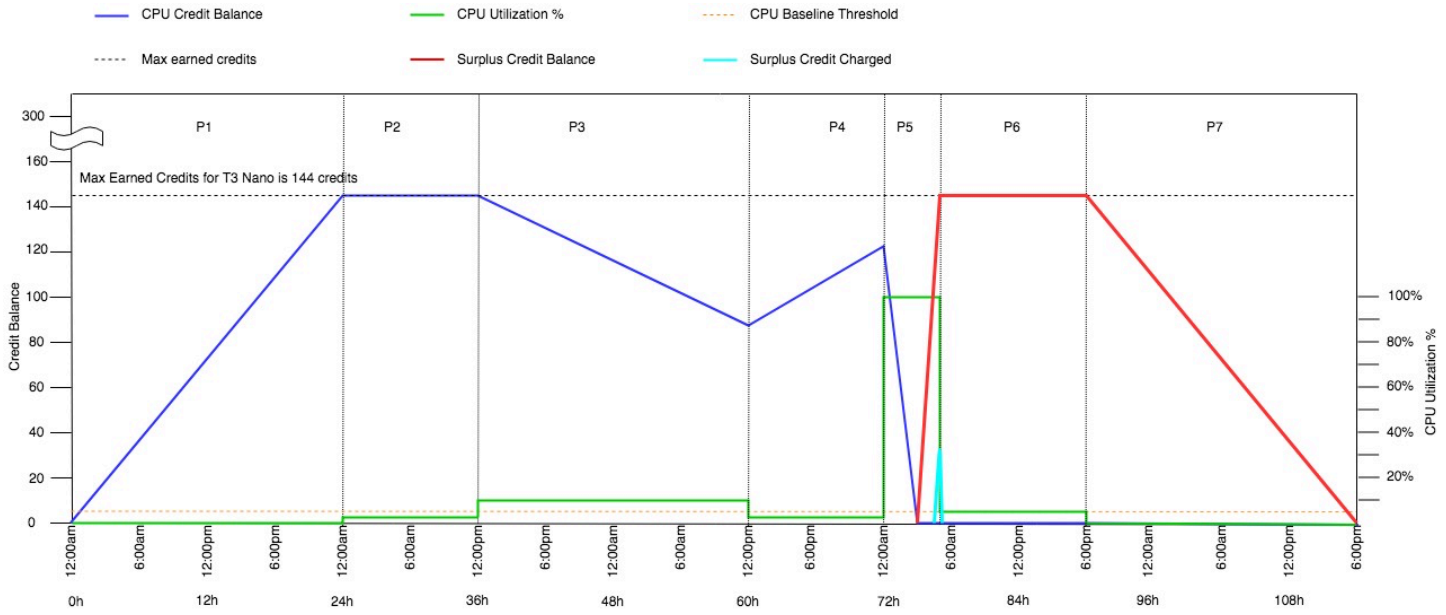
P3 – per le 24 ore successive, l'utilizzo della CPU è al 7% (superiore alla baseline), il che richiede una spesa del 57,6% dei crediti. L'istanza spende più crediti di quanti ne guadagna e il valore `CPUCreditBalance` si riduce a 86,4 crediti.

P4 – per le 12 ore successive, l'utilizzo della CPU si riduce al 2,5% (inferiore alla baseline), il che richiede una spesa di 36 crediti. Allo stesso tempo, l'istanza guadagna 72 crediti. L'istanza guadagna più crediti di quanti ne spende e il valore `CPUCreditBalance` aumenta a 122 crediti.

P5 – per le 5 ore successive, l'istanza aumenta al 100% dell'utilizzo della CPU e spende un totale di 570 crediti per sostenere l'espansione. Dopo circa un'ora, l'istanza esaurisce il suo intero `CPUCreditBalance` di 122 crediti e inizia a spendere crediti extra per sostenere l'utilizzo elevato della CPU, per un totale di 448 crediti extra in questo periodo di tempo (570-122=448). Quando il valore `CPUSurplusCreditBalance` raggiunge 144 crediti della CPU (il massimo che un'istanza `t3.nano` può guadagnare in un periodo di 24 ore), tutti i crediti extra spesi successivamente non possono essere compensati con crediti guadagnati. I crediti extra spesi successivamente ammontano a 304 crediti (448-144=304), il che si traduce in un piccolo costo aggiuntivo al termine dell'ora per 304 crediti.

P6 – per le 13 ore successive, l'utilizzo della CPU è al 5% (pari alla baseline). L'istanza guadagna lo stesso numero di crediti che spende, senza eccessi da ripagare il `CPUSurplusCreditBalance`. Il valore `CPUSurplusCreditBalance` rimane a 144 crediti.

P7 – per le ultime 24 ore di questo esempio, l'istanza è inattiva e l'utilizzo della CPU è allo 0%. In questo arco di tempo, l'istanza guadagna 144 crediti, che utilizza per ripagare il `CPUSurplusCreditBalance`.



Esempio 2: spiegazione dell'uso del credito con T2 in modalità illimitata

Questo esempio illustra l'utilizzo della CPU di un'istanza `t2.nano` avviata come `unlimited` e in che modo spende i crediti guadagnati ed extra per sostenere l'utilizzo della CPU.

Un'istanza `t2.nano` guadagna 72 crediti CPU in un periodo continuo di 24 ore, che può utilizzare per 72 minuti di utilizzo di vCPU. Quando esaurisce il saldo di crediti della CPU (rappresentato dalla CloudWatch metrica`CPUCreditBalance`), può spendere i crediti CPU in eccesso, che non ha ancora guadagnato, per esaurirli per tutto il tempo necessario. Dato che un'istanza `t2.nano` guadagna un massimo di 72 crediti in un periodo di 24 ore, può spendere crediti extra fino a quel valore massimo senza alcun addebito immediato. Se spende più di 72 crediti CPU, viene addebitata la differenza alla fine dell'ora.

L'intento dell'esempio, illustrato dal seguente grafico, è quello di mostrare come un'istanza possa ottimizzare le prestazioni utilizzando i crediti extra anche dopo aver esaurito il suo `CPUCreditBalance`. È possibile presumere che, all'inizio della linea temporale nel grafico, l'istanza abbia un saldo del credito accumulato uguale al numero massimo di crediti che può guadagnare in 24 ore. l seguente flusso di lavoro fa riferimento ai punti numerati sul grafico:

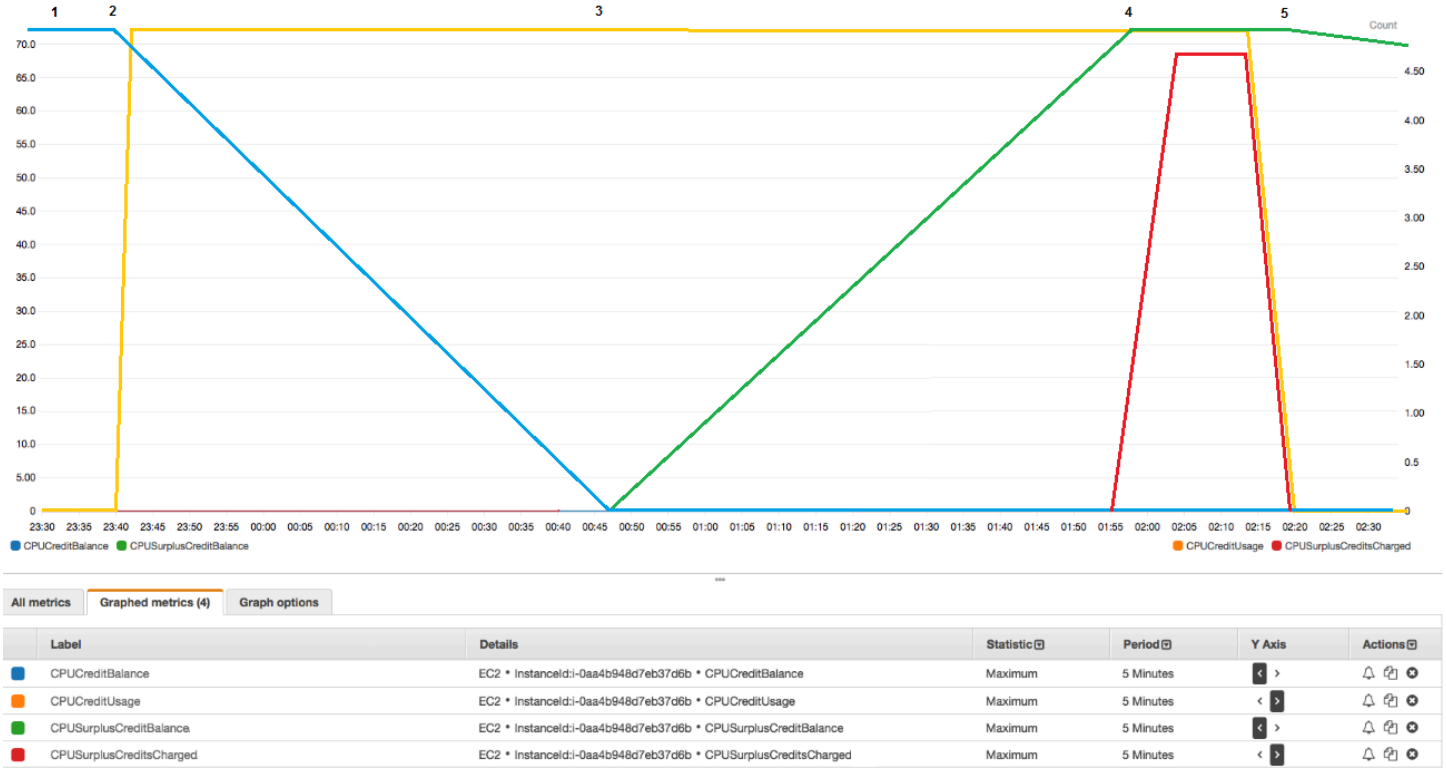
1 – nei primi 10 minuti, `CPUCreditUsage` è a 0 e il valore `CPUCreditBalance` rimane al suo massimo di 72.

2 – alle 23:40, con l'aumentare dell'utilizzo della CPU, l'istanza spende i crediti della CPU e il valore `CPUCreditBalance` diminuisce.

3 – intorno alle 00:47, l'istanza esaurisce l'intero `CPUCreditBalance` e inizia a spendere crediti extra per sostenere l'utilizzo elevato della CPU.

4 – i crediti extra vengono spesi fino all'01:55, quando il valore `CPUSurplusCreditBalance` raggiunge 72 crediti CPU. Questo corrisponde al massimo che un'istanza `t2.nano` può guadagnare in un periodo di 24 ore. Eventuali crediti extra spesi successivamente non possono essere compensati con crediti guadagnati nel periodo di 24 ore, il che si traduce in un piccolo costo aggiuntivo al termine dell'ora.

5 – l'istanza continua a spendere crediti extra fino a circa le 02:20. A questo punto, l'utilizzo della CPU è inferiore alla baseline e l'istanza inizia a guadagnare crediti a 3 crediti all'ora (o 0,25 crediti ogni 5 minuti), utilizzati per pagare il `CPUSurplusCreditBalance`. Dopo che il valore `CPUSurplusCreditBalance` si riduce a 0, l'istanza inizia ad accumulare crediti guadagnati nel suo `CPUCreditBalance` a 0,25 crediti ogni 5 minuti.



Calcolo della fattura (istanza Linux)

I crediti in eccesso costano $0,05 per v. CPU-hour L'istanza ha speso circa 25 crediti in eccesso tra le 01:55 e le 02:20, il che equivale a 0,42 v. CPU-hours I costi aggiuntivi per questa istanza sono 0,42 v x 0 USD. CPU-hours 05/vCPU-ora = 0,021 USD, arrotondato a 0,02 USD. Ecco la fattura di fine mese per questa istanza T2 Unlimited:

Amazon Elastic Compute Cloud running Linux/UNIX		
$0.0058 per On Demand Linux t2.nano Instance Hour	720.000 Hrs	$4.18

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.05 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.02

Calcolo della fattura (istanza Windows)

I crediti in eccedenza costano 0,096 USD per v. CPU-hour L'istanza ha speso circa 25 crediti in eccesso tra le 01:55 e le 02:20, il che equivale a 0,42 v. CPU-hours I costi aggiuntivi per questa istanza sono 0,42 v x 0 USD. CPU-hours 096/vCPU-ora = 0,04032 USD, arrotondato a 0,04 USD. Ecco la fattura di fine mese per questa istanza T2 Unlimited:

Amazon Elastic Compute Cloud running Windows		
$0.0081 per On Demand Windows t2.nano Instance Hour	720.000 Hrs	$5.83

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.096 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.04

È possibile impostare gli avvisi di fatturazione per essere avvisati ogni ora di eventuali addebiti accumulati e agire, se necessario.

Modalità standard per istanze a prestazioni espandibili

Un'istanza a prestazioni espandibili configurata come `standard` è adatta ai carichi di lavoro con un utilizzo medio della CPU costantemente inferiore all'utilizzo di base dell'istanza. Per superare la baseline, l'istanza spende i crediti accumulati nel suo saldo del credito CPU. Se l'istanza sta esaurendo i crediti accumulati, l'utilizzo della CPU viene gradualmente ridotto al livello di prestazioni di base, in modo che l'istanza non subisca una forte riduzione delle prestazioni una volta esaurito il saldo del credito CPU. Per ulteriori informazioni, consulta Concetti chiave per istanze a prestazioni espandibili.

Indice

- Concetti di modalità standard per istanze espandibili
  - Come funzionano le istanze a prestazioni espandibili Standard
  - Crediti di lancio
  - Limiti dei crediti di lancio
  - Differenze tra crediti di lancio e crediti guadagnati
- Esempi di modalità standard per istanze espandibili
  - Esempio 1: spiegazione dell'uso del credito con T3 Standard
  - Esempio 2: spiegazione dell'uso del credito con T2 Standard
    - Periodo 1: 1 – 24 ore
    - Periodo 2: 25 – 36 ore
    - Periodo 3: 37 – 61 ore
    - Periodo 4: 62 – 72 ore
    - Periodo 5: 73 – 75 ore
    - Periodo 6: 76 – 90 ore

- Periodo 7: 91 – 96 ore

Concetti di modalità standard per istanze espandibili

La modalità `standard` è un'opzione di configurazione per le istanze a prestazioni espandibili. Può essere abilitata o disabilitata in qualsiasi momento per un'istanza in esecuzione o arrestata. Puoi impostare `standard` come opzione di credito predefinita a livello di account per AWS regione, per famiglia di istanze Burstable Performance, in modo che tutte le nuove istanze Burstable Performance presenti nell'account vengano lanciate utilizzando l'opzione di credito predefinita.

Come funzionano le istanze a prestazioni espandibili Standard

Quando un'istanza a prestazioni espandibili configurata come `standard` è in fase di esecuzione, guadagna continuamente (a una risoluzione a livello di millisecondo) un tasso fisso di crediti guadagnati all'ora. Quando un'istanza T2 Standard viene interrotta, perde tutti i crediti accumulati e il suo saldo attivo viene azzerato. Quando viene riavviata, riceve una nuova serie di crediti di lancio e inizia ad accumulare crediti guadagnati. Per le istanze T4g, T3a e T3 standard, il saldo di crediti della CPU viene conservato per sette giorni, trascorsi i quali l'istanza viene arrestata e i crediti vengono persi. Se avvii l'istanza entro sette giorni, non viene perso alcun credito.

Le istanze T2 Standard ricevono due tipi di crediti CPU: crediti guadagnati e crediti di lancio. Quando un'istanza di T2 Standard è in fase di esecuzione, guadagna continuamente (a una risoluzione a livello di millisecondo) un tasso fisso di crediti guadagnati all'ora. All'inizio, non ha guadagnato ancora i crediti necessari per una buona esperienza di avvio; pertanto, per fornire una buona esperienza di startup, riceve inizialmente i crediti di lancio, che spende mentre accumula crediti guadagnati.

Le istanze T4g, T3a e T3 non ricevono mai crediti di avvio perché supportano la modalità illimitata. La configurazione del credito in modalità illimitata consente alle istanze T4g, T3a e T3 di utilizzare tutta la CPU necessaria per superare la baseline e per tutto il tempo necessario.

Crediti di lancio

Le istanze T2 Standard ottengono 30 crediti di lancio per vCPU al lancio o all'avvio, mentre le istanze T1 Standard ottengono 15 crediti di lancio. Ad esempio, un'istanza `t2.micro` ha un vCPU e ottiene 30 crediti di lancio, mentre un'istanza `t2.xlarge` ha quattro vCPU e ottiene 120 crediti di lancio. I crediti di lancio sono progettati per fornire una buona esperienza di startup in modo da consentire immediatamente dopo l'avvio l'ottimizzazione delle istanze prima che abbiano accumulato crediti guadagnati.

Per primi vengono spesi i crediti di lancio, prima dei crediti guadagnati. I crediti di lancio non spesi vengono accumulati nel saldo del credito CPU, ma non contano per il limite del saldo del credito CPU. Ad esempio, un'istanza `t2.micro` ha un limite del saldo del credito CPU di 144 crediti guadagnati. Se viene avviata e rimane inattiva per 24 ore, il suo saldo del credito CPU raggiunge 174 (30 crediti di lancio + 144 crediti guadagnati), che è oltre il limite. Tuttavia, una volta che l'istanza spende i 30 crediti di lancio, il saldo del credito non può superare 144. Per ulteriori informazioni sul limite del saldo del credito CPU per ciascuna dimensione dell'istanza, consulta la tabella del credito.

La tabella seguente elenca l'allocazione iniziale del credito CPU ricevuta all'avvio e il numero di vCPU.

Tipo di istanza	Crediti di lancio	vCPU
`t1.micro`	15	1
`t2.nano`	30	1
`t2.micro`	30	1
`t2.small`	30	1
`t2.medium`	60	2
`t2.large`	60	2
`t2.xlarge`	120	4
`t2.2xlarge`	240	8

Limiti dei crediti di lancio

Il numero di volte in cui le istanza T2 Standard possono ricevere crediti di lancio è limitato. Il limite predefinito è di 100 avvii di tutte le istanze T2 Standard combinate per account, per regione, per periodo continuo di 24 ore. Ad esempio, il limite viene raggiunto quando un'istanza viene interrotta e avviata 100 volte in un periodo di 24 ore oppure quando vengono avviate 100 istanze in un periodo di 24 ore o se vengono avviate altre combinazioni equivalenti a 100 avvii. I nuovi account potrebbero avere un limite inferiore, che aumenta nel tempo in base al tuo utilizzo.

> **Tip**
>
> Per garantire che i carichi di lavoro ottengano sempre le prestazioni di cui hanno bisogno, passa a Modalità illimitata per istanze a prestazioni espandibili o prendi in considerazione l'utilizzo di una dimensione di istanza più grande.

Differenze tra crediti di lancio e crediti guadagnati

La seguente tabella elenca le differenze tra i crediti di lancio e i crediti guadagnati.

	Crediti di lancio	Crediti guadagnati
Tasso di guadagno di crediti	Le istanze T2 Standard ottengono 30 crediti di lancio per vCPU all'avvio. Se un'istanza T2 passa da `unlimited` a `standard`, non ottiene i crediti di lancio al momento del passaggio.	Ogni istanza T2 guadagna continuamente (a una risoluzione a livello di millisecondo) un tasso fisso di crediti CPU all'ora, a seconda delle dimensioni dell'istanza. Per ulteriori informazioni sul numero di crediti CPU guadagnati per dimensione dell'istanza, consulta tabella del credito.
Limite di guadagno di crediti	Il limite per la ricezione di crediti di lancio è di 100 avvii di tutte le istanze T2 Standard combinate per account, per regione, per periodo continuo di 24 ore. I nuovi account potrebbero avere un limite inferiore, che aumenta nel tempo in base al tuo utilizzo.	Un'istanza T2 può accumulare più crediti rispetto al limite del saldo del credito CPU. Se il saldo del credito CPU ha raggiunto il suo limite, tutti i crediti guadagnati dopo il raggiungimento del limite vengono scartati. I crediti di lancio non contano per il limite. Per ulteriori informazioni sul limite del saldo del credito CPU per ciascuna dimensione dell'istanza T2, consulta la tabella del credito.
Utilizzo crediti	Per primi vengono spesi i crediti di lancio, prima dei crediti guadagnati.	I crediti guadagnati vengono spesi solo dopo aver speso tutti i crediti di lancio.

	Crediti di lancio	Crediti guadagnati
Scadenza crediti	Quando è in esecuzione un'istanza T2 Standard, i crediti di lancio non scadono. Quando un'istanza di T2 Standard si interrompe o passa a T2 Unlimited, tutti i crediti di lancio vengono persi.	Quando un'istanza T2 è in esecuzione, i crediti guadagnati accumulati non scadono. Quando l'istanza T2 si interrompe, tutti i crediti guadagnati accumulati vengono persi.

Il numero di crediti di lancio accumulati e di crediti guadagnati accumulati è monitorato dal parametro CloudWatch `CPUCreditBalance`. Per ulteriori informazioni, consulta `CPUCreditBalance` nella tabella dei parametri CloudWatch .

Esempi di modalità standard per istanze espandibili

Di seguito vengono forniti esempi che spiegano l'utilizzo del credito quando le istanze sono configurate come `standard`.

Esempi

- Esempio 1: spiegazione dell'uso del credito con T3 Standard
- Esempio 2: spiegazione dell'uso del credito con T2 Standard

Esempio 1: spiegazione dell'uso del credito con T3 Standard

In questo esempio, è possibile vedere in che modo un'istanza `t3.nano` avviata come `standard` guadagna, accumula e spende crediti guadagnati. Viene mostrato in che modo il saldo dei crediti rispecchia i crediti guadagnati accumulati.

Un'istanza `t3.nano` in esecuzione guadagna 144 crediti ogni 24 ore. Il suo limite del saldo del credito è 144 crediti guadagnati. Una volta che il limite viene raggiunto, i nuovi crediti guadagnati vengono scartati. Per ulteriori informazioni sul numero di crediti che può essere guadagnato e accumulato, consulta la tabella del credito.

È possibile avviare un'istanza T3 Standard e utilizzarla immediatamente. In alternativa, è possibile avviare un'istanza T3 Standard e lasciarla inattiva per alcuni giorni prima di eseguire applicazioni su di essa. L'utilizzo o l'inattività di un'istanza determina se i crediti vengono spesi o accumulati. Se un'istanza rimane inattiva per 24 ore dal momento in cui viene avviata, il saldo del credito raggiunge il limite, ovvero il numero massimo di crediti guadagnati che possono essere accumulati.

Questo esempio descrive un'istanza che rimane inattiva per 24 ore dal momento in cui viene avviata e illustra sette periodi di tempo per 96 ore, mostrando la frequenza a cui i crediti vengono guadagnati, accumulati, spesi e scartati e il valore del saldo del credito alla fine di ciascun periodo.

l seguente flusso di lavoro fa riferimento ai punti numerati sul grafico:

P1 - All'ora– 0 sul grafico l'istanza viene avviata come `standard` e inizia immediatamente a guadagnare crediti. L'istanza rimane inattiva dal momento in cui viene avviata —(l'utilizzo della CPU è pari allo 0%)— e non vengono spesi crediti. Tutti i crediti non spesi vengono accumulati nel saldo del credito. Per le prime 24 ore, `CPUCreditUsage` è a 0 e il valore `CPUCreditBalance` raggiunge il suo massimo di 144.

P2 – per le 12 ore successive, l'utilizzo della CPU è al 2,5%, ovvero inferiore al 5% della baseline. L'istanza guadagna più crediti di quanti ne spende, ma il valore `CPUCreditBalance` non può superare il suo massimo di 144 crediti. Tutti i crediti guadagnati in eccesso rispetto al limite vengono scartati.

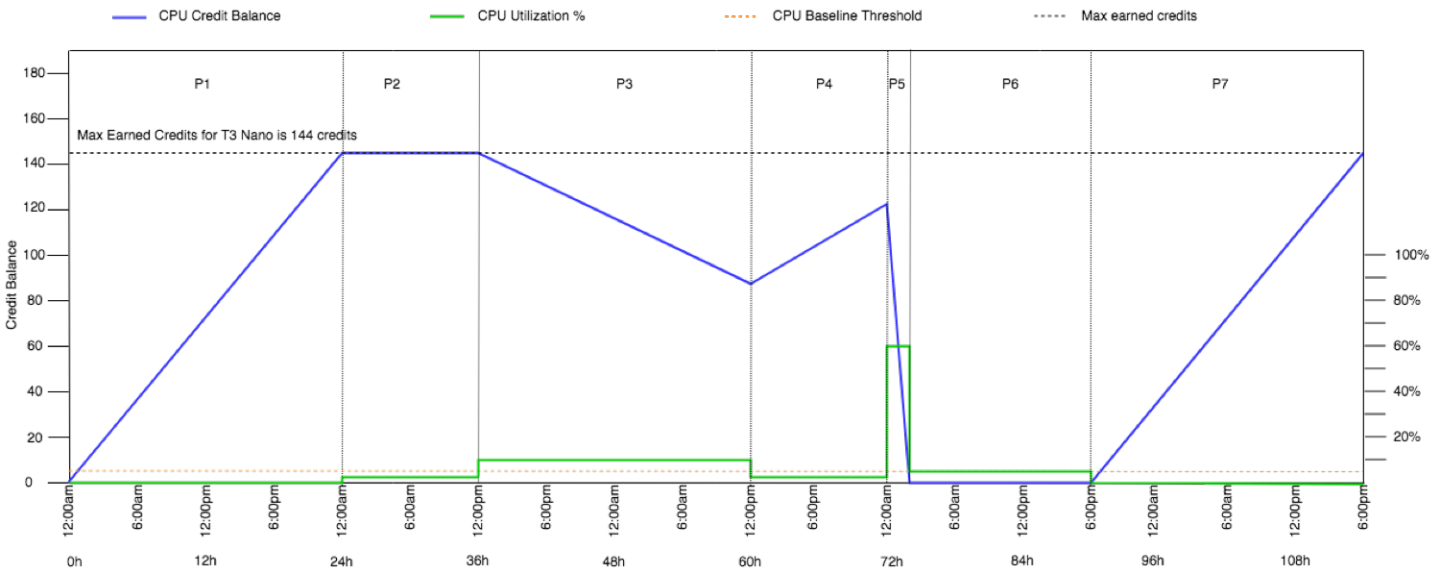
P3 – per le 24 ore successive, l'utilizzo della CPU è al 7% (superiore alla baseline), il che richiede una spesa del 57,6% dei crediti. L'istanza spende più crediti di quanti ne guadagna e il valore `CPUCreditBalance` si riduce a 86,4 crediti.

P4 – per le 12 ore successive, l'utilizzo della CPU si riduce al 2,5% (inferiore alla baseline), il che richiede una spesa di 36 crediti. Allo stesso tempo, l'istanza guadagna 72 crediti. L'istanza guadagna più crediti di quanti ne spende e il valore `CPUCreditBalance` aumenta a 122 crediti.

P5: per le 2 ore successive, l'istanza raggiunge il 60% di utilizzo della CPU ed esaurisce il suo intero valore `CPUCreditBalance` di 122 crediti. Al termine di questo periodo, con il `CPUCreditBalance` a zero, l'utilizzo di base scende al livello delle prestazioni di base del 5%. Al livello base, l'istanza guadagna lo stesso numero di crediti che spende.

P6 – per le 14 ore successive, l'utilizzo della CPU è al 5% (livello baseline). L'istanza guadagna lo stesso numero di crediti che spende. Il valore `CPUCreditBalance` rimane a 0.

P7 – per le ultime 24 ore di questo esempio, l'istanza è inattiva e l'utilizzo della CPU è allo 0%. In questo arco di tempo, l'istanza guadagna 144 crediti, che accumula nel suo `CPUCreditBalance`.



Esempio 2: spiegazione dell'uso del credito con T2 Standard

In questo esempio, è possibile vedere in che modo un'istanza `t2.nano` avviata come `standard` guadagna, accumula e spende crediti di lancio e guadagnati. Viene mostrato in che modo il saldo dei crediti riflette non solo i crediti guadagnati accumulati, ma anche i crediti di lancio accumulati.

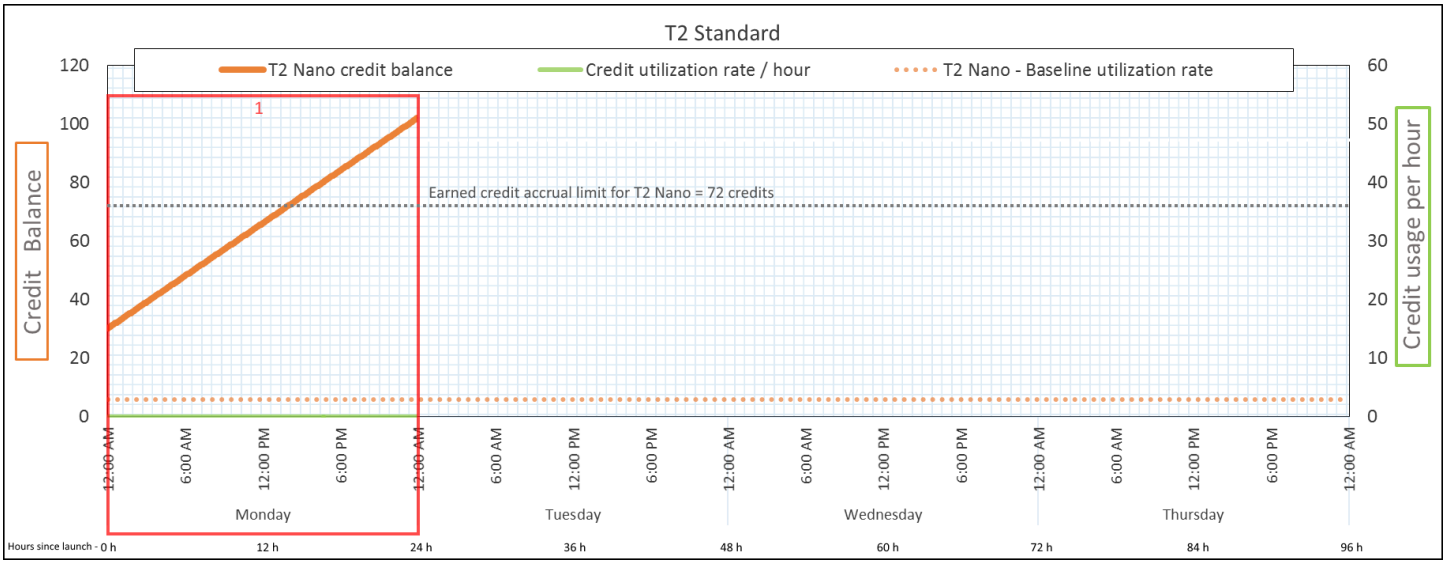
Un'istanza `t2.nano` ottiene 30 crediti di lancio quando viene avviata e guadagna 72 crediti ogni 24 ore. Il suo limite del saldo del credito è di 72 crediti guadagnati; i crediti di lancio non contano per il limite. Una volta che il limite viene raggiunto, i nuovi crediti guadagnati vengono scartati. Per ulteriori informazioni sul numero di crediti che può essere guadagnato e accumulato, consulta la tabella del credito. Per ulteriori informazioni sui limiti, consulta Limiti dei crediti di lancio.

È possibile avviare un'istanza T2 Standard e utilizzarla immediatamente. In alternativa, è possibile avviare un'istanza T2 Standard e lasciarla inattiva per alcuni giorni prima di eseguire applicazioni su di essa. L'utilizzo o l'inattività di un'istanza determina se i crediti vengono spesi o accumulati. Se un'istanza rimane inattiva per 24 ore dal momento in cui viene avviata, il saldo del credito sembra superare il limite poiché il saldo riflette sia i crediti guadagnati accumulati sia i crediti di lancio accumulati. Tuttavia, una volta utilizzata la CPU, i crediti di lancio vengono spesi per primi. Successivamente, il limite riflette sempre il numero massimo di crediti guadagnati che può essere accumulato.

Questo esempio descrive un'istanza che rimane inattiva per 24 ore dal momento in cui viene avviata e illustra sette periodi di tempo per 96 ore, mostrando la frequenza a cui i crediti vengono guadagnati, accumulati, spesi e scartati e il valore del saldo del credito alla fine di ciascun periodo.

Periodo 1: 1 – 24 ore

All'ora 0 sul grafico, l'istanza T2 viene avviata come `standard` e ottiene immediatamente 30 crediti di lancio. Guadagna crediti mentre è in fase di esecuzione. L'istanza rimane inattiva dal momento in cui viene avviata —(l'utilizzo della CPU è pari allo 0%)— e non vengono spesi crediti. Tutti i crediti non spesi vengono accumulati nel saldo del credito. A circa 14 ore dopo l'avvio, il saldo del credito è 72 (30 crediti di lancio + 42 crediti guadagnati), che equivale a ciò che l'istanza può guadagnare in 24 ore. A 24 ore dopo il lancio, il saldo del credito supera 72 crediti perché i crediti di lancio non spesi vengono accumulati nel— saldo del credito e il saldo del credito è 102 crediti: 30 crediti di lancio + 72 crediti guadagnati.



Metrica	Valore
Tasso di spesa di crediti	0 crediti in 24 ore (0% di utilizzo della CPU)
Tasso di guadagno di crediti	72 crediti in 24 ore
Tasso di scarto di crediti	0 crediti in 24 ore
Saldo del credito	102 crediti (30 crediti di lancio + 72 crediti guadagnati)

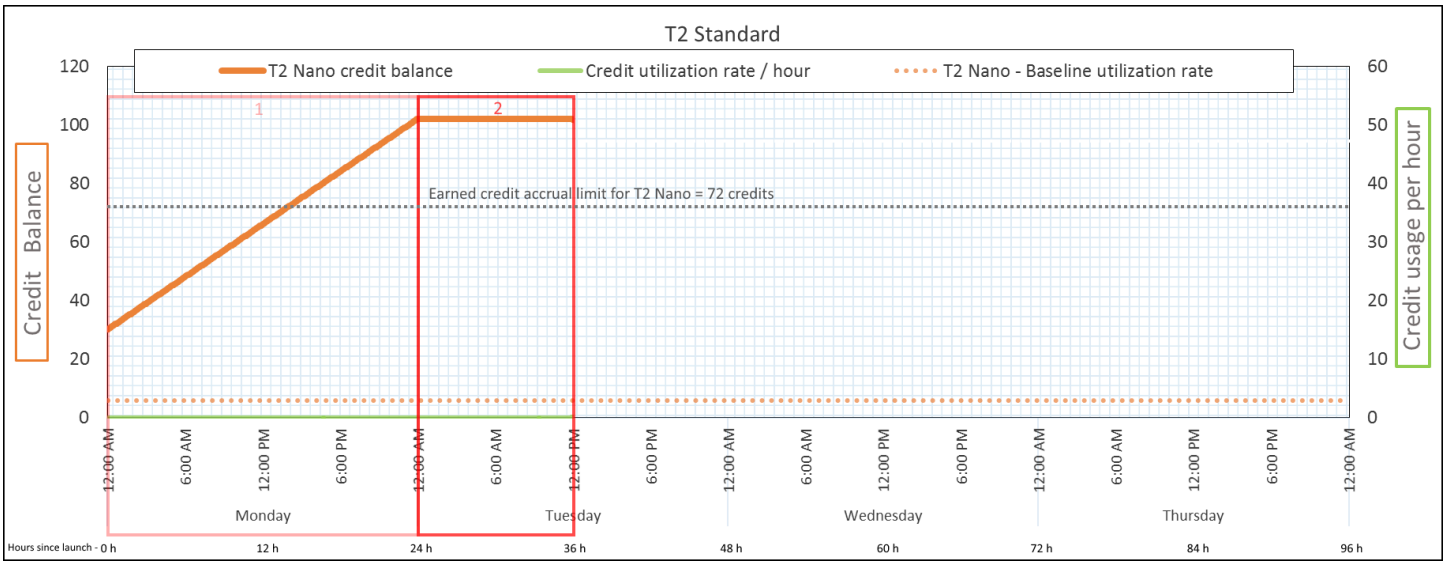
Conclusioni

Se dopo l'avvio non viene utilizzata CPU, l'istanza accumula più crediti di quanto possa guadagnare in 24 ore (30 crediti di lancio + 72 crediti guadagnati = 102 crediti).

In uno scenario reale, un'istanza EC2 consuma un numero ridotto di crediti durante l'avvio e l'esecuzione, il che impedisce al saldo di raggiungere il valore teorico massimo in questo esempio.

Periodo 2: 25 – 36 ore

Per le successive 12 ore, l'istanza continua a rimanere inattiva e guadagna crediti, ma il saldo del credito non aumenta. Si stabilizza a 102 crediti (30 crediti di lancio + 72 crediti guadagnati). Il saldo del credito ha raggiunto il limite di 72 crediti guadagnati accumulati, pertanto i crediti appena guadagnati vengono scartati.



Metrica	Valore
Tasso di spesa di crediti	0 crediti in 24 ore (0% di utilizzo della CPU)
Tasso di guadagno di crediti	72 crediti in 24 ore (3 crediti all'ora)
Tasso di scarto di crediti	72 crediti in 24 ore (100% del tasso di guadagno di crediti)
Saldo del credito	102 crediti (30 crediti di lancio + 72 crediti guadagnati),— il saldo è invariato

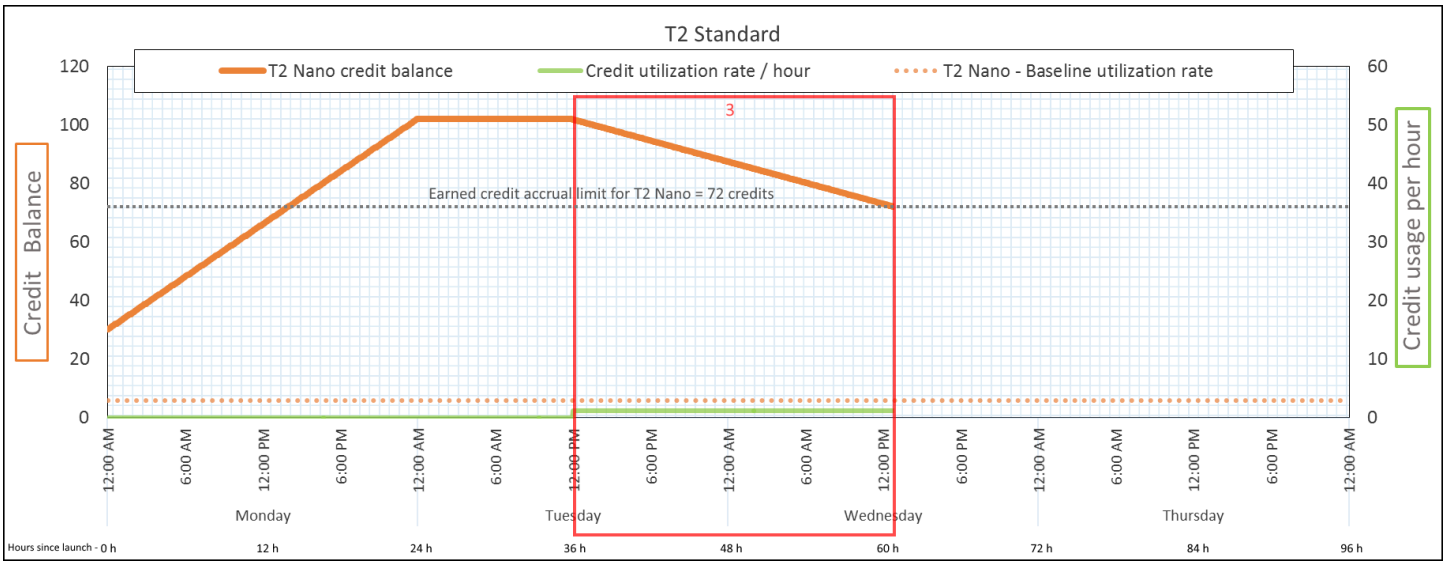
Conclusioni

Un'istanza guadagna costantemente crediti, ma non può accumulare ulteriori crediti guadagnati se il saldo del credito ha raggiunto il suo limite. Una volta che il limite viene raggiunto, i nuovi crediti

guadagnati vengono scartati. I crediti di lancio non contano per il limite del saldo del credito. Se il saldo include crediti di lancio accumulati, il saldo sembra superare il limite.

Periodo 3: 37 – 61 ore

Per le successive 25 ore, l'istanza utilizza il 2% di CPU, cosa che richiede 30 crediti. Nello stesso periodo, guadagna 75 crediti, ma il saldo del credito diminuisce. Il saldo diminuisce perché i crediti di lancio accumulati vengono spesi per primi, mentre i crediti appena guadagnati vengono scartati perché il saldo del credito è già al limite di 72 crediti guadagnati.



Metrica	Valore
Tasso di spesa di crediti	28,8 crediti in 24 ore (1,2 crediti all'ora, 2% di utilizzo della CPU, 40% del tasso di guadagno di crediti) e 30 crediti— in 25 ore
Tasso di guadagno di crediti	72 crediti in 24 ore
Tasso di scarto di crediti	72 crediti in 24 ore (100% del tasso di guadagno di crediti)
Saldo del credito	72 crediti (30 crediti di lancio sono stati spesi, 72 crediti guadagnati rimangono non spesi)

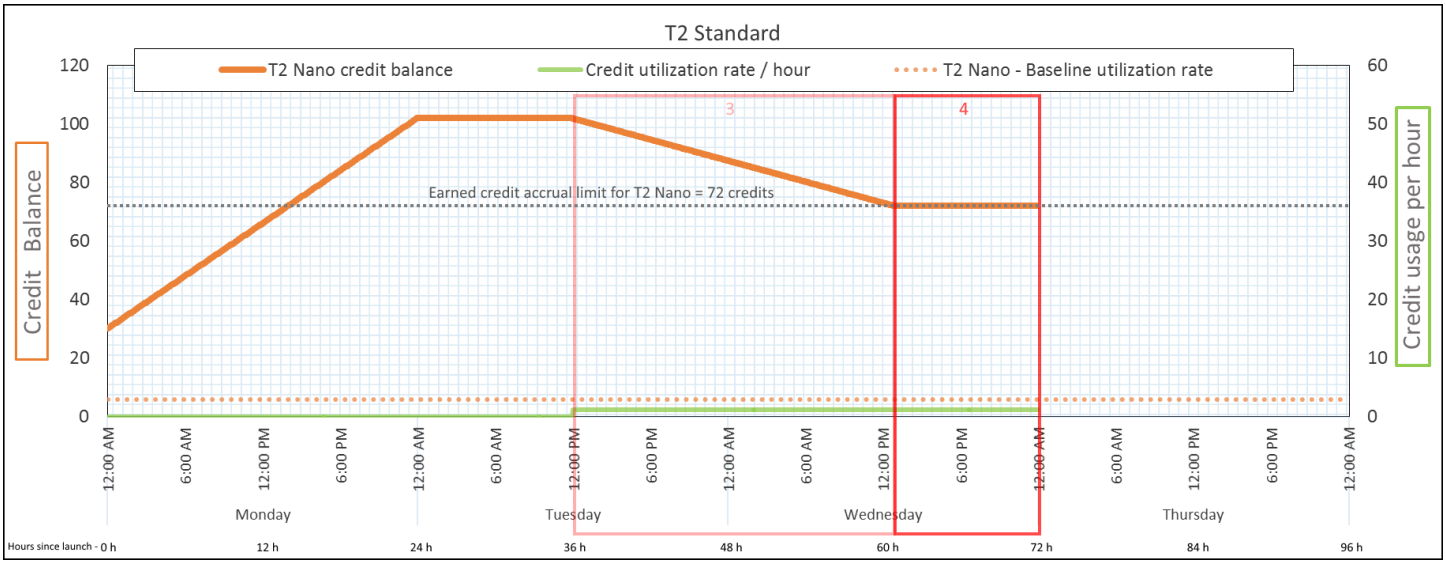
Conclusioni

Un'istanza spende per primi i crediti di lancio, prima dei crediti guadagnati. I crediti di lancio non contano per il limite del credito. Dopo l'avvio, i crediti vengono spesi, il saldo non può mai superare il numero di crediti che si può guadagnare in 24 ore. Inoltre, mentre un'istanza è in esecuzione, non è possibile ottenere più crediti di lancio.

Periodo 4: 62 – 72 ore

Per le successive 11 ore, l'istanza utilizza il 2% di CPU, cosa che richiede 13,2 crediti. Questo è lo stesso utilizzo della CPU del periodo precedente, ma il saldo non diminuisce. Rimane a 72 crediti.

Il saldo non diminuisce perché il tasso di guadagno di crediti è superiore al tasso di spesa di crediti. Nel periodo in cui l'istanza spende 13,2 crediti, guadagna anche 33 crediti. Tuttavia, il limite del saldo è 72 crediti, quindi tutti i crediti guadagnati che superano il limite vengono scartati. Il saldo si stabilizza a 72 crediti, non a 102 crediti durante il periodo 2, perché non sono presenti crediti di lancio accumulati.



Metrica	Valore
Tasso di spesa di crediti	28,8 crediti in 24 ore (1,2 crediti all'ora, 2% di utilizzo della CPU, 40% del tasso di guadagno di crediti) e 13.2— crediti in 11 ore
Tasso di guadagno di crediti	72 crediti in 24 ore
Tasso di scarto di crediti	43,2 crediti in 24 ore (60% del tasso di guadagno di crediti)

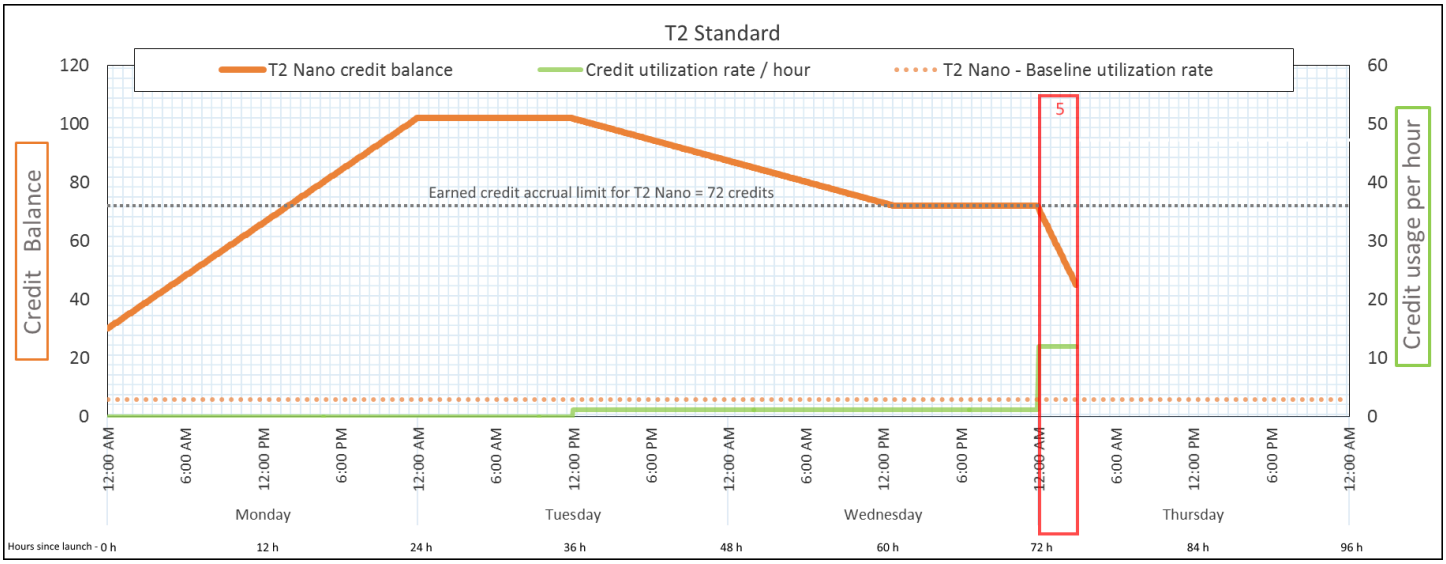
Metrica	Valore
Saldo del credito	72 crediti (0 crediti di lancio + 72 crediti guadagnati), —il saldo è al limite

Conclusioni

Quando i crediti di lancio sono stati spesi, il limite del saldo del credito viene determinato dal numero di crediti che un'istanza può guadagnare in 24 ore. Se l'istanza guadagna più crediti di quelli che spende, i crediti appena guadagnati oltre il limite vengono scartati.

Periodo 5: 73 – 75 ore

Per le successive 3 ore, l'istanza è caratterizzata da picchi al 20% di utilizzo della CPU, cosa che richiede 36 crediti. L'istanza guadagna nove crediti nelle stesse tre ore, il che si traduce in una diminuzione del saldo netto di 27 crediti. Al termine delle tre ore, il saldo del credito è di 45 crediti guadagnati.



Metrica	Valore
Tasso di spesa di crediti	288 crediti in 24 ore (12 crediti all'ora, 20% di utilizzo della CPU, 400% del— tasso di guadagno di crediti) e 36 crediti in 3 ore
Tasso di guadagno di crediti	72 crediti in 24 ore (9 crediti in 3 ore)

Metrica	Valore
Tasso di scarto di crediti	0 crediti in 24 ore
Saldo del credito	45 crediti (saldo precedente (72) - crediti spesi (36) + crediti guadagnati (9)): il saldo diminuisce di 216 crediti ogni 24 ore (tasso di spesa 288/24 + tasso di guadagno 72/24 = tasso di diminuzione del saldo) 216/24

Conclusioni

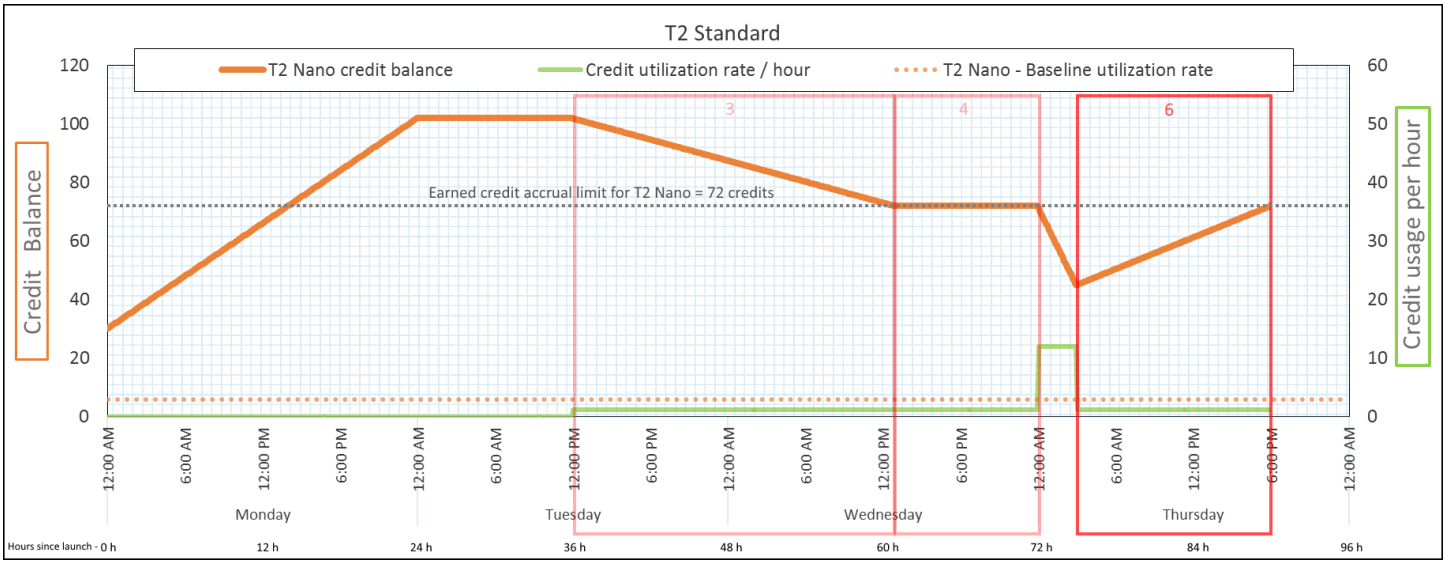
Se un'istanza spende più crediti di quanti ne guadagna, il suo saldo del credito diminuisce.

Periodo 6: 76 – 90 ore

Per le successive 15 ore, l'istanza utilizza il 2% di CPU, cosa che richiede 18 crediti. Questo è lo stesso utilizzo della CPU nei periodi 3 e 4. Tuttavia, il saldo aumenta in questo periodo, mentre è diminuito nel periodo 3 e si è stabilizzato nel periodo 4.

Nel periodo 3, i crediti di lancio accumulati sono stati spesi, mentre i crediti guadagnati che superano il limite del credito vengono scartati, causando una diminuzione del saldo del credito. Nel periodo 4, l'istanza ha speso meno crediti rispetto a quelli guadagnati. Inoltre, i crediti guadagnati che superavano il limite del credito sono stati scartati, quindi il saldo si è stabilizzato al massimo di 72 crediti.

In questo periodo, non sono presenti crediti di lancio accumulati e il numero di crediti guadagnati accumulati nel saldo è inferiore al limite. Nessun credito guadagnato viene scartato. Inoltre, l'istanza guadagna più crediti di quanti ne spende, causando un aumento del credito del saldo.



Metrica	Valore
Tasso di spesa di crediti	28,8 crediti in 24 ore (1,2 crediti all'ora, 2% di utilizzo della CPU, 40% del tasso di guadagno di crediti) e 18 crediti —in 15 ore
Tasso di guadagno di crediti	72 crediti in 24 ore (45 crediti in 15 ore)
Tasso di scarto di crediti	0 crediti in 24 ore
Saldo del credito	72 crediti (il saldo aumenta a un tasso di 43,2 crediti ogni 24 ore, tasso di variazione = tasso di spesa 28. 8/24 + tasso di guadagno) 72/24

Conclusioni

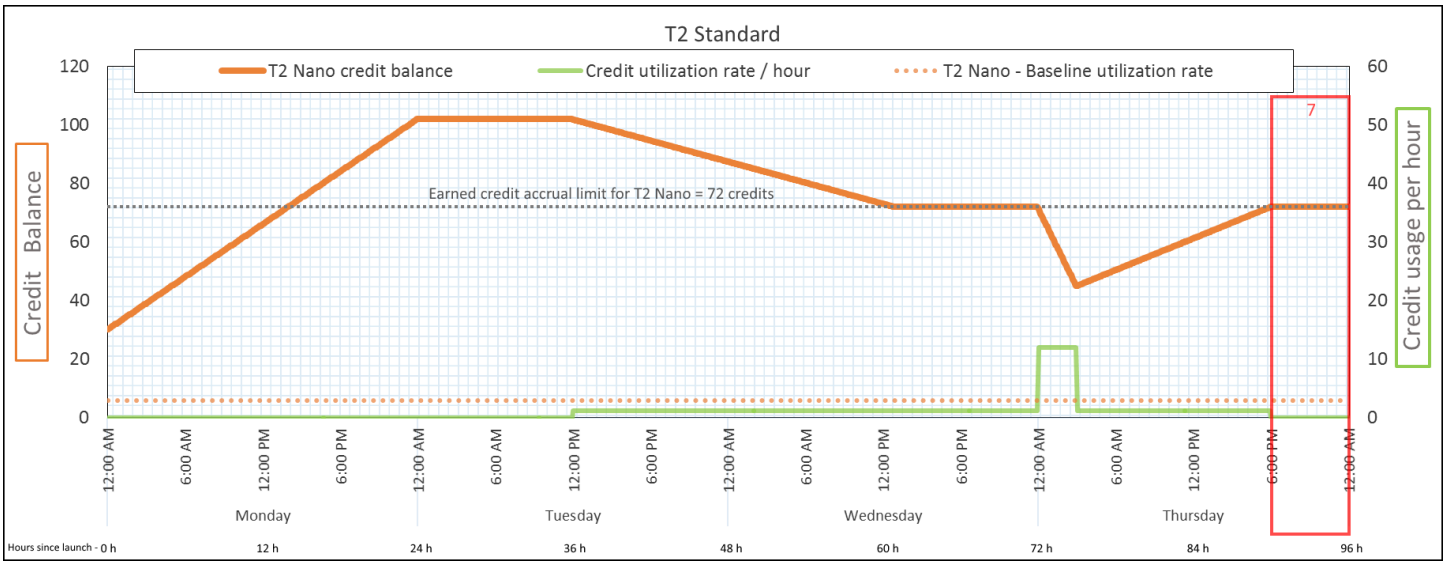
Se un'istanza spende meno crediti di quanti ne guadagna, il suo saldo del credito aumenta.

Periodo 7: 91 – 96 ore

Per le successive sei ore, l'istanza rimane— inattiva (l'utilizzo della CPU è pari allo 0%) e non vengono— spesi crediti. Questo è lo stesso utilizzo della CPU del periodo 2, ma il saldo non si stabilizza a 102 crediti, ma a 72 crediti, che è il limite —di saldo del credito per l'istanza.

Nel periodo 2, il saldo del credito includeva 30 crediti di lancio accumulati. I crediti di lancio sono stati spesi nel periodo 3. Un'istanza in esecuzione non può ottenere più crediti di lancio. Una volta

raggiunto il limite del saldo del credito, tutti i crediti guadagnati che superano il limite vengono scartati.



Metrica	Valore
Tasso di spesa di crediti	0 crediti in 24 ore (0% di utilizzo della CPU)
Tasso di guadagno di crediti	72 crediti in 24 ore
Tasso di scarto di crediti	72 crediti in 24 ore (100% del tasso di guadagno di crediti)
Saldo del credito	72 crediti (0 crediti di lancio, 72 crediti guadagnati)

Conclusioni

Un'istanza guadagna costantemente crediti, ma non può accumulare ulteriori crediti guadagnati se è stato raggiunto il limite del saldo del credito. Una volta che il limite viene raggiunto, i nuovi crediti guadagnati vengono scartati. Il limite del saldo del credito è determinato dal numero di crediti che un'istanza può guadagnare in 24 ore. Per ulteriori informazioni sui limiti del saldo del credito, consulta la tabella del credito.

Configurazione delle istanze a prestazioni espandibili

Le fasi da seguire per avviare, monitorare e modificare le istanze a prestazioni espandibili (istanze T) sono simili. La differenza principale è la specifica crediti predefinita all'avvio delle istanze.

Ogni famiglia di istanze T viene fornita con la seguente specifica di credito predefinita:

- Le istanze T4g, T3a e T3 vengono avviate come `unlimited`
- Le istanze T3 su un host dedicato possono essere avviate come `standard`
- Le istanze T2 vengono avviate come `standard`

È possibile modificare la specifica crediti predefinita per l'account.

Processi

- Configurazione delle specifiche del credito al momento dell'avvio
- Configurare un gruppo Auto Scaling per impostare la specifica del credito come illimitato
- Gestione della specifica del credito di un'istanza a prestazioni espandibili
- Gestione della specifica del credito predefinita per un account

Configurazione delle specifiche del credito al momento dell'avvio

Puoi avviare le tue istanze T con una specifica del credito di `unlimited` o `standard`.

Le procedure seguenti descrivono come utilizzare la console EC2 o la AWS CLI. Per informazioni sull'utilizzo di un gruppo Auto Scaling, consulta Configurare un gruppo Auto Scaling per impostare la specifica del credito come illimitato.

Console

Per configurare la specifica del credito di un'istanza al momento dell'avvio

1. Segui la procedura per avviare un'istanza.
2. In Instance type (Tipo di istanza), seleziona un tipo di istanza T.
3. Espandi Advanced details (Dettagli avanzati). In Specifica del credito, seleziona una specifica del credito.
4. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza).

AWS CLI

Per impostare la specifica del credito di un'istanza al momento dell'avvio

Utilizza il comando run-instances con l'opzione `--credit-specification`.

```
--credit-specification CpuCredits=unlimited
```

PowerShell

Per impostare la specifica del credito di un'istanza al momento dell'avvio

Utilizzare il New-EC2Instance cmdlet con il `-CreditSpecification_CpuCredit` parametro.

```
-CreditSpecification_CpuCredit unlimited
```

Configurare un gruppo Auto Scaling per impostare la specifica del credito come illimitato

Quando vengono avviate le istanze T, per una buona esperienza del processo di bootstrap richiedono crediti CPU. Se viene utilizzato un gruppo Auto Scaling per avviare le istanze, è consigliabile configurare le istanze come `unlimited`. In questo modo, le istanze utilizzeranno i crediti extra quando vengono avviate o riavviate automaticamente dal gruppo Auto Scaling. L'uso di crediti extra previene le limitazioni di prestazioni.

Creazione di un modello di avvio

È necessario utilizzare un modello di avvio per avviare le istanze come `unlimited` in un gruppo Auto Scaling. Una configurazione di lancio non supporta il lancio di istanze come `unlimited`.

Console

Per creare un modello di avvio che imposti le specifiche del credito

1. Seguire la procedura Creazione di un modello di avvio con impostazioni avanzate nella Guida per l'utente di Amazon EC2 Auto Scaling.
2. In Launch template contents (Contenuti modello di avvio), per Instance type (Tipo di istanza), scegliere una dimensione di istanza.
3. Per avviare le istanze come `unlimited` in un gruppo Auto Scaling, in Advanced details (Dettagli avanzati), per Credit specification (Specifica credito), scegliere Unlimited (Illimitato).

4. Una volta definiti i parametri del modello di avvio, scegliere Create launch template (Crea modello di avvio).

AWS CLI

Per creare un modello di avvio che imposti le specifiche del credito

Utilizzare il comando create-launch-template.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --version-description FirstVersion \
    --launch-template-data CreditSpecification={CpuCredits=unlimited}
```

PowerShell

Per creare un modello di avvio che imposti le specifiche del credito

Utilizza il cmdlet New-EC2LaunchTemplate. Definisci le specifiche del credito per i dati del modello di avvio come segue.

```
$creditSpec = New-Object Amazon.EC2.Model.CreditSpecificationRequest
$creditSpec.CpuCredits = "unlimited"
$launchTemplateData = New-Object Amazon.EC2.Model.RequestLaunchTemplateData
$launchTemplateData.CreditSpecification = $creditSpec
```

Associazione di un gruppo Auto Scaling a un modello di avvio

Per associare il modello di avvio a un gruppo Auto Scaling occorre creare il gruppo Auto Scaling utilizzando il modello di avvio o aggiungere il modello di avvio a un gruppo Auto Scaling esistente.

Console

Come creare un gruppo con scalabilità automatica utilizzando un modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Sulla barra di navigazione nella parte superiore della schermata, selezionare la stessa regione utilizzata durante la creazione del modello di avvio.

3. Nel riquadro di navigazione, selezionare Groups (Gruppi Auto Scaling), Create group (Crea gruppo Auto Scaling).
4. Scegliere Modello di avvio, selezionare il modello di avvio, quindi scegliere Fase successiva.
5. Compilare i campi per il gruppo Auto Scaling. Dopo aver esaminato le impostazioni di configurazione in Review page (Pagina di revisione), scegliere Create Auto Scaling group (Crea gruppo Auto Scaling). Per ulteriori informazioni, consulta la sezione relativa alla creazione di un gruppo Auto Scaling utilizzando un modello di avvio della Guida per l'utente di Amazon EC2 Auto Scaling.

Come aggiungere un modello di avvio a un gruppo con scalabilità automatica esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Sulla barra di navigazione nella parte superiore della schermata, selezionare la stessa regione utilizzata durante la creazione del modello di avvio.
3. Nel riquadro di navigazione, selezionare Groups (Gruppi Auto Scaling).
4. Nell'elenco dei gruppi Auto Scaling, selezionare un gruppo Auto Scaling e scegliere Actions (Operazioni), Edit (Modifica).
5. Nella scheda Dettagli, per Modello di avvio, scegliere un modello di avvio, quindi scegliere Salva.

AWS CLI

Come creare un gruppo con scalabilità automatica utilizzando un modello di avvio

Utilizza il comando create-auto-scaling-group e specifica il parametro `--launch-template`.

Come aggiungere un modello di avvio a un gruppo con scalabilità automatica esistente

Utilizza il comando update-auto-scaling-group e specifica il parametro `--launch-template`.

PowerShell

Come creare un gruppo con scalabilità automatica utilizzando un modello di avvio

Utilizzare il New-ASAutoScalingGroup cmdlet e specificare il `-LaunchTemplate_LaunchTemplateId` parametro or. `-LaunchTemplate_LaunchTemplateName`

Come aggiungere un modello di avvio a un gruppo con scalabilità automatica esistente

Utilizzare il Update-ASAutoScalingGroup cmdlet e specificare il parametro or. `-LaunchTemplate_LaunchTemplateId -LaunchTemplate_LaunchTemplateName`

Gestione della specifica del credito di un'istanza a prestazioni espandibili

È possibile cambiare la specifica crediti di un'istanza T in esecuzione o interrotta in qualsiasi momento da `unlimited` a `standard` e viceversa.

Tieni presente che in modalità `unlimited`, un'istanza può spendere crediti extra, il che potrebbe comportare un costo aggiuntivo. Per ulteriori informazioni, consulta Possibilità di addebito dei costi per i crediti extra.

Console

Per gestire la specifica del credito di un'istanza T

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Istanze.
3. (Facoltativo) Seleziona un'istanza. Nella scheda Dettagli, trova Specifica del credito. Il valore è `unlimited` o `standard`.
4. (Facoltativo) Per modificare la specifica del credito per diverse istanze contemporaneamente, selezionale tutte.
5. Scegliere Actions (Operazioni), Instance settings (Impostazioni istanza), Change credit specification (Modifica specifica credito). Questa opzione è abilitata solo se è stata selezionata un'istanza T.
6. In Modalità Illimitata, seleziona o deseleziona la casella di controllo accanto all'ID di ogni istanza.

AWS CLI

Per visualizzare la specifica del credito di un'istanza T

Utilizzare il comando describe-instance-credit-specifications. Se non specifichi un ID istanza, vengono restituite tutte le istanze con specifica del credito `unlimited`. L'output includerebbe anche le istanze precedentemente configurate con la specifica del credito `unlimited`. Ad esempio, se un'istanza T3 viene ridimensionata in un'istanza M4 mentre è configurata come `unlimited`, Amazon EC2 restituisce l'istanza M4.

```
aws ec2 describe-instance-credit-specifications \
    --instance-id i-1234567890abcdef0 \
    --query InstanceCreditSpecifications[].CpuCredits \
    --output text
```

Di seguito è riportato un output di esempio.

```
unlimited
```

Per impostare la specifica del credito di un'istanza T

Utilizzare il comando modify-instance-credit-specification.

```
aws ec2 modify-instance-credit-specification \
    --region us-east-1 \
    --instance-credit-specification
 "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

PowerShell

Per visualizzare la specifica del credito di un'istanza T

Utilizza il cmdlet Get-EC2CreditSpecification.

```
(Get-EC2CreditSpecification `
    -InstanceId i-1234567890abcdef0).CpuCredits
```

Di seguito è riportato un output di esempio.

```
unlimited
```

Per impostare la specifica del credito di un'istanza T

Utilizza il cmdlet Edit-EC2InstanceCreditSpecification.

```
Edit-EC2InstanceCreditSpecification `
    -Region us-east-1 `
    -InstanceCreditSpecification @({InstanceId="i-1234567890abcdef0"
 CpuCredits="unlimited"})
```

Gestione della specifica del credito predefinita per un account

Ogni famiglia di istanze T viene fornita con una specifica di credito predefinita. È possibile modificare la specifica di credito predefinita per ogni famiglia di istanze T a livello di account per regione. AWS I valori validi per la specifica del credito predefinita sono `unlimited` e `standard`.

Se utilizzi la procedura guidata di avvio istanze nella console EC2 per avviare le istanze, il valore selezionato per la specifica del credito sostituisce la specifica crediti predefinita a livello di account. Se utilizzi AWS CLI to launch istances, tutte le nuove istanze T presenti nell'account vengono avviate utilizzando la specifica di credito predefinita. La specifica crediti per le istanze esistenti in esecuzione o arrestate non è interessata.

Considerazione

La specifica crediti predefinita per una famiglia di istanze può essere modificata solo una volta in un periodo di 5 minuti e fino a quattro volte in un periodo di 24 ore.

Console

Per gestire la specifica del credito predefinita

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Per modificare il Regione AWS, usa il selettore di regione nell'angolo in alto a destra della pagina.
3. Nel pannello di navigazione seleziona Pannello di controllo.
4. Nella scheda Attributi dell'account, in Impostazioni, scegli Specifica del credito predefinita.
5. Scegliere Gestisci.
6. Per ogni famiglia di istanze, scegliere Unlimited (Illimitato) o Standard (Standard), quindi scegliere Update (Aggiorna).

AWS CLI

Per ottenere la specifica del credito predefinita

Utilizzare il comando get-default-credit-specification.

```
aws ec2 get-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
```

```
    --query InstanceFamilyCreditSpecifications[].CpuCredits \
    --output text
```

Di seguito è riportato un output di esempio.

```
standard
```

Per impostare la specifica del credito predefinita

Utilizzare il comando modify-default-credit-specification. L'esempio seguente imposta il valore su `unlimited`.

```
aws ec2 modify-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --cpu-credits unlimited
```

PowerShell

Per ottenere la specifica del credito predefinita

Utilizza il cmdlet Get-EC2DefaultCreditSpecification.

```
(Get-EC2DefaultCreditSpecification `
    -Region us-east-1 `
    -InstanceFamily t2).CpuCredits
```

Di seguito è riportato un output di esempio.

```
standard
```

Per impostare la specifica del credito predefinita

Utilizza il cmdlet Edit-EC2DefaultCreditSpecification. L'esempio seguente imposta il valore su `unlimited`.

```
Edit-EC2DefaultCreditSpecification `
    -Region us-east-1 `
    -InstanceFamily t2 `
    -CpuCredit unlimited
```

Monitoraggio dei crediti CPU per istanze espandibili

EC2 invia le metriche ad Amazon. CloudWatch Puoi visualizzare le metriche relative al credito della CPU nelle metriche per istanza di Amazon EC2 della CloudWatch console o utilizzando questa opzione per elencare le metriche AWS CLI per ogni istanza. Per ulteriori informazioni, consulta CloudWatch metriche disponibili per le tue istanze.

Indice

- Metriche aggiuntive per istanze con prestazioni straordinarie CloudWatch
- Calcolo dell'utilizzo dei crediti CPU

Metriche aggiuntive per istanze con prestazioni straordinarie CloudWatch

Le istanze Burstable Performance hanno queste CloudWatch metriche aggiuntive, che vengono aggiornate ogni cinque minuti:

- `CPUCreditUsage` – Il numero di crediti CPU spesi durante il periodo di misurazione.
- `CPUCreditBalance` - Il numero di– crediti CPU accumulati da un'istanza. Questo saldo è esaurito quando la CPU ottimizza le prestazioni e i crediti CPU vengono spesi più rapidamente di quanto guadagnati.
- `CPUSurplusCreditBalance` – Il numero di crediti CPU extra spesi per sostenere l'utilizzo della CPU quando il valore `CPUCreditBalance` è zero.
- `CPUSurplusCreditsCharged` – Il numero di crediti CPU extra che supera il numero massimo di crediti della CPU che un'istanza può guadagnare in un periodo di 24 ore e che può quindi implicare costi aggiuntivi.

Gli ultimi due parametri si applicano solo alle istanze configurate come `unlimited`.

La tabella seguente descrive le CloudWatch metriche per le istanze di prestazioni burstable. Per ulteriori informazioni, consulta CloudWatch metriche disponibili per le tue istanze.

Parametro	Descrizione
`CPUCreditUsage`	Il numero di crediti CPU spesi dall'istanza per l'utilizzo della CPU. Un credito CPU equivale a un vCPU che viene eseguito al 100% dell'utilizzo per un minuto o una combinazione equivalen te di vCPU, utilizzo e tempo (per esempio, un vCPU che viene

Parametro	Descrizione
	eseguito al 50% dell'utilizzo per due minuti o due vCPU che vengono eseguiti al 25% dell'utilizzo per due minuti). I parametri di credito CPU sono disponibili solo con una frequenza di 5 minuti. Se specifichi un periodo superiore a 5 minuti, usa la statistica `Sum` al posto di quella `Average`. Unità: crediti (v) CPU-minutes
`CPUCreditBalance`	Il numero di crediti CPU ottenuti, che un'istanza ha accumulato o da quando è stata lanciata o avviata. Per le T2 Standard `CPUCreditBalance` include anche il numero di crediti di lancio che sono stati accumulati. I crediti vengono accumulati nel saldo del credito dopo che sono stati ottenuti e rimossi dal saldo del credito una volta spesi. Il saldo del credito ha un limite massimo, determinato dalla dimensione dell'istanza. Una volta che il limite viene raggiunto, tutti i nuovi crediti guadagnati vengono scartati. Per le T2 Standard, i crediti di lancio non contano per il limite. I crediti in `CPUCreditBalance` sono disponibili affinché l'istanza li spenda per andare oltre l'utilizzo di base della CPU. Quando l'istanza è in fase di esecuzione, i crediti in `CPUCreditBalance` non scadono. Quando un'istanza T4g, T3a o T3 viene arrestata, il valore `CPUCreditBalance` viene conservato per sette giorni. Successivamente, tutti i crediti accumulati vengono persi. Quando un'istanza T2 si arresta, il valore `CPUCreditBalance` non persiste e tutti i crediti accumulati vengono persi. I parametri di credito CPU sono disponibili solo con una frequenza di 5 minuti. Unità: Crediti (vCPU-minutes)

Parametro	Descrizione
`CPUSurplusCreditBalance`	Il numero di crediti extra spesi da un'istanza `unlimited` quando il rispettivo valore `CPUCreditBalance` è pari a zero. Il valore `CPUSurplusCreditBalance` viene saldato con i crediti CPU ottenuti. Se il numero dei crediti extra va oltre il numero massimo di crediti che un'istanza può ottenere in un periodo di 24 ore, i crediti extra spesi, eccedenti il limite, incorreranno in costi aggiuntivi. Unità: Crediti (vCPU-minutes)
`CPUSurplusCreditsCharged`	Il numero di crediti extra spesi da un'istanza, che non sono saldati con i crediti CPU ottenuti e che pertanto incorrono in costi aggiuntivi. I crediti extra spesi subiscono costi aggiuntivi quando si verifica uno dei seguenti casi: • I crediti extra spesi vanno oltre il numero massimo di crediti che un'istanza può ottenere in un periodo di 24 ore. I crediti extra spesi, che eccedono il limite, subiscono costi aggiuntivi alla fine dell'ora; • l'istanza viene arrestata o terminata; • l'istanza passa da `unlimited` a `standard`. Unità: Crediti (vCPU-minutes)

Calcolo dell'utilizzo dei crediti CPU

L'utilizzo dei crediti CPU delle istanze viene calcolato utilizzando le CloudWatch metriche delle istanze descritte nella tabella precedente.

Amazon EC2 invia le metriche ogni cinque minuti. CloudWatch Un riferimento a un valore precedente di un parametro in qualsiasi momento implica il valore precedente del parametro inviato cinque minuti fa.

Calcolo dell'utilizzo dei crediti CPU per istanze standard

- Il saldo dei crediti della CPU aumenta se l'utilizzo della CPU è inferiore alla baseline, quando i crediti spesi sono meno dei crediti guadagnati nell'intervallo precedente di cinque minuti.
- Il saldo dei crediti della CPU diminuisce se l'utilizzo della CPU è superiore alla baseline, quando i crediti spesi sono più dei crediti guadagnati nell'intervallo precedente di cinque minuti.

La seguente equazione rappresenta matematicamente questa operazione:

Example

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -
 CPUCreditUsage]
```

La dimensione dell'istanza determina il numero di crediti che l'istanza può guadagnare all'ora e il numero di crediti guadagnati che può accumulare nel saldo del credito. Per ulteriori informazioni sul numero di crediti guadagnati all'ora e sul limite del saldo del credito per ogni dimensione di istanza, consulta la tabella del credito.

Esempio

In questo esempio viene utilizzata l'istanza `t3.nano`. Per calcolare il valore `CPUCreditBalance` dell'istanza, utilizzare l'equazione precedente come segue:

- `CPUCreditBalance` – L'attuale saldo del credito da calcolare.
- `prior CPUCreditBalance` – Il saldo del credito di cinque minuti fa. In questo esempio, un'istanza ha accumulato due crediti.
- `Credits earned per hour` – Un'istanza `t3.nano` guadagna sei crediti all'ora.
- `5/60`— Rappresenta l'intervallo di cinque minuti tra CloudWatch la pubblicazione delle metriche. Moltiplica i crediti guadagnati all'ora per 5/60 (cinque minuti) per ottenere il numero di crediti guadagnati dall'istanza negli ultimi cinque minuti. Un'istanza `t3.nano` guadagna 0,5 crediti ogni cinque minuti.
- `CPUCreditUsage` – Quanti crediti sono stati spesi dall'istanza negli ultimi cinque minuti. In questo esempio, l'istanza ha speso un credito negli ultimi cinque minuti.

Con questi valori, è possibile calcolare il valore `CPUCreditBalance`:

Example

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

Calcolo dell'utilizzo dei crediti CPU per istanze in modalità illimitata

Quando un'istanza di prestazioni espandibile deve superare la baseline, spende sempre i crediti accumulati prima di spendere crediti extra. Quando esaurisce il suo saldo di credito CPU accumulato, può spendere i crediti extra per espandere la CPU finché necessario. Quando l'utilizzo della CPU è inferiore alla baseline, i crediti extra vengono sempre pagati prima che l'istanza accumuli crediti guadagnati.

Utilizziamo il termine `Adjusted balance` nelle seguenti equazioni per riflettere l'attività che si verifica in questo intervallo di cinque minuti. Utilizziamo questo valore per ottenere i valori delle `CPUSurplusCreditBalance` CloudWatch metriche `CPUCreditBalance` e.

Example

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits
 earned per hour * (5/60) - CPUCreditUsage]
```

Un valore di `0` per `Adjusted balance` indica che l'istanza ha speso tutti i suoi crediti guadagnati per l'ottimizzazione e non sono stati spesi crediti extra. Di conseguenza, sia `CPUCreditBalance` sia `CPUSurplusCreditBalance` sono impostati su `0`.

Un valore `Adjusted balance` positivo indica che i crediti guadagnati accumulati dall'istanza e i precedenti crediti extra, se presenti, sono stati pagati. Di conseguenza, il valore `Adjusted balance` è assegnato a `CPUCreditBalance` e il `CPUSurplusCreditBalance` è impostato su `0`. Le dimensioni dell'istanza determinano il numero massimo di crediti che può accumulare.

Example

```
CPUCreditBalance = min [max earned credit balance, Adjusted balance]
CPUSurplusCreditBalance = 0
```

Un valore `Adjusted balance` negativo indica che l'istanza ha speso tutti i suoi crediti guadagnati che ha accumulato e, inoltre, ha anche speso crediti extra per l'ottimizzazione. Di conseguenza, il valore `Adjusted balance` viene assegnato a `CPUSurplusCreditBalance` e `CPUCreditBalance` è impostato su `0`. Anche in questo caso, le dimensioni dell'istanza determinano il numero massimo di crediti che può accumulare.

Example

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]
CPUCreditBalance = 0
```

Se i crediti extra spesi superano il numero massimo di crediti che un'istanza può accumulare, il saldo del credito extra è impostato al massimo, come mostrato nell'equazione precedente. I restanti crediti extra sono addebitati come rappresentato dal parametro `CPUSurplusCreditsCharged`.

Example

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

Infine, quando l'istanza termina, vengono addebitati eventuali crediti extra monitorati dal `CPUSurplusCreditBalance`. Se l'istanza passa da `unlimited` a `standard`, viene addebitato anche qualsiasi `CPUSurplusCreditBalance` restante.

Accelerazione delle prestazioni con istanze GPU

GPU-based le istanze forniscono l'accesso alle GPU NVIDIA con migliaia di core di elaborazione. Puoi utilizzare queste istanze per accelerare le applicazioni scientifiche, tecniche e di rendering sfruttando i framework di elaborazione in parallelo CUDA o Open Computing Language (OpenCL). Puoi utilizzarle anche per le applicazioni grafiche, inclusi i giochi e le applicazioni 3D in streaming e altri carichi di lavoro grafici.

Prima di poter attivare o ottimizzare un' GPU-based istanza, è necessario installare i driver appropriati, come segue:

- Per installare i driver NVIDIA su un'istanza con una GPU NVIDIA collegata, ad esempio un'istanza P3 o G4dn, consulta Driver NVIDIA.
- Per installare i driver AMD su un'istanza con una GPU AMD collegata, ad esempio un'istanza G4ad, consulta Driver AMD.

Indice

- Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze Amazon EC2 GPU-based
- Ottimizza le impostazioni GPU sulle istanze Amazon EC2
- Impostazione di display Dual 4K su istanze G4ad Linux
- Inizia a utilizzare le istanze con accelerazione GPU

Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze Amazon EC2 GPU-based

Per attivare le applicazioni virtuali GRID su GPU-based istanze dotate di GPU NVIDIA (NVIDIA GRID Virtual Workstation è abilitata per impostazione predefinita), devi definire il tipo di prodotto per il driver. Il processo utilizzato dipende dal sistema operativo dell'istanza.

Istanze Linux

Per attivare le applicazioni GRID Virtual sulle istanze Linux

1. Creare il file `/etc/nvidia/gridd.conf` a partire dal file modello fornito.

   ```
   [ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
   ```

2. Aprire il file `/etc/nvidia/gridd.conf` nell'editor di testo preferito.
3. Trova la riga `FeatureType` e impostala uguale a `0`. quindi aggiungere una riga con `IgnoreSP=TRUE`.

   ```
   FeatureType=0 IgnoreSP=TRUE
   ```

4. Salvare il file e uscire.
5. Riavviare l'istanza per rendere effettiva la nuova configurazione.

   ```
   [ec2-user ~]$ sudo reboot
   ```

Istanze Windows

Per attivare le applicazioni GRID Virtual sulle istanze Windows

1. Eseguire regedit.exe per aprire l'editor del registro.
2. Accedere a `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global\GridLicensing`.
3. Aprire il menu contestuale (pulsante destro del mouse) nel riquadro a destra e scegliere New (Nuovo), DWORD.
4. Per Nome, inserisci e digita. FeatureType `Enter`
5. Apri il menu contestuale (clic con il pulsante destro del mouse) FeatureType e scegli Modifica.
6. Per Value data (Dati valore), digitare `0` per le applicazioni NVIDIA GRID Virtual e scegliere OK.

7. Aprire il menu contestuale (pulsante destro del mouse) nel riquadro a destra e scegliere New (Nuovo), DWORD.
8. Per Name (Nome), inserire IgnoreSP e digitare `Enter`.
9. Aprire il menu contestuale (pulsante destro del mouse) su IgnoreSP e scegliere Modify (Modifica).
10. Per Value data (Dati valore), digitare 1 e scegliere OK.
11. Chiudere l'editor del Registro di sistema.

Ottimizza le impostazioni GPU sulle istanze Amazon EC2

Esistono molte ottimizzazioni delle impostazioni GPU che puoi effettuare per raggiungere le prestazioni ottimali sulle istanze NVIDIA GPU. Con alcuni di questi tipi di istanze, il driver NVIDIA utilizza una funzione autoboost, che varia le velocità di clock della GPU. Disattivando l'autoboost e impostando le velocità di clock delle GPU sulla loro frequenza massima è possibile ottenere prestazioni ottimali costanti delle istanze GPU.

Ottimizza le impostazioni GPU su Linux

1. Configurare le impostazioni GPU per renderle persistenti. L'esecuzione di questo comando può richiedere diversi minuti.

   ```
   [ec2-user ~]$ sudo nvidia-persistenced
   ```

2. [Solo istanze G3] Disabilita la funzione autoboost per tutte le GPU sull'istanza.

   ```
   [ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
   ```

3. Impostare tutte le velocità di clock delle GPU sulla frequenza massima. Utilizzare le velocità di clock di memoria e grafica specificate nei comandi seguenti.

   Alcune versioni del driver NVIDIA non supportano l'impostazione della velocità di clock dell'applicazione e visualizzano l'errore `"Setting applications clocks is not supported for GPU..."`, che può essere ignorato.

   - Istanze G3:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
     ```

   - Istanze G4dn:

```
[ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
```

- Istanze G5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 6250,1710
```

- Istanze G6, G6f, Gr6 e Gr6f:

```
[ec2-user ~]$ sudo nvidia-smi -ac 6251,2040
```

- Istanze G6e:

```
[ec2-user ~]$ sudo nvidia-smi -ac 9001,2520
```

- Istanze G7e:

```
[ec2-user ~]$ sudo nvidia-smi -ac 12481,2430
```

- Istanze G7:

```
[ec2-user ~]$ sudo nvidia-smi -ac 12501,2415
```

- Istanze P3 e P3dn:

```
[ec2-user ~]$ sudo nvidia-smi -ac 877,1530
```

- Istanze P4d:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

- Istanze P4de:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- Istanze P5:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

- Istanze P5e e P5en:

```
[ec2-user ~]$ sudo nvidia-smi -ac 3201,1980
```

- P6-B200 istanze:

```
[ec2-user ~]$ sudo nvidia-smi -ac 3996,1965
```

- P6-B300 istanze:

```
[ec2-user ~]$ sudo nvidia-smi -ac 3996,2032
```

Ottimizza le impostazioni GPU su Windows

1. Apri una PowerShell finestra e vai alla cartella di installazione di NVIDIA.

```
PS C:\> cd "C:\Windows\System32\DriverStore\FileRepository\nvgridsw_aws.inf_*\"
```

2. [Solo istanze G3] Disabilita la funzione autoboost per tutte le GPU sull'istanza.

```
PS C:\> .\nvidia-smi --auto-boost-default=0
```

3. Impostare tutte le velocità di clock delle GPU sulla frequenza massima. Utilizzare le velocità di clock di memoria e grafica specificate nei comandi seguenti.

   Alcune versioni del driver NVIDIA non supportano l'impostazione della velocità di clock dell'applicazione e visualizzano l'errore `"Setting applications clocks is not supported for GPU..."`, che può essere ignorato.

   - Istanze G3:

```
PS C:\> .\nvidia-smi -ac "2505,1177"
```

   - Istanze G4dn:

```
PS C:\> .\nvidia-smi -ac "5001,1590"
```

   - Istanze G5:

```
PS C:\> .\nvidia-smi -ac "6250,1710"
```

- Istanze G6, G6f, Gr6 e Gr6f:

```
PS C:\> .\nvidia-smi -ac "6251,2040"
```

- Istanze G6e:

```
PS C:\> .\nvidia-smi -ac "9001,2520"
```

- Istanze P3 e P3dn:

```
PS C:\> .\nvidia-smi -ac "877,1530"
```

Impostazione di display Dual 4K su istanze G4ad Linux

Dopo aver avviato un'istanza G4ad, puoi impostare display Dual 4K.

Per installare i driver AMD e configurare doppi schermi

1. Collegati alla tua istanza di Linux per ottenere l'indirizzo del bus PCI della GPU da come destinazione per il doppio 4K (2×4k):

   ```
   lspci -vv | grep -i amd
   ```

   Otterrai un output simile al seguente:

   ```
   00:1e.0 Display controller: Advanced Micro Devices, Inc. [*AMD*/ATI] Device 7362 (rev
    c3)
   Subsystem: Advanced Micro Devices, Inc. [AMD/ATI] Device 0a34
   ```

2. Tieni presente che l'indirizzo del bus PCI nell'output precedente è 00:1e.0. Crea un file denominato `/etc/modprobe.d/amdgpu.conf` e aggiungi:

   ```
   options amdgpu virtual_display=0000:00:1e.0,2
   ```

3. Per installare i driver AMD su Linux, consulta Driver AMD per la tua istanza EC2. Se hai già installato il driver AMD della GPU, occorrerà rigenerare i moduli del kernel amdgpu tramite dkms.
4. Utilizza il file xorg.conf seguente per definire la topologia dello schermo doppio (2×4K) e salva il file in `/etc/X11/xorg.conf`:

```
~$ cat /etc/X11/xorg.conf
Section "ServerLayout"
    Identifier     "Layout0"
    Screen          0 "Screen0"
    Screen        1 "Screen1"
    InputDevice     "Keyboard0" "CoreKeyboard"
    InputDevice     "Mouse0" "CorePointer"
    Option          "Xinerama" "1"
EndSection
Section "Files"
    ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath "/opt/amdgpu/lib/xorg/modules"
    ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
    ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
    ModulePath "/usr/lib64/xorg/modules"
    ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Mouse0"
    Driver         "mouse"
    Option         "Protocol" "auto"
    Option         "Device" "/dev/psaux"
    Option         "Emulate3Buttons" "no"
    Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Keyboard0"
    Driver         "kbd"
EndSection

Section "Monitor"
    Identifier     "Virtual"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "Primary" "true"
EndSection

Section "Monitor"
    Identifier     "Virtual-1"
    VendorName     "Unknown"
    ModelName      "Unknown"
```

```
    Option         "RightOf" "Virtual"
EndSection

Section "Device"
    Identifier     "Device0"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Device"
    Identifier     "Device1"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Extensions"
    Option         "DPMS" "Disable"
EndSection

Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection

Section "Screen"
    Identifier     "Screen1"
    Device         "Device1"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
```

```
    EndSubSection
EndSection
```

5. Configura DCV seguendo le istruzioni nella configurazione di un desktop interattivo.
6. Una volta completata la configurazione di DCV, riavvia.
7. Controlla se il driver funziona:

```
dmesg | grep amdgpu
```

   La risposta dovrebbe essere simile alla seguente:

```
Initialized amdgpu
```

8. Dovresti vedere nell'output per`DISPLAY=:0 xrandr -q`a cui sono collegati 2 display virtuali:

```
~$ DISPLAY=:0 xrandr -q
Screen 0: minimum 320 x 200, current 3840 x 1080, maximum 16384 x 16384
Virtual connected primary 1920x1080+0+0 (normal left inverted right x axis y axis)
 0mm x 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
 640x480  59.94 59.94
Virtual-1 connected 1920x1080+1920+0 (normal left inverted right x axis y axis) 0mm x
 0mm
```

```
  4096x3112  60.00
  3656x2664  59.99
  4096x2160  60.00
  3840x2160  60.00
  1920x1200  59.95
  1920x1080  60.00
  1600x1200  59.95
  1680x1050  60.00
  1400x1050  60.00
  1280x1024  59.95
  1440x900 59.99
  1280x960 59.99
  1280x854 59.95
  1280x800 59.96
  1280x720 59.97
  1152x768 59.95
  1024x768 60.00 59.95
  800x600  60.32 59.96 56.25
  848x480  60.00 59.94
  720x480  59.94
640x480  59.94 59.94
```

9. Quando ti colleghi in DCV, modifica la risoluzione su 2×4K, confermando che il supporto per due monitor è registrato da DCV.



Configurare un desktop interattivo per Linux

Dopo aver confermato che il driver della GPU AMD è stato installato sull'istanza Linux e che amdgpu è in uso, è possibile installare un desktop manager interattivo. Si consiglia l'ambiente desktop MATE per la massima garanzia in termini di compatibilità e prestazioni.

Prerequisito

Aprire un editor di testo e salvare quanto segue come file denominato `xorg.conf`. Questo file sarà necessario sull'istanza.

```
Section "ServerLayout"
Identifier     "Layout0"
Screen          0 "Screen0"
```

```
InputDevice     "Keyboard0" "CoreKeyboard"
InputDevice     "Mouse0" "CorePointer"
EndSection
Section "Files"
ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
ModulePath "/opt/amdgpu/lib/xorg/modules"
ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
ModulePath "/usr/lib64/xorg/modules"
ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Mouse0"
Driver         "mouse"
Option         "Protocol" "auto"
Option         "Device" "/dev/psaux"
Option         "Emulate3Buttons" "no"
Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Keyboard0"
Driver         "kbd"
EndSection
Section "Monitor"
Identifier     "Monitor0"
VendorName     "Unknown"
ModelName      "Unknown"
EndSection
Section "Device"
Identifier     "Device0"
Driver         "amdgpu"
VendorName     "AMD"
BoardName      "Radeon MxGPU V520"
BusID          "PCI:0:30:0"
EndSection
Section "Extensions"
Option         "DPMS" "Disable"
EndSection
Section "Screen"
Identifier     "Screen0"
Device         "Device0"
Monitor        "Monitor0"
```

```
DefaultDepth   24
Option         "AllowEmptyInitialConfiguration" "True"
SubSection "Display"
    Virtual    3840 2160
    Depth      32
EndSubSection
EndSection
```

Per configurare un desktop interattivo su Amazon Linux 2

1. Installare l'archivio EPEL.

   ```
   [ec2-user ~]$ sudo amazon-linux-extras install epel -y
   ```

2. Installare il desktop MATE.

   ```
   [ec2-user ~]$ sudo amazon-linux-extras install mate-desktop1.x -y
   [ec2-user ~]$ sudo yum groupinstall "MATE Desktop" -y
   [ec2-user ~]$ sudo systemctl disable firewalld
   ```

3. Copiare il file `xorg.conf` su `/etc/X11/xorg.conf`.
4. Riavviare l'istanza.

   ```
   [ec2-user ~]$ sudo reboot
   ```

5. (Facoltativo) Installare il server Amazon DCV per utilizzare Amazon DCV come protocollo di visualizzazione ad alte prestazioni, quindi connettersi a una sessione Amazon DCV utilizzando il client preferito.

Per configurare un desktop interattivo su Ubuntu

1. Installare il desktop MATE.

   ```
   $ sudo apt install xorg-dev ubuntu-mate-desktop -y
   $ sudo apt purge ifupdown -y
   ```

2. Copiare il file `xorg.conf` su `/etc/X11/xorg.conf`.
3. Riavviare l'istanza.

   ```
   $ sudo reboot
   ```

4. Installare il codificatore AMF per la versione appropriata di Ubuntu.

```
$ sudo apt install ./amdgpu-pro-20.20-*/amf-amdgpu-pro_20.20-*_amd64.deb
```

5. (Facoltativo) Installare il server Amazon DCV per utilizzare Amazon DCV come protocollo di visualizzazione ad alte prestazioni, quindi connettersi a una sessione Amazon DCV utilizzando il client preferito.
6. Dopo l'installazione di DCV assegnare le autorizzazioni video per l'utente DCV:

```
$ sudo usermod -aG video dcv
```

Per configurare un desktop interattivo in CentOS

1. Installare l'archivio EPEL.

```
$ sudo yum update -y
$ sudo yum install epel-release -y
```

2. Installare il desktop MATE.

```
$ sudo yum groupinstall "MATE Desktop" -y
$ sudo systemctl disable firewalld
```

3. Copiare il file `xorg.conf` su `/etc/X11/xorg.conf`.
4. Riavviare l'istanza.

```
$ sudo reboot
```

5. (Facoltativo) Installare il server Amazon DCV per utilizzare Amazon DCV come protocollo di visualizzazione ad alte prestazioni, quindi connettersi a una sessione Amazon DCV utilizzando il client preferito.

Inizia a utilizzare le istanze con accelerazione GPU

I tipi di istanza con accelerazione GPU di ultima generazione, come quelle mostrate nell'elenco seguente, offrono le funzionalità di prestazioni più elevate per le applicazioni di deep learning e

calcolo ad alte prestazioni (HPC). Seleziona il link relativo al tipo di istanza per saperne di più sulle sue funzionalità.

- Famiglia P6
- Famiglia P6
- Famiglia P5

Per un elenco completo delle specifiche dei tipi di istanza per i tipi di istanza accelerati, consulta Elaborazione accelerata nel riferimento sui Tipi di istanza Amazon EC2.

Configurazione software

Il modo più semplice per iniziare a utilizzare i tipi di istanze accelerate da GPU di ultima generazione è avviare un'istanza da un'AMI di AWS Deep Learning preconfigurata con tutto il software richiesto. Per le ultime novità da utilizzare con AWS Deep Learning AMIs i tipi di istanze con accelerazione GPU, consulta P6 Supported DLAMI nella Developer Guide. AWS Deep Learning AMIs

Se devi creare un'AMI personalizzata per avviare istanze che ospitano applicazioni di deep learning o HPC, consigliamo di installare le seguenti versioni software minime sopra l'immagine di base.

Tipo di istanza	Driver NVIDIA	CUDA	NVIDIA GDRCopy	Installatore di EFA	NCCL	EFA K8s [1]
G7	595	13.2	2.5.1	1,48,0	2,29,7-1	0,5,10
G7e	575	12.9	2.5	1,45,0	2,283	0,5,10
P5	530	12.1	2.3	1.24.1	2.18.3	0.4.4
P5.4xlarge	530	12.1	2.3	1.43.1 [2]	2.18.3	0.4.4
P5e	550	12.1	2.3	1.24.1	2.18.3	05.5
P5en	550	12.1	2.3	1.24.1	2.18.3	05.6
P6-B200	570	12.8	2.5	1,41,0	2.26.2-1	0,5,10
P6e-GB200	570	12.8	2.5	1,41,0	2.26.2-1	0,5,10

Tipo di istanza	Driver NVIDIA	CUDA	NVIDIA GDRCopy	Installatore di EFA	NCCL	EFA K8s [1]
P6-B300	580	13,0	2.5	1,44,0	2,283	0,5,10

[1] La colonna EFA K8s contiene la versione minima suggerita per `aws-efa-k8s-device-plugin`.

[2] Esiste un problema di compatibilità che riguarda i `P5.4xlarge` casi in cui la GPU-to-GPU comunicazione utilizza Elastic Fabric Adapter (EFA) e la NVIDIA Collective Communications Library (NCCL). Per mitigare il problema, imposta la variabile di ambiente `FI_HMEM_DISABLE_P2P` su `1` e assicurati di installare la versione 1.43.1 o successive di EFA.

> **Note**
>
> Se usi la versione 1.41.0 del programma di installazione EFA, il `aws-ofi-nccl plugin` è incluso. Per le versioni precedenti del programma di installazione EFA, utilizza il `aws-ofi-nccl plugin` versione `1.7.2-aws` o successive.

Ti consigliamo inoltre di configurare l'istanza in modo da non utilizzare più approfonditamente. C-states Per ulteriori informazioni, consulta High performance and low latency by limiting deep C-states nella Amazon Linux 2 User Guide. Le più recenti AMI GPU di AWS Deep Learning Base sono preconfigurate per non essere utilizzate in profondità. C-states

Per la configurazione di rete ed Elastic Fabric Adapter (EFA) consulta Ottimizzare la larghezza di banda della rete sulle istanze Amazon EC2 con più schede di rete.

Istanze Amazon EC2 Mac

Le istanze Mac di EC2 sono ideali per sviluppare, creare, testare e firmare applicazioni per piattaforme Apple, come iPhone, iPad, Mac, Vision Pro, Apple Watch, Apple TV e Safari. Puoi connetterti all'istanza del Mac utilizzando SSH o Apple Remote Desktop (ARD).

> **Note**
>
> L'unità di fatturazione è l'host dedicato. Le istanze in esecuzione su tale host non hanno alcun costo aggiuntivo.

Le istanze Mac Amazon EC2 supportano in modo nativo il sistema operativo macOS.

- Le istanze Mac x86 di EC2 (`mac1.metal`) si basano su hardware Mac mini 2018 con processori Intel Core i7 di ottava generazione (Coffee Lake) a 3,2 GHz, 6 core fisici e 12 logici e 32 GiB di memoria.
- Le istanze Mac M1 di EC2 (`mac2.metal`) si basano su hardware Mac mini 2020 con processore Apple M1, CPU a 8 core, GPU a 8 core, 16 GiB di memoria e Apple Neural Engine a 16 core.
- Le istanze Mac M1 Ultra di EC2 (`mac2-m1ultra.metal`) si basano su hardware Mac Studio 2022 con processore Apple M1 Ultra, CPU a 20 core, GPU a 64 core, 128 GiB di memoria e Apple Neural Engine a 32 core.
- Le istanze Mac M2 di EC2 (`mac2-m2.metal`) si basano su hardware Mac mini 2023 con processore Apple M2, CPU a 8 core, GPU a 10 core, 24 GiB di memoria e Apple Neural Engine a 16 core.
- Le istanze Mac M2 Pro di EC2 (`mac2-m2pro.metal`) si basano su hardware Mac mini 2023 con processore Apple M2 Pro, CPU a 12 core, GPU a 19 core, 32 GiB di memoria e Apple Neural Engine a 16 core.
- Le istanze Mac M4 di EC2 (`mac-m4.metal`) si basano su hardware Mac mini 2024 con processore Apple M4, CPU a 10 core, GPU a 10 core, 24 GiB di memoria e Apple Neural Engine a 16 core.
- Le istanze Mac M4 Pro di EC2 (`mac-m4pro.metal`) si basano su hardware Mac mini 2024 con processore Apple M4 Pro, CPU a 14 core, GPU a 20 core, 48 GiB di memoria e Apple Neural Engine a 16 core.

Gli host dedicati Mac di Amazon EC2 supportano il ripristino automatico degli host dedicati e la manutenzione degli host basata sul riavvio.

Indice

- Considerazioni
- Preparazione dell'istanza
- AMI macOS EC2
- EC2 macOS Init
- Monitoraggio di sistema Amazon EC2 per macOS
- Risorse correlate
- Avvia un'istanza Mac utilizzando Console di gestione AWS o AWS CLI

- Connettiti all'istanza Mac utilizzando SSH o una GUI
- Aggiornamento del sistema operativo e il software per le istanze Mac di Amazon EC2
- Aumentare le dimensioni di un volume EBS sull'istanza Mac
- Come terminare l'istanza Mac di Amazon EC2
- Configurazione della protezione dell'integrità del sistema per istanze Mac di Amazon EC2
- Trova le versioni macOS supportate per il tuo host dedicato Mac Amazon EC2
- Sottoscrizione alle notifiche delle AMI macOS
- Recupera gli ID AMI di macOS utilizzando AWS Systems Manager API Parameter Store
- Note di rilascio delle AMI macOS di Amazon EC2

Considerazioni

Le seguenti considerazioni si applicano alle istanze Mac:

- Le istanze Mac sono disponibili solo come istanze bare metal su Host dedicati, con un periodo di allocazione minimo di 24 ore prima di poter rilasciare Host dedicato. È possibile avviare un'istanza Mac per ogni Host dedicato. Puoi condividere l'host dedicato con AWS gli account o le unità organizzative all'interno della tua AWS organizzazione o con l'intera organizzazione. AWS
- Le istanze Mac sono disponibili in diverse Regioni AWS versioni. Per un elenco della disponibilità delle istanze Mac in ciascuna di esse Regioni AWS, consulta i tipi di istanze Amazon EC2 per regione.
- Le istanze Mac sono disponibili solo come On-Demand istanze. Non sono disponibili come Istanze spot o Istanze riservate. È possibile contenere le spese sulle istanze Mac acquistando un Savings Plan.
- La compatibilità dei diversi tipi di istanze Mac con Amazon Machine Images (AMI) specifiche per macOS varia. Per ulteriori informazioni, consulta Note di rilascio delle AMI macOS di Amazon EC2.
- L'hotplug EBS è supportato.
- AWS non gestisce né supporta l'unità SSD interna sull'hardware Apple. È fortemente consigliato l'utilizzo di volumi Amazon EBS. I volumi EBS offrono gli stessi vantaggi di elasticità, disponibilità e durata sulle istanze Mac come per qualsiasi altra istanza EC2.
- Per prestazioni ottimali, consigliamo di utilizzare un volume Amazon EBS con 10.000 IOPS e 400 MiB/s throughput con istanze Mac. Per ulteriori informazioni, consulta Tipi di volumi di Amazon EBS nella Guida per l'utente di Amazon EBS.
- Le istanze Mac ora supportano Amazon EC2 Auto Scaling.

- Su istanze Mac x86, gli aggiornamenti automatici del software sono disabilitati. Consigliamo di applicare gli aggiornamenti e di testarli sull'istanza prima di mettere l'istanza in produzione. Per ulteriori informazioni, consulta Aggiornamento del sistema operativo e il software per le istanze Mac di Amazon EC2.
- Quando arresti o termini un'istanza Mac, viene eseguito un flusso di lavoro di scrubbing su Host dedicato. Per ulteriori informazioni, consulta Come terminare l'istanza Mac di Amazon EC2.
- **Important**

  Le funzionalità di Apple Intelligence non sono disponibili quando si avvia l'hardware Mac da un volume esterno. Poiché per impostazione predefinita le istanze Mac di EC2 si avviano da volumi EBS esterni, non supportano le funzionalità di Apple Intelligence.
- **Warning**

  Non utilizzare. FileVault Se abiliti FileVault, l'host non si avvia perché le partizioni sono bloccate. Se viene richiesta la crittografia dei dati, utilizza Amazon EBS per evitare problemi di avvio e impatto sulle prestazioni. Con la crittografia Amazon EBS, le operazioni di crittografia si verificano sui server host, garantendo la sicurezza sia dei dati a riposo che di quelli in transito tra le istanze e la relativa archiviazione EBS collegata. Per ulteriori informazioni, consulta Crittografia Amazon EBS nella Guida per l'utente di Amazon EBS.

Preparazione dell'istanza

Dopo avere avviato un'istanza Mac, dovrai attendere che l'istanza sia pronta prima di poterti connettere ad essa. Per un'AMI AWS venduta con un'istanza Mac x86 o un'istanza Mac in silicio Apple, il tempo di avvio può variare da circa 6 minuti a 20 minuti. A seconda delle dimensioni del volume Amazon EBS scelto, dell'inclusione di script aggiuntivi nei dati utente o del software aggiuntivo caricato su un'AMI macOS personalizzata, il tempo di avvio potrebbe aumentare.

Puoi utilizzare un piccolo script della shell (interprete di comandi) come quello riportato di seguito per eseguire il polling dell'API describe-instance-status per sapere quando l'istanza è pronta per la connessione. Nel comando seguente, sostituisci il l'ID dell'istanza di esempio con il tuo.

```
for i in $(seq 1 200); do aws ec2 describe-instance-status --instance-
ids=i-1234567890abcdef0 \
    --query='InstanceStatuses[0].InstanceStatus.Status'; sleep 5; done;
```

AMI macOS EC2

Amazon EC2 macOS è progettato per fornire un ambiente stabile, sicuro e ad alte prestazioni per i carichi di lavoro degli sviluppatori in esecuzione su istanze Amazon EC2 Mac. Le AMI macOS EC2 includono pacchetti che consentono una facile integrazione con AWS, ad esempio, gli strumenti di configurazione Launch e le librerie e gli strumenti più diffusi. AWS

Per ulteriori informazioni sulle AMI EC2 macOS, consulta Note di rilascio delle AMI macOS di Amazon EC2.

AWS fornisce regolarmente AMI EC2 macOS aggiornate che includono aggiornamenti ai pacchetti di proprietà di macOS e alla versione macOS più recente AWS e completamente testata. Inoltre, AWS fornisce AMI aggiornate con gli ultimi aggiornamenti della versione secondaria o gli aggiornamenti della versione principale non appena questi possono essere completamente testati e controllati. Se non è necessario conservare i dati o le personalizzazioni delle istanze Mac, è possibile ottenere gli aggiornamenti più recenti avviando una nuova istanza utilizzando l'AMI corrente e quindi terminando l'istanza precedente. In caso contrario, è possibile scegliere gli aggiornamenti da applicare alle istanze Mac.

Per informazioni su come abbonarsi alle notifiche dell'AMI macOS, consulta Sottoscrizione alle notifiche delle AMI macOS.

EC2 macOS Init

EC2 macOS Init viene utilizzato per inizializzare le istanze Mac EC2 al momento dell'avvio. Utilizza gruppi di priorità per eseguire gruppi logici di attività contemporaneamente.

Il file launchd plist è `/Library/LaunchDaemons/com.amazon.ec2.macos-init.plist`. I file per EC2 macOS Init si trovano in `/usr/local/aws/ec2-macos-init`.

Per ulteriori informazioni, consulta https://github.com/aws/ec2-macos-init.

Monitoraggio di sistema Amazon EC2 per macOS

Amazon EC2 System Monitor per macOS fornisce metriche di utilizzo della CPU ad Amazon. CloudWatch Invia queste metriche a un dispositivo seriale personalizzato CloudWatch in periodi di 1 minuto. È possibile abilitare o disabilitare questo agente come segue. È abilitato per impostazione predefinita.

```
sudo setup-ec2monitoring [enable | disable]
```

> **Note**
>
> Il monitoraggio di sistema Amazon EC2 per macOS attualmente non è supportato sulle istanze Mac con processore Apple.

Risorse correlate

Per informazioni sui prezzi, consulta Pricing.

Per ulteriori informazioni sulle istanze Mac, consulta la sezione relativa alle Istanze Amazon EC2 Mac.

Per ulteriori informazioni sulle specifiche hardware e sulle prestazioni di rete delle istanze Mac, consulta Istanze per uso generico.

Avvia un'istanza Mac utilizzando Console di gestione AWS o AWS CLI

Le istanze Mac EC2 richiedono un host dedicato. Devi prima allocare un host al tuo account e quindi avviare l'istanza sull'host.

Puoi avviare un'istanza Mac utilizzando Console di gestione AWS o AWS CLI.

Avviare un'istanza Mac utilizzando la console

Per avviare un'istanza Mac su un Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Alloca l'host dedicato, come indicato di seguito:
    a. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
    b. Scegliere Allocate Host dedicato (Alloca host dedicato), quindi effettuare le seguenti operazioni:
        i. In Famiglia di istanze, scegli una famiglia di istanze Mac. Se la famiglia di istanze non appare nell'elenco, non è supportata nella regione selezionata.
        ii. In Tipo di istanza, scegli il tipo di istanza in base alla famiglia di istanze selezionata.
        iii. Per Availability Zone (Zona di disponibilità), scegliere la zona di disponibilità per il Host dedicato.
        iv. Per Quantity (Quantità), mantieni il valore 1.

v. Scegli Alloca.

3. Avvia l'istanza sull'host, come indicato di seguito:

   a. Selezionare il Host dedicato che è stato creato e quindi effettuare le seguenti operazioni:

      i. Scegli Actions (Azioni), Launch instance(s) onto host (Avvia istanze sull'host).

      ii. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), seleziona un'AMI macOS.

      iii. In Tipo di istanza, seleziona un tipo di istanza Mac.

      iv. In Dettagli avanzati, verifica che Tenancy, Host tenancy di e ID host tenancy siano preconfigurati in base all'host dedicato creato. Aggiorna Tenancy affinity (Affinità tenancy) in base alle necessità.

      v. Completare la procedura guidata specificando volumi EBS, gruppi di sicurezza e coppie di chiavi in base alle esigenze.

      vi. Nel pannello Summary (Riepilogo), scegliere Launch instance (Avvia istanza).

   b. Una pagina di conferma indicherà che l'istanza si sta avviando. Scegli View Instances (Visualizza istanze) per chiudere la pagina di conferma e tornare alla console. Lo stato iniziale di un'istanza è `pending`. L'istanza è pronta quando il suo stato cambia in `running` e passa i controlli di stato.

Avvia un'istanza Mac usando il AWS CLI

Allocazione dell'host dedicato

Utilizza il comando allocate-hosts per allocare un host dedicato per la tua istanza Mac, sostituendo il `instance-type` con un tipo di istanza Mac valido e la `region` e la `availability-zone` con quelle appropriate al tuo ambiente.

```
aws ec2 allocate-hosts --region us-east-1 --instance-type mac1.metal --availability-
zone us-east-1b --auto-placement "on" --quantity 1
```

Avvio dell'istanza sull'host

Utilizza il comando run-instances per avviare un'istanza Mac, sostituendo nuovamente `instance-type` con un tipo di istanza Mac valido e la `region` e la `availability-zone` con i valori utilizzati in precedenza.

```
aws ec2 run-instances --region us-east-1 --instance-type mac1.metal --placement
 Tenancy=host --image-id ami_id --key-name my-key-pair
```

Lo stato iniziale di un'istanza è `pending`. L'istanza è pronta quando il suo stato cambia in `running` e passa i controlli di stato. Utilizza il comando describe-instance-status per visualizzare le informazioni sullo stato dell'istanza.

```
aws ec2 describe-instance-status --instance-ids i-017f8354e2dc69c4f
```

Di seguito è riportato un esempio di output per un'istanza in esecuzione che ha superato i controlli di stato.

```
{
    "InstanceStatuses": [
        {
            "AvailabilityZone": "us-east-1b",
            "InstanceId": "i-017f8354e2dc69c4f",
            "InstanceState": {
                "Code": 16,
                "Name": "running"
            },
            "InstanceStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            },
            "SystemStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            }
        }
    ]
```

```
}
```

Connettiti all'istanza Mac utilizzando SSH o una GUI

È possibile connettersi all'istanza Mac utilizzando SSH o un'interfaccia utente grafica (GUI).

Più utenti possono accedere al sistema operativo contemporaneamente. In genere esiste una sessione individuale User:GUI, a causa del servizio Screen Sharing integrato sulla porta 5900. L'utilizzo di SSH all'interno di macOS supporta più sessioni fino al limite "Sessioni massime" nel `sshd_config`.

Connettersi all'istanza tramite SSH

Le istanze Amazon EC2 Mac non consentono l'SSH root remoto per impostazione predefinita. L'account ec2-user è configurato per accedere da remoto utilizzando SSH. Anche l'account ec2-user dispone di privilegi sudo. Dopo aver effettuato la connessione all'istanza, è possibile aggiungere altri utenti.

Per supportare la connessione all'istanza tramite SSH, avviare l'istanza utilizzando una coppia di chiavi e un gruppo di sicurezza che consente l'accesso SSH e assicurarsi che l'istanza disponga di connettività Internet. Fornire il file `.pem` per la coppia di chiavi quando ci si connette all'istanza.

Utilizza la seguente procedura per stabilire una connessione a un'istanza Mac tramite un client SSH. Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta Risoluzione dei problemi di connessione all'istanza Linux di Amazon EC2.

Per connettersi all'istanza tramite SSH

1. Verificare che nel computer locale sia installato un client SSH immettendo ssh nella riga di comando. Se il computer non riconosce il comando, cercare un client SSH per il sistema operativo e installarlo.
2. Ottenere il nome DNS pubblico dell'istanza. Utilizzando la console Amazon EC2 è possibile trovare il nome DNS pubblico sia nelle schede Details (Dettagli) che nelle schede Networking (Rete). Usando il AWS CLI, puoi trovare il nome DNS pubblico usando il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instances.html describe-instances.
3. Individuare il file `.pem` per la coppia di chiavi specificata al momento dell'avvio dell'istanza.
4. Connettersi all'istanza utilizzando il seguente comando ssh, specificando il nome DNS pubblico dell'istanza e il file `.pem`.

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

L'autenticazione delle password è disabilitata per evitare attacchi di forza bruta alle password. Prima di apportare modifiche alla configurazione SSH, apri `/usr/local/aws/ec2-macos-init/init.toml` e imposta `secureSSHDConfig` su `false`.

Connessione all'interfaccia utente grafica (GUI) dell'istanza

Per connettersi all'interfaccia utente grafica dell'istanza utilizzando VNC, Apple Remote Desktop (ARD) o l'applicazione di condivisione schermo di Apple, attenersi alla procedura seguente (inclusa in macOS).

> **Note**
>
> macOS 10.14 e versioni successive permette di controllare solo se la condivisione dello schermo è abilitata tramite le Preferenze di sistema.

Connessione all'istanza tramite client ARD o client VNC

1. Verificare che il computer locale disponga di un client ARD o di un client VNC che supporti ARD installato. Su macOS è possibile sfruttare l'applicazione Condivisione schermo integrata. In caso contrario, cercare un ARD per il sistema operativo e installarlo.
2. Dal computer locale, connettersi all'istanza utilizzando SSH.
3. Impostare una password per l'account ec2-user utilizzando il comando passwd come segue.

   ```
   [ec2-user ~]$ sudo passwd ec2-user
   ```
4. Installa e avvia macOS Screen Sharing utilizzando il comando seguente.

   ```
   [ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
   ```
5. Disconnettiti dall'istanza digitando exit e premendo Invio.
6. Dal computer, connettersi all'istanza utilizzando il seguente comando ssh. Oltre alle opzioni illustrate nella sezione precedente, utilizzare l'opzione -L per abilitare l'inoltro alla porta e inoltrare tutto il traffico sulla porta locale 5900 al server ARD sull'istanza.

```
ssh -L 5900:localhost:5900 -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

7. Dal computer locale, utilizza il client ARD o VNC che supporta ARD per connetterti a localhost su `localhost:5900`. Ad esempio, utilizzare l'applicazione Condivisione schermo su macOS come segue:

   a. Apri il Finder e seleziona Vai.

   b. Seleziona Connetti al server.

   c. Nel campo Indirizzo del server, inserisci `vnc://localhost:5900`.

   d. Accedi come richiesto, utilizzando **`ec2-user`** come nome utente e la password creata per l'account ec2-user.

Modifica della risoluzione dello schermo macOS sulle istanze Mac

Dopo avere stabilito la connessione all'istanza Mac di EC2 utilizzando ARD o un client VNC che supporta ARD, puoi modificare la risoluzione dello schermo dell'ambiente macOS utilizzando uno qualsiasi degli strumenti o delle utilità macOS disponibili pubblicamente, come displayplacer.

Modifica della risoluzione dello schermo mediante displayplacer

1. Installa displayplacer.

```
[ec2-user ~]$ brew tap jakehilborn/jakehilborn && brew install displayplacer
```

2. Visualizza le informazioni correnti sullo schermo e le possibili risoluzioni dello schermo.

```
[ec2-user ~]$ displayplacer list
```

3. Applica la risoluzione dello schermo desiderata.

```
[ec2-user ~]$ displayplacer "id:<screenID> res:<width>x<height> origin:(0,0)
 degree:0"
```

   Ad esempio:

```
RES="2560x1600"
```

```
displayplacer "id:69784AF1-CD7D-B79B-E5D4-60D937407F68 res:${RES} scaling:off
 origin:(0,0) degree:0"
```

Aggiornamento del sistema operativo e il software per le istanze Mac di Amazon EC2

L'argomento seguente spiega come aggiornare il sistema operativo e il software sulle istanze Mac Apple Silicon (Mac2,,, Mac2-m1ultra Mac2-m2 Mac2-m2pro Mac-m4, e Mac-m4pro) e sulle istanze Mac x86 (Mac1).

Warning

L'installazione delle versioni beta o in anteprima di macOS è disponibile solo sulle istanze Mac con processore Apple. Amazon EC2 non qualifica le versioni beta o in anteprima di macOS e non garantisce che le istanze rimarranno funzionanti dopo un aggiornamento a una versione macOS di pre-produzione.
Cercare di installare versioni beta o in anteprima di macOS sulle istanze Mac Amazon EC2 x86 comporterà un peggioramento dell'host dedicato Mac EC2 quando arresti o termini l'istanza e ti impedirà di avviare o lanciare una nuova istanza su quell'host.

Note

Se esegui un aggiornamento macOS locale prima che AWS rilasci un'AMI ufficiale, l'aggiornamento si applica solo all'host selezionato. Se disponi di altri host o se ne avvii di nuovi, devi eseguire lo stesso processo di aggiornamento anche su tali host. Ogni versione di macOS richiede una versione firmware minima sull'hardware Apple Mac sottostante. L'aggiornamento locale viene applicato solo al firmware sull'host selezionato e non viene trasferito su altri host nuovi o esistenti. Per verificare quali versioni di macOS sono compatibili con il tuo host dedicato Mac di Amazon EC2, consulta Find supported macOS versions for your Amazon EC2 Mac Dedicated Host.

Aggiornamento del software su istanze Mac con processore Apple

Prerequisiti

A causa di un aggiornamento nella configurazione del driver di rete, la versione 1.0.2 del driver ENA non è compatibile con macOS 13.3 o versioni successive. Se desideri installare una versione macOS 13.3 o successiva in versione beta, in anteprima o in produzione e non hai installato il driver ENA più recente, utilizza la procedura seguente per installare una nuova versione del driver.

Installazione di una nuova versione del driver ENA

1. In una finestra del terminale, connettiti all'istanza Mac con processore Apple utilizzando SSH.
2. Aggiorna Homebrew e scarica l'applicazione ENA nel file `Applications` con il seguente comando.

```
[ec2-user ~]$ brew update
```

```
[ec2-user ~]$ brew install amazon-ena-ethernet-dext
```

3. Disconnettiti dall'istanza digitando exit e premendo Invio.
4. Usa il client VNC per attivare l'applicazione ENA.
   a. Configura il client VNC utilizzando Connessione all'interfaccia utente grafica (GUI) dell'istanza.
   b. Dopo esserti connesso all'istanza utilizzando l'applicazione Screen Sharing, vai alla cartella Applicazioni e apri l'applicazione ENA.
   c. Scegli Attiva.
   d. Per confermare che il driver sia stato attivato correttamente, esegui il comando riportato di seguito nella finestra del terminale. L'output del comando mostra che il vecchio driver è nello stato di terminazione in corso e il nuovo driver è nello stato attivato.

```
systemextensionsctl list;
```

   e. Dopo aver riavviato l'istanza, sarà presente solo il nuovo driver.

Aggiornamento del software

Sulle istanze Mac con processore Apple, è necessario completare diversi passaggi per eseguire un aggiornamento del sistema operativo in loco. Ciò include la delega della proprietà del volume root Amazon EBS all'utente amministrativo del volume root EBS. Puoi scegliere di farlo automaticamente utilizzando un'API Amazon EC2 oppure manualmente eseguendo i comandi sulla tua istanza.

Automated volume ownership delegation (Recommended)

Considerazioni

- Il completamento dell'attività di delega della proprietà del volume può richiedere dai 30 ai 90 minuti. Durante questo periodo, l'istanza non è raggiungibile.
- Sono supportate le seguenti versioni macOS:
  - Mac2 | Mac2-m1ultra — macOS Ventura (versione 13.0 o successiva)
  - Mac2-m2 | Mac2-m2pro — macOS Ventura (versione 13.2 o successiva)
  - Mac-m4 | Mac-m4pro — macOS Sequoia (versione 15.6 o successiva)
- Le istanze devono avere un solo volume avviabile e ogni volume collegato può avere un solo utente amministratore aggiuntivo.

Passaggio 1: impostazione di una password e abilitazione del token sicuro per l'utente amministrativo del volume root EBS

Devi impostare una password e abilitare il token sicuro per l'utente amministrativo del volume root Amazon EBS (`ec2-user`).

> **Note**
>
> La password e il token sicuro vengono impostati la prima volta che ti connetti a un'istanza Mac con processore Apple utilizzando l'interfaccia grafica (GUI). Se in precedenza hai effettuato la connessione all'istanza utilizzando la GUI, non devi eseguire questi passaggi.

1. Connettiti all'istanza tramite SSH.
2. Imposta la password per l'utente `ec2-user`.

```
$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
```

3. Abilita il token sicuro per l'utente `ec2-user`. In `-oldPassword`, specifica la stessa password del passaggio precedente. In `-newPassword`, specifica una password diversa. Il comando seguente presuppone che la vecchia e la nuova password siano salvate nei file `.txt`.

```
$ sysadminctl -oldPassword `cat old_password.txt` -newPassword `cat
 new_password.txt`
```

4. Verifica che il token sicuro sia abilitato.

```
$ sysadminctl -secureTokenStatus ec2-user
```

Passaggio 2: delega della proprietà del volume root Amazon EBS all'utente amministrativo del volume root EBS

Per delegare la proprietà, devi creare un'attività di delega della proprietà del volume.

1. Utilizza il comando create-delegate-mac-volume-ownership-task per creare l'attività. In `--instance-id`, specifica l'ID dell'istanza da controllare. In `--mac-credentials`, specifica le seguenti credenziali:

   - Utente amministrativo del disco interno
     - Nome utente: solo l'utente amministrativo predefinito (`aws-managed-user`) è supportato e viene utilizzato per impostazione predefinita. Non puoi specificare un utente amministrativo diverso.
     - Password: se non hai modificato la password predefinita per `aws-managed-user`, specifica la password predefinita, che è vuota. Altrimenti, specifica la password.
   - Utente amministrativo del volume root Amazon EBS
     - Nome utente: se non hai modificato l'utente amministrativo predefinito, specifica `ec2-user`. Altrimenti, specifica il nome utente per l'utente amministrativo.
     - Password: specifica la password che hai impostato per l'utente amministrativo del volume root nel Passaggio 1 precedente.

```
aws ec2 create-delegate-mac-volume-ownership-task \
--instance-id i-1234567890abcdef0 \
--mac-credentials file://mac-credentials.json
```

I seguenti contenuti fanno parte del file `mac-credentials.json` indicato negli esempi precedenti.

```
{
  "internalDiskPassword":"internal-disk-admin_password",
  "rootVolumeUsername":"root-volume-admin_username",
  "rootVolumePassword":"root-volume-admin_password"
}
```

2. Attendi il completamento dell'attività di delega della proprietà del volume e che l'istanza ritorni a uno stato integro. Utilizza il comando describe-mac-modification-tasks. In `--mac-modification-task-id`, specifica l'ID dell'attività di delega della proprietà del volume del passaggio precedente.

```
aws ec2 describe-mac-modification-tasks \
--mac-modification-task-id task-id
```

3. Una volta completata l'attività di delega della proprietà del volume, continua con il Passaggio 3.

Passaggio 3: aggiornamento del software

Dopo aver delegato la proprietà del volume root Amazon EBS, segui i passaggi descritti in Aggiornamento del software su istanze Mac x86 (di seguito) per aggiornare il software.

Manual volume ownership delegation

Durante questa procedura si creano due password: Una password è per l'utente amministrativo del volume root Amazon EBS (`ec2-user`) e l'altra per l'utente amministrativo del disco interno (`aws-managed-user`). Ricorda queste password poiché le utilizzerai durante la procedura.

> **Note**
>
> Su macOS Big Sur, con questa procedura puoi eseguire solo aggiornamenti minori come l'aggiornamento da macOS Big Sur 11.7.3 a macOS Big Sur 11.7.4. Per macOS Monterey o versioni successive, puoi eseguire aggiornamenti software importanti.

Per accedere al disco interno

1. Dal computer locale, nel terminale, connettiti all'istanza Mac con processore Apple tramite SSH con il seguente comando. Per ulteriori informazioni, consulta Connettersi all'istanza tramite SSH.

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

2. Installa e avvia macOS Screen Sharing utilizzando il comando seguente.

```
[ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
sudo launchctl load -w /System/Library/LaunchDaemons/
com.apple.screensharing.plist
```

3. Imposta una password per `ec2-user` con il comando seguente. Ricorda la password perché la userai in seguito.

```
[ec2-user ~]$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
```

4. Disconnettiti dall'istanza digitando exit e premendo INVIO.
5. Dal computer locale, nel Terminale, riconnettiti all'istanza con un tunnel SSH alla porta VNC usando il seguente comando.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 ec2-user@instance-public-
dns-name
```

> **Note**
>
> Non uscire da questa sessione SSH fino a quando non sono stati completati i seguenti passaggi di connessione VNC e GUI. Quando l'istanza viene riavviata, la connessione si chiude automaticamente.

6. Dal computer locale, connettiti a `localhost:5900` seguendo la procedura seguente:
   a. Apri il Finder e seleziona Vai.
   b. Seleziona Connetti al server.
   c. Nel campo Indirizzo del server, inserisci `vnc://localhost:5900`.

7. Nella finestra macOS, connettiti alla sessione remota dell'istanza Mac con processore Apple come `ec2-user`, utilizzando la password creata nel passaggio 3.
8. Accedere al disco interno, denominato InternalDisk, utilizzando una delle seguenti opzioni.

   a. Per macOS Ventura o versioni successive: apri Impostazioni di sistema, seleziona Generale nel riquadro sinistro, quindi Disco di startup nella parte inferiore destra del riquadro.

   b. Per macOS Monterey o versioni precedenti: apri Preferenze di Sistema, seleziona Disco di startup, quindi sblocca il riquadro selezionando l'icona del lucchetto nella parte inferiore sinistra della finestra.

   Suggerimento per la risoluzione dei problemi:

   Se devi montare il disco interno, esegui il seguente comando nel Terminale.

   ```
   APFSVolumeName="InternalDisk" ; SSDContainer=$(diskutil list | grep
    "Physical Store disk0" -B 3 | grep "/dev/disk" | awk {'print $1'} ) ;
    diskutil apfs addVolume $SSDContainer APFS $APFSVolumeName
   ```

9. Scegli il disco interno, denominato InternalDisk, e seleziona Riavvia. Seleziona nuovamente Riavvia quando richiesto.

   Important

   Se il disco interno è denominato Macintosh HD anziché InternalDisk, l'istanza deve essere arrestata e riavviata in modo che l'host dedicato possa essere aggiornato. Per ulteriori informazioni, consulta Come terminare l'istanza Mac di Amazon EC2.

Utilizza la procedura seguente per delegare la proprietà all'utente amministrativo. Quando ti riconnetti all'istanza con SSH, esegui l'avvio dal disco interno utilizzando l'utente amministrativo speciale (`aws-managed-user`). La password iniziale per `aws-managed-user` è vuota, quindi è necessario sovrascriverla alla prima connessione. Ripeti quindi i passaggi per installare e avviare macOS Screen Sharing poiché il volume di avvio è cambiato.

Per delegare la proprietà all'amministratore di un volume Amazon EBS

1. Dal computer locale, nel terminale, connettiti all'istanza Mac con processore Apple con il seguente comando.

```
ssh -i /path/key-pair-name.pem aws-managed-user@instance-public-dns-name
```

2. Quando visualizzi l'avviso `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, esegui una delle operazioni seguenti per risolvere il problema.

   a. Cancella gli host noti usando il seguente comando. Quindi, ripeti il passaggio precedente.

   ```
   rm ~/.ssh/known_hosts
   ```

   b. Aggiungi la stringa seguente al comando SSH del passaggio precedente.

   ```
   -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
   ```

3. Imposta la password per `aws-managed-user` con il seguente comando. La password iniziale per `aws-managed-user` è vuota, quindi è necessario sovrascriverla alla prima connessione.

   a.
   ```
   [aws-managed-user ~]$ sudo /usr/bin/dscl . -passwd /Users/aws-managed-user password
   ```

   b. Quando ricevi il prompt`Permission denied. Please enter user's old password:`, premi INVIO.

   > Suggerimento per la risoluzione dei problemi:
   >
   > Se ricevi il messaggio di errore `passwd: DS error: eDSAuthFailed`, usa il seguente comando.
   >
   > ```
   > [aws-managed-user ~]$ sudo passwd aws-managed-user
   > ```

4. Installa e avvia macOS Screen Sharing utilizzando il comando seguente.

```
[aws-managed-user ~]$ sudo launchctl enable system/com.apple.screensharing
```

```
sudo launchctl load -w /System/Library/LaunchDaemons/
com.apple.screensharing.plist
```

5. Disconnettiti dall'istanza digitando exit e premendo INVIO.
6. Dal computer locale, nel Terminale, riconnettiti all'istanza con un tunnel SSH alla porta VNC usando il seguente comando.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 aws-managed-user@instance-
public-dns-name
```

7. Dal computer locale, connettiti a `localhost:5900` seguendo la procedura seguente:
   a. Apri il Finder e seleziona Vai.
   b. Seleziona Connetti al server.
   c. Nel campo Indirizzo del server, inserisci `vnc://localhost:5900`.
8. Nella finestra macOS, connettiti alla sessione remota dell'istanza Mac con processore Apple come `aws-managed-user`, utilizzando la password creata nel passaggio 3.

> **Note**
>
> Quando ti viene richiesto di accedere con il tuo ID Apple, seleziona Configura in seguito.

9. Accedi al volume Amazon EBS utilizzando una delle opzioni seguenti.
   a. Per macOS Ventura o versioni successive: apri Impostazioni di sistema, seleziona Generale nel riquadro sinistro, quindi Disco di avvio nella parte inferiore destra del riquadro.
   b. Per macOS Monterey o versioni precedenti: apri Preferenze di sistema, seleziona Disco di avvio, quindi sblocca il riquadro tramite l'icona del lucchetto nella parte inferiore sinistra della finestra.

> **Note**
>
> Fino al riavvio, quando viene richiesta una password di amministratore, usa quella configurata in precedenza per `aws-managed-user`. La password potrebbe essere diversa da quella impostata per `ec2-user` o dall'account amministratore

predefinito dell'istanza. Le istruzioni seguenti indicano quando utilizzare la password di amministratore dell'istanza.

10. Seleziona il volume Amazon EBS (il volume non denominato InternalDisk nella finestra Startup Disk) e scegli Riavvia.

> **Note**
>
> Se disponi di più volumi Amazon EBS avviabili collegati all'istanza Mac con processore Apple, assicurati di utilizzare un nome univoco per ogni volume.

11. Conferma il riavvio, quindi scegli Autorizza utenti quando richiesto.
12. Nel riquadro Autorizza utente per questo volume, verifica che l'utente amministrativo (per impostazione predefinita, `ec2-user`) sia selezionato, quindi scegli Autorizza.
13. Inserisci la password `ec2-user` creata nel passaggio 3 della procedura precedente, quindi seleziona Continua.
14. Quando richiesto, inserisci la password per l'utente amministrativo speciale (`aws-managed-user`).
15. Dal computer locale, nel Terminale, riconnettiti all'istanza utilizzando SSH con nome utente `ec2-user`.

> **Suggerimento per la risoluzione dei problemi:**
>
> Se visualizzi l'avviso `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, esegui il comando seguente e riconnettiti all'istanza tramite SSH.
>
> ```
> rm ~/.ssh/known_hosts
> ```

16. Per eseguire l'aggiornamento del software, usa i comandi in Aggiornamento del software su istanze Mac x86.

Aggiornamento del software su istanze Mac x86

Su istanze Mac x86 puoi installare aggiornamenti del sistema operativo da Apple utilizzando il comando `softwareupdate`.

Per installare aggiornamenti del sistema operativo da Apple su istanze Mac x86

1. Elencare i pacchetti con gli aggiornamenti disponibili utilizzando il seguente comando.

```
[ec2-user ~]$ softwareupdate --list
```

2. Installare tutti gli aggiornamenti o solo aggiornamenti specifici. Per installare aggiornamenti specifici, utilizzare il seguente comando.

```
[ec2-user ~]$ sudo softwareupdate --install label
```

   Per installare invece tutti gli aggiornamenti, utilizzare il seguente comando.

```
[ec2-user ~]$ sudo softwareupdate --install --all --restart
```

Gli amministratori di sistema possono utilizzarlo AWS Systems Manager per implementare aggiornamenti del sistema operativo preapprovati su istanze Mac x86. Per ulteriori informazioni, consulta la Guida per l'utente di AWS Systems Manager.

È possibile utilizzare Homebrew per installare gli aggiornamenti ai pacchetti nelle AMI macOS EC2, in modo da avere la versione più recente di questi pacchetti nelle istanze. È possibile anche utilizzare Homebrew per installare ed eseguire applicazioni macOS comuni su Amazon EC2 macOS. Per ulteriori informazioni, consulta la documentazione di Homebrew.

Per installare gli aggiornamenti utilizzando Homebrew

1. Aggiornare Homebrew utilizzando il seguente comando.

```
[ec2-user ~]$ brew update
```

2. Elencare i pacchetti con gli aggiornamenti disponibili utilizzando il seguente comando.

```
[ec2-user ~]$ brew outdated
```

3. Installare tutti gli aggiornamenti o solo aggiornamenti specifici. Per installare aggiornamenti specifici, utilizzare il seguente comando.

```
[ec2-user ~]$ brew upgrade package name
```

Per installare invece tutti gli aggiornamenti, utilizzare il seguente comando.

```
[ec2-user ~]$ brew upgrade
```

Aumentare le dimensioni di un volume EBS sull'istanza Mac

Puoi aumentare le dimensioni dei tuoi volumi Amazon EBS sull'istanza Mac. Per ulteriori informazioni, consulta Volumi elastici Amazon EBS nella Guida per l'utente di Amazon EBS.

Dopo aver aumentato le dimensioni del volume, è necessario aumentare le dimensioni del container APFS come segue.

Aumentare lo spazio su disco disponibile per l'uso

1. Determinare se è necessario riavviare. Se si ridimensiona un volume EBS esistente su un'istanza Mac in esecuzione, è necessario riavviare l'istanza per rendere disponibile la nuova dimensione. Se la modifica dello spazio su disco è stata eseguita durante l'avvio, non sarà necessario riavviare il sistema.

   Visualizzare lo stato corrente delle dimensioni del disco:

   ```
   [ec2-user ~]$  diskutil list external physical
   /dev/disk0 (external, physical):
      #:                       TYPE NAME                    SIZE       IDENTIFIER
      0:                 GUID_partition_scheme           *322.1 GB     disk0
      1:                 EFI EFI                          209.7 MB     disk0s1
      2:                 Apple_APFS Container disk2       321.9 GB     disk0s2
   ```

2. Copia e incolla il comando seguente.

   ```
   [ec2-user ~]$ PDISK=$(diskutil list physical external | head -n1 | cut -d" " -f1)
   APFSCONT=$(diskutil list physical external | grep "Apple_APFS" | tr -s " " | cut -
   d" " -f8)
   yes | sudo diskutil repairDisk $PDISK
   ```

3. Copia e incolla il comando seguente.

   ```
   [ec2-user ~]$ sudo diskutil apfs resizeContainer $APFSCONT 0
   ```

Come terminare l'istanza Mac di Amazon EC2

Quando interrompi un'istanza Mac, questa rimane nello stato `stopping` per circa 15 minuti prima di passare allo stato `stopped`.

Quando arresti o interrompi un'istanza Mac, Amazon EC2 esegue un flusso di lavoro di scrubbing sull'host dedicato sottostante per cancellare l'SSD interno, per cancellare le variabili NVRAM persistenti e per aggiornare il dispositivo con il firmware più recente. Ciò garantisce che le istanze Mac forniscano la stessa sicurezza e privacy dei dati delle altre istanze Nitro EC2. Consente anche di eseguire le AMI macOS più recenti. Durante il flusso di lavoro di scrubbing, l'host dedicato entra temporaneamente in stato di sospensione. Su istanze Mac x86, il completamento del flusso di lavoro di scrubbing può richiedere fino a 50 minuti. Se Amazon EC2 deve aggiornare il firmware del dispositivo, il completamento del flusso di lavoro potrebbe richiedere fino a 3 ore. Sulle istanze Apple Silicon Mac, il completamento del flusso di lavoro di pulizia potrebbe richiedere fino a 4,5 ore.

Non è possibile avviare l'istanza Mac interrotta o avviare una nuova istanza Mac fino al termine del flusso di lavoro di scrubbing, a quel punto Host dedicato entra nello stato `available`.

La misurazione e la fatturazione vengono sospese quando l'host dedicato entra nello stato `pending`. Non viene addebitato alcun addebito per la durata del flusso di lavoro di scrubbing.

Rilasciare l'Host dedicato per l'istanza Mac

Quando hai finito di utilizzare l'istanza Mac, puoi rilasciare l'Host dedicato. Prima di poter rilasciare il Host dedicato, è necessario interrompere o terminare l'istanza Mac. Non è possibile rilasciare l'host finché il periodo di allocazione non superi il periodo minimo di 24 ore.

Per rilasciare l'Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza e scegliere Instance State (Stato istanza), quindi scegliere Stop instance (Interrompi istanza) o Terminate instance (Termina istanza).
4. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
5. Selezionare il Host dedicato e scegliere Actions (Azioni), Release host (Rilascia host).
6. Quando viene richiesta la conferma, scegliere Release (Rilascia).

Configurazione della protezione dell'integrità del sistema per istanze Mac di Amazon EC2

Puoi configurare le impostazioni di System Integrity Protection (SIP) per le istanze Mac x86 e Mac con processore Apple. SIP è una funzionalità di sicurezza fondamentale di macOS che aiuta a prevenire l'esecuzione non autorizzata di codice e le modifiche a livello di sistema. Per ulteriori informazioni, consulta About System Integrity Protection.

Puoi abilitare o disabilitare completamente la funzionalità SIP oppure abilitare o disabilitare selettivamente impostazioni SIP specifiche. Consigliamo di disabilitare la funzionalità SIP solo temporaneamente per eseguire le attività necessarie e quindi di riattivarla il prima possibile. Lasciare la funzionalità SIP disabilitata potrebbe rendere l'istanza vulnerabile al codice dannoso.

La configurazione SIP è supportata in tutte le AWS regioni in cui sono supportate le istanze Mac di Amazon EC2.

Argomenti

- Considerazioni
- Configurazioni SIP predefinite
- Controllo della configurazione SIP
- Prerequisiti per istanze Mac con processore Apple
- Configurazione delle impostazioni SIP
- Controllo dello stato dell'attività di configurazione SIP

Considerazioni

- Sono supportati i seguenti tipi di istanza Mac di Amazon EC2 e versioni macOS:
  - Mac1 | Mac2 | Mac2-m1ultra — macOS Ventura (versione 13.0 o successiva)
  - Mac2-m2 | Mac2-m2pro — macOS Ventura (versione 13.2 o successiva)
  - Mac-m4 | Mac-m4pro — macOS Sequoia (versione 15.6 o successiva)

  > **Note**
  >
  > Le versioni beta e di anteprima di macOS non sono supportate.

- Puoi specificare una configurazione SIP personalizzata per abilitare o disabilitare selettivamente le singole impostazioni SIP. Se implementi una configurazione personalizzata, connettiti all'istanza e

verifica le impostazioni per assicurarti che i requisiti siano implementati correttamente e funzionino come previsto.

Le configurazioni SIP potrebbero cambiare con gli aggiornamenti di macOS. Consigliamo di rivedere le impostazioni SIP personalizzate dopo ogni aggiornamento della versione di macOS per garantire la compatibilità continua e la corretta funzionalità delle configurazioni di sicurezza.

- Per istanze Mac x86, le impostazioni SIP vengono applicate a livello di istanza. Qualsiasi volume root collegato all'istanza erediterà automaticamente le impostazioni SIP configurate.

  Per le istanze Mac con processore Apple, le impostazioni SIP vengono applicate a livello di volume. I volumi root collegati all'istanza non ereditano le impostazioni SIP. Se colleghi un altro volume root, devi riconfigurare le impostazioni SIP allo stato richiesto.
- Il completamento delle attività di configurazione SIP può richiedere fino a 90 minuti. L'istanza rimane irraggiungibile mentre è in corso l'attività di configurazione SIP.
- Le configurazioni SIP non vengono trasferite su snapshot o AMI create successivamente dall'istanza.
- Le istanze Mac con processore Apple devono avere un solo volume avviabile e ogni volume collegato può avere un solo utente amministrativo aggiuntivo.

Configurazioni SIP predefinite

La tabella seguente elenca la configurazione SIP predefinita per le istanze Mac x86 e Mac con processore Apple.

	Istanze Mac con processore Apple	Istanze Mac x86
Interno Apple	Abilitato	Disabilitato
Protezioni del filesystem	Abilitato	Disabilitato
Sistema di base	Abilitato	Abilitato
Restrizioni di debugging	Abilitato	Abilitato
Restrizioni Dtrace	Abilitato	Abilitato
Firma Kext	Abilitato	Abilitato

	Istanze Mac con processore Apple	Istanze Mac x86
Protezioni Nvram	Abilitato	Abilitato

Controllo della configurazione SIP

Consigliamo di controllare la configurazione SIP prima e dopo aver apportato le modifiche per assicurarti che sia configurata come previsto.

Per verificare la configurazione SIP di un'istanza Mac di Amazon EC2

Connettiti all'istanza tramite SSH, quindi esegui il comando seguente nella riga di comando.

```
$ csrutil status
```

Di seguito è riportato un output di esempio.

```
System Integrity Protection status: enabled.

Configuration:
    Apple Internal: enabled
    Kext Signing: disabled
    Filesystem Protections: enabled
    Debugging Restrictions: enabled
    DTrace Restrictions: enabled
    NVRAM Protections: enabled
    BaseSystem Verification: disabled
```

Prerequisiti per istanze Mac con processore Apple

Prima di poter configurare le impostazioni SIP per le istanze Mac con processore Apple, devi impostare una password e abilitare il token sicuro per l'utente amministrativo del volume root Amazon EBS (`ec2-user`),

> **Note**
>
> La password e il token sicuro vengono impostati la prima volta che ti connetti a un'istanza Mac con processore Apple utilizzando l'interfaccia grafica (GUI). Se in precedenza hai

effettuato la connessione all'istanza utilizzando la GUI o stai usando un'istanza Mac x86 non devi eseguire questi passaggi.

> **Note**
>
> Tutti i nomi utente e le password macOS utilizzati per l'autenticazione macOS devono contenere tra 4 e 16 caratteri per l'utilizzo con le chiamate API delle impostazioni SIP.

Per impostare una password e abilitare il token sicuro per l'utente amministrativo del volume root EBS

1. Connettiti all'istanza tramite SSH.
2. Imposta la password per l'utente `ec2-user`.

```
$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
```

3. Abilita il token sicuro per l'utente `ec2-user`. In `-oldPassword`, specifica la stessa password del passaggio precedente. In `-newPassword`, specifica una password diversa. Il comando seguente presuppone che la vecchia e la nuova password siano salvate nei file `.txt`.

```
$ sysadminctl -oldPassword `cat old_password.txt` -newPassword `cat
 new_password.txt`
```

4. Verifica che il token sicuro sia abilitato.

```
$ sysadminctl -secureTokenStatus ec2-user
```

Configurazione delle impostazioni SIP

Quando configuri le impostazioni SIP per la tua istanza, puoi abilitare o disabilitare tutte le impostazioni SIP oppure puoi specificare una configurazione personalizzata che abiliti o disabiliti selettivamente impostazioni SIP specifiche.

> **Note**
>
> Se implementi una configurazione personalizzata, connettiti all'istanza e verifica le impostazioni per assicurarti che i requisiti siano implementati correttamente e funzionino come previsto.
> Le configurazioni SIP potrebbero cambiare con gli aggiornamenti di macOS. Consigliamo di rivedere le impostazioni SIP personalizzate dopo ogni aggiornamento della versione di macOS per garantire la compatibilità continua e la corretta funzionalità delle configurazioni di sicurezza.

Per configurare le impostazioni SIP per la tua istanza, devi creare un'attività di configurazione SIP. L'attività di configurazione SIP specifica le impostazioni SIP per l'istanza.

Quando crei una configurazione SIP per un'istanza Mac con processore Apple, devi specificare le credenziali seguenti:

- Utente amministrativo del disco interno
  - Nome utente: solo l'utente amministrativo predefinito (`aws-managed-user`) è supportato e viene utilizzato per impostazione predefinita. Non puoi specificare un utente amministrativo diverso.
  - Password: se non hai modificato la password predefinita per `aws-managed-user`, specifica la password predefinita, che è vuota. Altrimenti, specifica la password.
- Utente amministrativo del volume root Amazon EBS
  - Nome utente: se non hai modificato l'utente amministrativo predefinito, specifica `ec2-user`. Altrimenti, specifica il nome utente per l'utente amministrativo.
  - Password: devi specificare sempre la password.

Utilizza i seguenti metodi per creare un'attività di configurazione SIP.

Console

Per creare una configurazione SIP tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione a sinistra, scegli Istanze, quindi seleziona l'istanza Mac di Amazon EC2.

3. Nella scheda Sicurezza, scegli Modifica Mac, Modifica System Integrity Protection.
4. Per abilitare tutte le impostazioni SIP, seleziona Abilita SIP. Per disabilitare tutte le impostazioni SIP, deseleziona Abilita SIP.
5. Per specificare una configurazione personalizzata che abiliti o disabiliti selettivamente impostazioni SIP specifiche, seleziona Specifica una configurazione SIP personalizzata, quindi seleziona o deseleziona le impostazioni SIP da abilitare o disabilitare.
6. Specifica le credenziali per l'utente del volume root e il proprietario del disco interno.
7. Scegli Crea attività di modifica SIP.

AWS CLI

Per creare un'attività di configurazione SIP utilizzando AWS CLI

Utilizza il comando create-mac-system-integrity-protection-modification-task.

Abilitazione o disabilitazione di tutte le impostazioni SIP

Per abilitare o disabilitare completamente tutte le impostazioni SIP, utilizza solo il parametro `--mac-system-integrity-protection-status`.

Il comando di esempio seguente abilita tutte le impostazioni SIP.

```
aws ec2 create-mac-system-integrity-protection-modification-task \
--instance-id i-0abcdef9876543210 \
--mac-system-integrity-protection-status enabled \
--mac-credentials file://mac-credentials.json
```

Specificazione di una configurazione SIP personalizzata

Per specificare una configurazione SIP personalizzata che abilita o disabilita selettivamente determinate impostazioni SIP, specifica i parametri `--mac-system-integrity-protection-status` e `--mac-system-integrity-protection-configuration`. In questo caso, utilizza `mac-system-integrity-protection-status` per specificare lo stato SIP generale e usa `mac-system-integrity-protection-configuration` per abilitare o disabilitare selettivamente le singole impostazioni SIP.

Il comando di esempio seguente crea un'attività di configurazione SIP per abilitare tutte le impostazioni SIP, tranne `NvramProtections` e `FilesystemProtections`.

```
aws ec2 create-mac-system-integrity-protection-modification-task \
--instance-id i-0abcdef9876543210 \
--mac-system-integrity-protection-status enabled \
--mac-system-integrity-protection-configuration
 "NvramProtections=disabled, FilesystemProtections=disabled" \
--mac-credentials file://mac-credentials.json
```

Il comando di esempio seguente crea un'attività di configurazione SIP per disabilitare tutte le impostazioni SIP, tranne `DtraceRestrictions`.

```
aws ec2 create-mac-system-integrity-protection-modification-task \
--instance-id i-0abcdef9876543210 \
--mac-system-integrity-protection-status disabled \
--mac-system-integrity-protection-configuration "DtraceRestrictions=enabled" \
--mac-credentials file://mac-credentials.json
```

Contenuto del file mac-credentials.json

I seguenti contenuti fanno parte del file `mac-credentials.json` indicato negli esempi precedenti.

```
{
  "internalDiskPassword":"internal-disk-admin_password",
  "rootVolumeUsername":"root-volume-admin_username",
  "rootVolumePassword":"root-volume-admin_password"
}
```

Controllo dello stato dell'attività di configurazione SIP

Utilizza uno dei seguenti metodi per verificare lo stato delle attività di configurazione SIP.

Console

Per visualizzare le attività di configurazione SIP tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione a sinistra, scegli Istanze, quindi seleziona l'istanza Mac di Amazon EC2.
3. Nella scheda Sicurezza, scorri verso il basso fino alla sezione Attività di modifica Mac.

AWS CLI

Per verificare lo stato delle attività di configurazione SIP utilizzando AWS CLI

Utilizza il comando describe-mac-modification-tasks.

Trova le versioni macOS supportate per il tuo host dedicato Mac Amazon EC2

Puoi visualizzare le ultime versioni di macOS supportate dall'host dedicato Mac Amazon EC2. Con questa funzionalità, puoi verificare se l'host dedicato è in grado di supportare il lancio di istanze con le tue versioni macOS preferite.

Ogni versione di macOS richiede una versione firmware minima sull'Apple Mac sottostante per un avvio corretto. La versione del firmware per Apple Mac può diventare obsoleta se un host dedicato Mac è rimasto inattivo per un periodo di tempo prolungato o se contiene un'istanza in esecuzione da molto tempo.

Per garantire il supporto delle ultime versioni di macOS, puoi interrompere o terminare le istanze sull'host dedicato Mac allocato. Ciò attiva il flusso di lavoro di pulizia dell'host e aggiorna il firmware sull'Apple Mac sottostante per supportare le ultime versioni di macOS. Un host dedicato con un'istanza di lunga durata verrà aggiornato automaticamente quando interrompi o termini un'istanza in esecuzione.

Per ulteriori informazioni sui flussi di lavoro, consulta Come terminare l'istanza Mac di Amazon EC2.

Per ulteriori informazioni sull'avvio di istanze Mac, consulta Avvia un'istanza Mac utilizzando Console di gestione AWS o AWS CLI.

Puoi visualizzare informazioni sulle ultime versioni di macOS supportate sull'host dedicato allocato utilizzando la console Amazon EC2 o la AWS CLI.

Console

Per visualizzare le informazioni sul firmware dell'host dedicato utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Nella pagina Dettagli host dedicati, in Ultime versioni macOS supportate, puoi vedere le ultime versioni di macOS supportate dall'host.

AWS CLI

Per visualizzare le informazioni sul firmware dell'host dedicato utilizzando AWS CLI

Utilizzare il comando `describe-mac-hosts`, sostituendo `region` con la Regione AWS appropriata.

```
$ aws ec2 describe-mac-hosts --region us-east-1
  {
      "MacHosts": [
          {
              "HostId": "h-07879acf49EXAMPLE",
              "MacOSLatestSupportedVersions": [
                  "14.3",
                  "13.6.4",
                  "12.7.3"
              ]
          }
      ]
  }
```

Sottoscrizione alle notifiche delle AMI macOS

Per ricevere una notifica quando vengono rilasciate nuove AMI o quando bridgeOS è stato aggiornato, sottoscrivi le notifiche tramite Amazon SNS.

Per ulteriori informazioni sulle AMI EC2 macOS, consulta Note di rilascio delle AMI macOS di Amazon EC2.

Come sottoscrivere le notifiche delle AMI macOS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. È necessario utilizzare questa regione in quanto le notifiche SNS per le quali hai effettuato la sottoscrizione sono state create in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
4. Scegli Create Subscription (Crea sottoscrizione).
5. Nella finestra di dialogo Create subscription (Crea sottoscrizione) eseguire le seguenti operazioni:

a. In Topic ARN (ARN argomento) copiare e incollare uno dei seguenti nome della risorsa Amazon (ARN):

   - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-macos-ami-updates`**
   - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-bridgeos-updates`**

b. Per Protocollo), scegli una delle seguenti opzioni:

   - E-mail:

     In Endpoint digita l'indirizzo e-mail utilizzabile per ricevere le notifiche. Dopo aver creato la sottoscrizione, riceverai un messaggio di conferma con oggetto `AWS Notification - Subscription Confirmation`. Apri l'e-mail e seleziona Conferma sottoscrizione per completare la sottoscrizione.

   - SMS:

     In Endpoint digita un numero di telefono utilizzabile per ricevere le notifiche.

   - AWS Lambda, Amazon SQS, Amazon Data Firehose (le notifiche arriveranno in formato JSON):

     Per Endpoint inserisci l'ARN per la funzione Lambda, la coda SQS o il flusso Firehose utilizzabile per ricevere le notifiche.

c. Scegli Create Subscription (Crea sottoscrizione).

Quando le AMI macOS vengono rilasciate, inviamo notifiche ai sottoscrittori dell'argomento `amazon-ec2-macos-ami-updates`. Quando bridgeOS viene aggiornato, verranno inviate notifiche ai sottoscrittori dell'argomento `amazon-ec2-bridgeos-updates`. Se non desideri più ricevere queste notifiche, segui la procedura seguente per annullare la sottoscrizione.

Annullamento della sottoscrizione alle notifiche delle AMI macOS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. È necessario utilizzare questa regione in quanto le notifiche SNS sono state create in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).

4. Selezionare la sottoscrizione, quindi selezionare Actions (Operazioni), Delete subscriptions (Cancella sottoscrizioni). Quando viene richiesta la conferma, selezionare Delete (Cancella).

Recupera gli ID AMI di macOS utilizzando AWS Systems Manager API Parameter Store

Devi specificare un'AMI quando avvii un'istanza. Un'AMI è specifica per un'architettura Regione AWS del sistema operativo e del processore. Puoi visualizzare tutte le AMI macOS in un file Regione AWS e recuperare l'AMI macOS più recente interrogando l'API Parameter Store. AWS Systems Manager Con questi parametri pubblici non è necessario eseguire una ricerca manuale degli ID delle AMI macOS. I parametri pubblici sono disponibili per entrambe le AMI x86 e ARM64 macOS e possono essere integrati con i modelli esistenti. AWS CloudFormation

Autorizzazioni richieste

Per eseguire questa azione, il principale IAM deve disporre delle autorizzazioni per richiamare l'azione API `ssm:GetParameter`.

Per visualizzare un elenco di tutte le AMI macOS presenti nella versione corrente Regione AWS utilizzando AWS CLI

Usa il comando get-parameters-by-path per visualizzare un elenco di tutte le AMI macOS nella Regione attuale.

```
aws ssm get-parameters-by-path --path /aws/service/ec2-macos --recursive --query
 "Parameters[].Name"
```

Per recuperare l'ID AMI della principale AMI macOS più recente utilizzando AWS CLI

Usa il seguente comando get-parameter con il sottoparametro `image_id`. Nell'esempio seguente, sostituiscilo `sonoma` con una versione principale supportata da macOS, `x86_64_mac` con il processore e `region-code` con una supportata Regione AWS per la quale desideri l'ID macOS AMI più recente.

```
aws ssm get-parameter --name /aws/service/ec2-macos/sonoma/x86_64_mac/latest/image_id
 --region region-code
```

Per ulteriori informazioni, consulta Ricerca dei parametri pubblici AMI per macOS nella Guida per l'utente di AWS Systems Manager .

Note di rilascio delle AMI macOS di Amazon EC2

Le seguenti informazioni forniscono dettagli sui pacchetti inclusi di default nelle AMI macOS EC2 e riepilogano le modifiche per ogni versione di macOS AMI EC2.

Per informazioni su come abbonarsi alle notifiche dell'AMI macOS, consulta Sottoscrizione alle notifiche delle AMI macOS.

Le istanze Mac possono essere eseguite su uno dei seguenti sistemi operativi:

- macOS Mojave (versione 10.14) (solo istanze Mac x86)
- macOS Catalina (versione 10.15) (solo istanze Mac x86)
- macOS Big Sur (versione 11) (istanze x86 e Mac M1)
- macOS Monterey (versione 12) (istanze x86 e Mac M1)
- macOS Ventura (versione 13) (tutte le istanze Mac, le istanze Mac M2 e M2 Pro supportano macOS Ventura versione 13.2 o successiva)
- macOS Sonoma (versione 14) (tutte le istanze Mac)
- macOS Sequoia (versione 15) (tutte le istanze Mac)

> **Note**
>
> Le istanze Mac M4 e M4 Pro supportano macOS Sequoia versione 15.6 o successiva.

Approva le politiche sulla privacy della rete locale per macOS Sequoia

macOS Sequoia (versione 15) ha una nuova funzionalità Local Network Privacy che influisce sugli utenti dei IP-based servizi locali, incluso Amazon EC2 Instance Metadata Service (IMDS).

> **Important**
>
> Per assicurarti di avere un accesso ininterrotto ai IP-based servizi locali, segui i passaggi seguenti per approvare le politiche sulla privacy della rete locale.

Per approvare le politiche sulla privacy della rete locale

1. Connessione all'interfaccia utente grafica (GUI) dell'istanza.

2. Segui le istruzioni sullo schermo per approvare le politiche sulla privacy della rete locale.
3. Dopo aver approvato le politiche, crea un'AMI della tua istanza Mac EC2. Per ulteriori informazioni, consulta Crea un' EBS-backed AMI Amazon.

Tutte le istanze Mac EC2 lanciate dall'AMI appena creata manterranno le autorizzazioni di privacy della rete locale.

Pacchetti predefiniti inclusi nelle AMI macOS di Amazon EC2

La tabella seguente descrive i pacchetti inclusi per impostazione predefinita nelle AMI macOS EC2.

Pacchetti	Note di rilascio
EC2 macOS Init	https://github.com/aws/ec2-macos-init/tags
EC2 macOS Utils	https://github.com/aws/ec2-macos-utils/tags
Amazon Agente SSM	https://github.com/aws/amazon-ssm-agent/releases
AWS Command Line Interface (AWS CLI) versione 2	https://raw.githubusercontent.com/aws/aws-cli/v2/CHANGELOG.rst
Strumenti della riga di comando per Xcode	https://developer.apple.com/documentation/xcode-release-notes
Homebrew	https://github.com/Homebrew/brew/releases
EC2 Instance Connect	https://github.com/aws/aws-ec2-instance-connect-config/releases
Safari	https://developer.apple.com/documentation/safari-release-notes

Aggiornamenti delle AMI macOS di Amazon EC2

La tabella seguente descrive le modifiche incluse nelle versioni dell'AMI macOS EC2. Alcune modifiche vengono applicate a tutte le AMI macOS EC2, mentre altre vengono applicate a un sottoinsieme di tali AMI.

Aggiornamenti delle AMI macOS EC2

Versione	Modifiche
2026.09.02	Tutte le AMI • Aggiornato alla 2.36.36 `awscli` • Homebrew aggiornato alla versione 6.0.20 Rilascio di macOS Sonoma 14.8.9 (Apple silicon) • Contenuti di sicurezza di macOS Sonoma 14.8.9 • Safari aggiornato alla versione 26.6.1 • Contenuto di sicurezza di Safari 26.6.1 Rilascio di macOS Tahoe 26.6.2 • Contenuti di sicurezza di macOS Tahoe 26.6.2

2026.08.26	Tutte le AMI
	• Aggiornato alla 2.36.27 `awscli`
	• Homebrew aggiornato alla versione 6.0.18
	
	Rilascio di macOS Sonoma 14.8.9 (solo Intel, mac1.metal)
	• Contenuti di sicurezza di macOS Sonoma 14.8.9
	• Safari aggiornato alla versione 26.6.1
	  • Contenuto di sicurezza di Safari 26.6.1
	
	Rilascio di macOS Sequoia 15.7.9
	• Contenuto di sicurezza di macOS Sequoia 15.7.9
	• Safari aggiornato alla versione 26.6.1
	  • Contenuto di sicurezza di Safari 26.6.1

Versione	Modifiche
	Rilascio di macOS Tahoe 26.6.1 • Contenuti di sicurezza di macOS Tahoe 26.6.1

2026.08.13	Tutte le AMI
	• Aggiornato alla 2.36.12 `awscli`
	• Homebrew aggiornato alla versione 6.0.13
	
	Rilascio di macOS Sonoma 14.8.8 (solo Intel, mac1.metal)
	• Contenuti di sicurezza di macOS Sonoma 14.8.8
	• Safari aggiornato alla versione 26.6
	  • Contenuto di sicurezza di Safari 26.6
	
	Rilascio di macOS Sequoia 15.7.8
	• Contenuto di sicurezza di macOS Sequoia 15.7.8
	• Safari aggiornato alla versione 26.6
	  • Contenuto di sicurezza di Safari 26.6
	
	Rilascio di macOS Tahoe 26.6
	• Contenuti di sicurezza di macOS Tahoe 26.6
	• Strumenti a riga di comando aggiornati alla versione 26.6

2026.07.29	Rilascio di macOS Tahoe 26.5.2 • Contenuti di sicurezza di macOS Tahoe 26.5.2 • `awscli`Aggiornato alla 2.36.1 • Homebrew aggiornato alla versione 6.0.11

Versione	Modifiche

2026.05.19	Tutte le AMI
	• Aggiornato alla 2.34.46 `awscli`
	• Homebrew aggiornato alla 5.1.11
	
	Rilascio di macOS Sonoma 14.8.7
	• Contenuti di sicurezza di macOS Sonoma 14.8.7
	• Safari aggiornato alla versione 26.5
	  • Contenuto di sicurezza di Safari 26.5
	
	Rilascio di macOS Sequoia 15.7.7
	• Contenuto di sicurezza di macOS Sequoia 15.7.7
	• Safari aggiornato alla versione 26.5
	  • Contenuto di sicurezza di Safari 26.5
	
	Rilascio di macOS Tahoe 26.5
	• Contenuti di sicurezza di macOS Tahoe 26.5
	• Strumenti da riga di comando aggiornati alla versione 26.5

2026.04.20	Rilascio di macOS Tahoe 26.4.1 • Contenuti di sicurezza di macOS Tahoe 26.4.1 • Strumenti a riga di comando aggiornati alla versione 26.4.1 • Aggiornato `awscli` alla 2.34.32 • Homebrew aggiornato alla versione 5.1.7

Versione	Modifiche

2026.04.16	Tutte le AMI
	• Aggiornato a 2.34.27 `awscli`
	• Aggiornato `ec2-macos-init` alla 1.5.15
	• Homebrew aggiornato alla 5.1.5
	
	Rilascio di macOS Sonoma 14.8.5
	• Contenuto di sicurezza di macOS Sonoma 14.8.5
	• Safari aggiornato alla versione 26.4
	  • Contenuto di sicurezza di Safari 26.4
	
	Rilascio di macOS Sequoia 15.7.5
	• Contenuto di sicurezza di macOS Sequoia 15.7.5
	• Safari aggiornato alla versione 26.4
	  • Contenuto di sicurezza di Safari 26.4
	
	Rilascio di macOS Tahoe 26.4
	• Contenuti di sicurezza di macOS Tahoe 26.4
	• Strumenti a riga di comando aggiornati alla versione 26.4

2026.03.17	Rilascio di macOS Tahoe 26.3.1 • Cosa c'è di nuovo negli aggiornamenti per macOS Tahoe 26 • Strumenti da riga di comando aggiornati alla versione 26.3 • Aggiornato `awscli` alla 2.34.10 • Homebrew aggiornato alla versione 5.1.0

Versione	Modifiche

2026.03.03	Tutte le AMI
	• Aggiornato alla 2.33.31 `awscli`
	• Homebrew aggiornato alla 5.0.15
	
	Rilascio di macOS Sonoma 14.8.4
	• Contenuto di sicurezza di macOS Sonoma 14.8.4
	• Safari aggiornato alla versione 26.3
	  • Contenuto di sicurezza di Safari 26.3
	
	Rilascio di macOS Sequoia 15.7.4
	• Contenuto di sicurezza di macOS Sequoia 15.7.4
	• Safari aggiornato alla versione 26.3
	  • Contenuto di sicurezza di Safari 26.3
	
	Rilascio di macOS Tahoe 26.3
	• Contenuti di sicurezza di macOS Tahoe 26.3

Versione	Modifiche

2025.12.26	Tutte le AMI
	• Aggiornato alla 2.32.19 `awscli`
	• Aggiornato `amazon-ssm-agent` a 3.3.3270.0
	• Homebrew aggiornato alla versione 5.0.6
	
	Rilascio di macOS Sonoma 14.8.3
	• Contenuto di sicurezza di macOS Sonoma 14.8.3
	• Safari aggiornato alla versione 26.2
	  • Contenuto di sicurezza di Safari 26.2
	
	Rilascio di macOS Sequoia 15.7.3
	• Contenuto di sicurezza di macOS Sequoia 15.7.3
	• Safari aggiornato alla versione 26.2
	  • Contenuto di sicurezza di Safari 26.2
	• Strumenti da riga di comando aggiornati alla versione 26.2
	
	Rilascio di macOS Tahoe 26.2
	• Contenuti di sicurezza di macOS Tahoe 26.2
	• Strumenti a riga di comando aggiornati alla versione 26.2

Versione	Modifiche

2025.12.17	Tutte le AMI
	• Aggiornato alla 2.32.16 `awscli`
	• Homebrew aggiornato alla 5.0.5
	
	Rilascio di macOS Sonoma 14.8.2
	• Contenuto di sicurezza di macOS Sonoma 14.8.2
	• Safari aggiornato alla versione 26.1
	  • Contenuto di sicurezza di Safari 26.1
	
	Rilascio di macOS Sequoia 15.7.2
	• Contenuto di sicurezza di macOS Sequoia 15.7.2
	• Safari aggiornato alla versione 26.1
	  • Contenuto di sicurezza di Safari 26.1
	• Strumenti da riga di comando aggiornati alla versione 26.1
	
	Rilascio di macOS Tahoe 26.1
	• Contenuti di sicurezza di macOS Tahoe 26.1
	• Strumenti a riga di comando aggiornati alla versione 26.1

Versione	Modifiche

2025.11.18	Tutte le AMI
	• Aggiornato alla versione 2.31.35 `awscli`
	• Aggiornato `ec2-macos-init` alla 1.5.13
	• Aggiornato `ec2-macos-utils` alla 1.0.7
	• Homebrew aggiornato alla versione 5.0.1
	
	Rilascio di macOS Sonoma 14.8.1
	• Contenuto di sicurezza di macOS Sonoma 14.8.1
	• Safari aggiornato alla 26.0.1
	  • Contenuto di sicurezza di Safari 26.0.1
	
	Rilascio di macOS Sequoia 15.7.1
	• Contenuto di sicurezza di macOS Sequoia 15.7.1
	• Safari aggiornato alla versione 26.0.1
	  • Contenuto di sicurezza di Safari 18.6
	• Strumenti da riga di comando aggiornati alla versione 26.0
	
	Rilascio di macOS Tahoe 26.0.1
	• Contenuti di sicurezza di macOS Tahoe 26.0.1
	• Strumenti a riga di comando aggiornati alla versione 26.0

Versione	Modifiche
2025.09.04	Tutte le AMI • Aggiornato al 2.28.19 `awscli` • Aggiornato `ec2-instance-connect` alla 2.0.0-5 • Homebrew aggiornato alla versione 4.6.7 Rilascio di macOS Ventura 13.7.8 • Contenuti di sicurezza di macOS Ventura 13.7.8 Rilascio di macOS Sonoma 14.7.8 • Contenuto di sicurezza di macOS Sonoma 14.7.8 Rilascio di macOS Sequoia 15.6.1 • Contenuto di sicurezza di macOS Sequoia 15.6.1

Versione	Modifiche

2025.08.05	Tutte le AMI
	• Aggiornato `awscli` alla versione 2.28.0
	• Homebrew aggiornato alla versione 4.5.13
	
	Rilascio di macOS Ventura 13.7.7
	• Contenuti di sicurezza di macOS Ventura 13.7.7
	• Safari aggiornato alla versione 18.6
	  • Contenuto di sicurezza di Safari 18.6
	
	Rilascio di macOS Sonoma 14.7.7
	• Contenuto di sicurezza di macOS Sonoma 14.7.7
	• Safari aggiornato alla versione 18.6
	  • Contenuto di sicurezza di Safari 18.6
	
	Rilascio di macOS Sequoia 15.6
	• Contenuto di sicurezza di macOS Sequoia 15.6
	• AWS ENA Ethernet aggiornato alla versione 2.0.0

Versione	Modifiche

2025.06.27	Tutte le AMI
	• Aggiornato alla versione 2.27.40 `awscli`
	• Homebrew aggiornato alla versione 4.5.7
	• Immagini x86_64 migrate su RNA Ethernet dext AWS
	
	Rilascio di macOS Ventura 13.7.6
	• Contenuti di sicurezza di macOS Ventura 13.7.6
	• Safari aggiornato alla versione 18.5
	  • Contenuto di sicurezza di Safari 18.5
	
	Rilascio di macOS Sonoma 14.7.6
	• Contenuto di sicurezza di macOS Sonoma 14.7.6
	• Safari aggiornato alla versione 18.5
	  • Contenuti di sicurezza di Safari 18.5
	
	Rilascio di macOS Sequoia 15.5
	• Contenuto di sicurezza di macOS Sequoia 15.5
	• Strumenti da riga di comando aggiornati alla versione 16.4
	• AWS ENA Ethernet aggiornato alla versione 1.0.9

Versione	Modifiche

2025.05.21	Tutte le AMI
	• Aggiornato alla versione 2.27.7 `awscli`
	• Aggiornato `ec2-macos-init` alla 1.5.11
	• Aggiornato `ec2-macos-utils` alla 1.0.5
	• Homebrew aggiornato alla versione 4.5.1
	
	Rilascio di macOS Ventura 13.7.5
	• Contenuti di sicurezza di macOS Ventura 13.7.5
	• Safari aggiornato alla versione 18.4
	  • Contenuti di sicurezza di Safari 18.4
	
	Rilascio di macOS Sonoma 14.7.5
	• Contenuto di sicurezza di macOS Sonoma 14.7.5
	• Safari aggiornato alla versione 18.4
	  • Contenuti di sicurezza di Safari 18.4
	
	Rilascio di macOS Sequoia 15.4.1
	• Contenuto di sicurezza di macOS Sequoia 15.4.1
	• Strumenti a riga di comando aggiornati alla versione 16.3

Versione	Modifiche

2025.05.05	Tutte le AMI
	• Aggiornato alla 2.27.1 `awscli`
	• Aggiornato `ec2-macos-init` alla 1.5.11
	• Aggiornato `ec2-macos-system-monitor` alla 1.3.1
	• Aggiornato `ec2-macos-utils` alla 1.0.5
	• Homebrew aggiornato alla versione 4.4.32
	
	Rilascio di macOS Ventura 13.7.5
	• Contenuti di sicurezza di macOS Ventura 13.7.5
	• Safari aggiornato alla versione 18.4
	  • Contenuti di sicurezza di Safari 18.4
	
	Rilascio di macOS Sonoma 14.7.5
	• Contenuto di sicurezza di macOS Sonoma 14.7.5
	• Safari aggiornato alla versione 18.4
	  • Contenuti di sicurezza di Safari 18.4
	
	Rilascio di macOS Sequoia 15.4.1
	• Contenuto di sicurezza di macOS Sequoia 15.4.1

Versione	Modifiche
2025.03.18	Tutte le AMI • Aggiornato alla 2.24.2 `awscli` • Homebrew aggiornato alla versione 4.4.20 Rilascio di macOS Sequoia 15.3.1 • Contenuto di sicurezza di macOS Sequoia 15.3.1 Rilascio di macOS Sonoma 14.7.4 • Contenuto di sicurezza di macOS Sonoma 14.7.4 • Safari aggiornato alla versione 18.3 Rilascio di macOS Ventura 13.7.4 • Contenuti di sicurezza di macOS Ventura 13.7.4 • Safari aggiornato alla versione 18.3

Versione	Modifiche
2025.01.24	Tutte le AMI • Aggiornato alla 2.22.33 `awscli` • Homebrew aggiornato alla versione 4.4.15 Rilascio di macOS Sequoia 15.2 • Contenuto di sicurezza di macOS Sequoia 15.2 • Strumenti da riga di comando aggiornati alla versione 16.2 Rilascio di macOS Sonoma 14.7.2 • Contenuto di sicurezza di macOS Sonoma 14.7.2 • Safari aggiornato alla versione 18.2 • Strumenti da riga di comando aggiornati alla versione 16.2 Rilascio di macOS Ventura 13.7.2 • Contenuti di sicurezza di macOS Ventura 13.7.2 • Safari aggiornato alla versione 18.2

Versione	Modifiche
2024.12.20	Tutte le AMI • Homebrew aggiornato alla 4.4.8 • Aggiornato alla 2.22.5 `aws-cli` • `amazon-ssm-agent` aggiornato alla versione 3.3.987.0 Rilascio di macOS Sequoia 15.1.1 • Contenuto di sicurezza di macOS Sequoia 15.1.1 Rilascio di macOS Sonoma 14.7.1 • Contenuto di sicurezza di macOS Sonoma 14.7.1 • Safari aggiornato alla versione 18.1.1 Rilascio di macOS Ventura 13.7.1 • Contenuti di sicurezza di macOS Ventura 13.7.1 • Safari aggiornato alla versione 18.1.1

Versione	Modifiche

2024.10.28	Tutte le AMI
	• Homebrew aggiornato alla versione 4.4.2
	• `aws-cli` aggiornato alla versione 2.18.13
	• `amazon-ssm-agent` aggiornato alla versione 3.3.987.0
	• `ec2-macos-init` aggiornato alla versione 1.5.10
	• `ec2-macos-utils` aggiornato alla versione 1.0.4
	
	Rilascio di macOS Sequoia 15.0
	• Contenuti di sicurezza di macOS Sequoia 15
	
	Rilascio di macOS Sonoma 14.7
	• Contenuti di sicurezza di macOS Sonoma 14.7.
	• Strumenti riga di comando aggiornati alla versione 16.0
	• Safari aggiornato alla versione 18.0.1
	  • Contenuti di sicurezza di Safari 18
	
	Rilascio di macOS Ventura 13.7
	• Contenuti di sicurezza di macOS Ventura 13.7
	• Safari aggiornato alla versione 18.0.1
	  • Contenuti di sicurezza di Safari 18

Versione	Modifiche

2024,008,20	Tutte le AMI
	• Homebrew aggiornato alla versione 4.3.14
	• `aws-cli` aggiornato alla versione 2.17.29
	
	Rilascio di macOS Sonoma 14.6.1
	• Nessuna voce CVE pubblicata.
	
	Rilascio di macOS Ventura 13.6.9
	• Nessuna voce CVE pubblicata.
	• Safari aggiornato alla versione 17.6
	  • Contenuti di sicurezza di Safari 17.6
	
	Rilascio di macOS Monterey 12.7.6
	• Contenuti di sicurezza di macOS Monterey 12.7.6
	• Safari aggiornato alla versione 17.6
	  • Contenuti di sicurezza di Safari 17.6

Versione	Modifiche

2024,06,07	Tutte le AMI
	• Homebrew aggiornato alla versione 4.3.1-1
	• `aws-cli` aggiornato alla versione 2.15.56
	• `amazon-ssm-agent` aggiornato alla versione 3.3.380.0-1
	
	Rilascio di macOS Sonoma 14.5
	• Contenuti di sicurezza di macOS Sonoma 14.5
	
	Rilascio di macOS Ventura 13.6.7
	• Contenuti di sicurezza di macOS Ventura 13.6.7
	• Safari aggiornato alla versione 17.5
	  • Contenuti di sicurezza di Safari 17.5
	
	Rilascio di macOS Monterey 12.7.5
	• Contenuti di sicurezza di macOS Monterey 12.7.5
	• Safari aggiornato alla versione 17.5
	  • Contenuti di sicurezza di Safari 17.5

Versione	Modifiche

2024,004,12	Tutte le AMI
	• Homebrew aggiornato alla versione 4.2.16-1
	• `aws-cli` aggiornato alla versione 2.15.36
	
	Rilascio di macOS Sonoma 14.4.1
	• Contenuti di sicurezza di macOS Sonoma 14.4.1
	
	Rilascio di macOS Ventura 13.6.6
	• Contenuti di sicurezza di macOS Ventura 13.6.6
	• Safari aggiornato alla versione 17.4.1
	  • Contenuti di sicurezza di Safari 17.4.1
	
	Per macOS Monterey
	• Safari aggiornato alla versione 17.4.1
	  • Contenuti di sicurezza di Safari 17.4.1

Tipi di istanze Amazon EBS-optimized

Le istanze ottimizzate per Amazon EBS utilizzano uno stack di configurazione ottimizzato e forniscono larghezza di banda dedicata aggiuntiva per Amazon EBS. I/O Questa ottimizzazione offre le migliori prestazioni per i tuoi volumi EBS riducendo al minimo i conflitti tra Amazon EBS e altro traffico proveniente dalla tua istanza. I/O

Quando sono collegati a un'istanza ottimizzata per EBS, i volumi SSD per scopo generico (`gp2` e `gp3`) sono progettati per offrire come minimo il 90% delle prestazioni con capacità di IOPS allocata per il 99% del tempo in un dato anno, mentre i volumi SSD con capacità di IOPS allocata (`io1` e `io2`) sono progettati per offrire come minimo il 90% delle prestazioni della capacità di IOPS allocata per il 99,9% del tempo in un dato anno. Throughput Optimized HDD (`st1`) e Cold HDD (`sc1`) offrono almeno il 90% delle prestazioni di throughput previste il 99% delle volte in un determinato anno. Non-compliant i periodi sono distribuiti all'incirca in modo uniforme, con l'obiettivo di raggiungere il 99% del

throughput totale previsto ogni ora. Per ulteriori informazioni, consulta Tipi di volumi di Amazon EBS nella Guida per l'utente di Amazon EBS.

Alcuni tipi di istanza sono EBS-optimized predefiniti e non è necessario abilitarli e non hanno alcun effetto se si tenta di disabilitarli. Altri tipi di istanze supportano facoltativamente l'ottimizzazione EBS e puoi abilitarli durante o dopo l'avvio pagando una tariffa oraria aggiuntiva. Alcuni tipi di istanza non supportano l'ottimizzazione per EBS.

Per specifiche dettagliate sui tipi di istanza e sulle funzionalità, consulta la Guida ai tipi di istanza Amazon EC2.

Considerazioni

- Le prestazioni EBS di un'istanza sono limitate dai limiti di prestazioni del tipo di istanza o dalle prestazioni aggregate dei volumi collegati, a seconda di quale dei due valori sia inferiore. Per ottenere le massime prestazioni EBS, un'istanza deve disporre di volumi collegati che forniscano prestazioni combinate pari o superiori alle prestazioni massime dell'istanza. Ad esempio, per ottenere `80,000` IOPS per `r6i.16xlarge`, l'istanza deve disporre di almeno 5 volumi `gp2` forniti con `16,000` IOPS ciascuno (5 volumi x `16,000` IOPS = `80,000` IOPS), oppure può disporre di 1 volumi `gp3` forniti con `80,000` IOPS. Consigliamo di scegliere un tipo di istanza ottimizzata per EBS in grado di fornire una quantità maggiore di throughput dedicato Amazon EBS rispetto alle esigenze dell'applicazione. In caso contrario, la connessione tra Amazon EBS e Amazon EC2 può trasformarsi un collo di bottiglia delle prestazioni.
- Il numero massimo di volumi Amazon EBS che puoi collegare a un'istanza dipende dal tipo e dalle dimensioni dell'istanza. Per ulteriori informazioni, consulta Limiti di volume di Amazon EBS per le istanze Amazon EC2.
- I limiti massimi di IOPS e di throughput sono interdipendenti. A seconda delle I/O dimensioni, potresti raggiungere un limite prima dell'altro, il che può influire sulle prestazioni complessive. Per risultati ottimali, tieni in considerazione entrambi i limiti quando pianifichi il carico di lavoro.

EBS-optimized per impostazione predefinita

I seguenti tipi di istanza sono ottimizzati per EBS per impostazione predefinita. Non è necessario abilitare l'ottimizzazione EBS e, se la si disabilita, non si ottiene alcun effetto.

Istanze

- Uso generale
- Calcolo ottimizzato

- Memoria ottimizzata
- Archiviazione ottimizzata
- Elaborazione accelerata
- High-performance informatica

Uso generale

> **Note**
>
> I tipi di istanza M8a, M8g, M8gd, M8i, M8id, M9g, M9gd supportano ponderazioni configurabili della larghezza di banda M8i-flex. Con questi tipi di istanze, puoi ottimizzare la larghezza di banda di un'istanza per le prestazioni di rete o per le prestazioni di Amazon EBS. La tabella seguente mostra le prestazioni di banda larga predefinite di Amazon EBS per questi tipi di istanze. Per ulteriori informazioni, consulta Configurazione della ponderazione della larghezza di banda dell'istanza EC2.

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
a1.medium [1]	300	3500	37,50	437,50	2500	20000
a1.large [1]	525	3500	65,62	437,50	4000	20000
a1.xlarge [1]	800	3500	100,00	437,50	6000	20000
a1.2xlarge [1]	1750	3500	218,75	437,50	10000	20000
a1.4xlarge [2]	3500		437,5		20000	
a1.metal [2]	3500		437,5		20000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m4.large [2]	450		56,25		3600	
m4.xlarge [2]	750		93,75		6000	
m4.2xlarge [2]	1000		125,0		8000	
m4.4xlarge [2]	2000		250,0		16000	
m4.10xlarge [2]	4000		500,0		32000	
m4.16xlarge [2]	10000		1250,0		65000	
m5.large [1]	650	4750	81,25	593,75	3600	18750
m5.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5.4xlarge [2]	4750		593,75		18750	
m5.8xlarge [2]	6800		850,0		30000	
m5.12xlarge [2]	9500		1187.5		40000	
m5.16xlarge [2]	13600		1700,0		60000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m5.24xlarge [2]	19000		2375,0		80000	
m5.metal [2]	19000		2375,0		80000	
m5a.large [1]	650	2880	81,25	360,00	3600	16000
m5a.xlarge [1]	1085	2880	135,62	360,00	6000	16000
m5a.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
m5a.4xlarge [2]	2880		360,0		16000	
m5a.8xlarge [2]	4750		593,75		20000	
m5a.12xlarge [2]	6780		847,5		30000	
m5a.16xlarge [2]	9500		1187.5		40000	
m5a.24xlarge [2]	13750		1718,75		60000	
m5ad.large [1]	650	2880	81,25	360,00	3600	16000
m5ad.xlarge [1]	1085	2880	135,62	360,00	6000	16000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m5ad.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
m5ad.4xlarge [2]	2880		360,0		16000	
m5ad.8xlarge [2]	4750		593,75		20000	
m5ad.12xlarge [2]	6780		847,5		30000	
m5ad.16xlarge [2]	9500		1187.5		40000	
m5ad.24xlarge [2]	13750		1718,75		60000	
m5d.large [1]	650	4750	81,25	593,75	3600	18750
m5d.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5d.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5d.4xlarge [2]	4750		593,75		18750	
m5d.8xlarge [2]	6800		850,0		30000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m5d.12xlarge [2]	9500		1187.5		40000	
m5d.16xlarge [2]	13600		1700,0		60000	
m5d.24xlarge [2]	19000		2375,0		80000	
m5d.metal [2]	19000		2375,0		80000	
m5dn.large [1]	650	4750	81,25	593,75	3600	18750
m5dn.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5dn.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5dn.4xlarge [2]	4750		593,75		18750	
m5dn.8xlarge [2]	6800		850,0		30000	
m5dn.12xlarge [2]	9500		1187.5		40000	
m5dn.16xlarge [2]	13600		1700,0		60000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m5dn.24xlarge [2]	19000		2375,0		80000	
m5dn.metal [2]	19000		2375,0		80000	
m5n.large [1]	650	4750	81,25	593,75	3600	18750
m5n.xlarge [1]	1150	4750	143,75	593,75	6000	18750
m5n.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5n.4xlarge [2]	4750		593,75		18750	
m5n.8xlarge [2]	6800		850,0		30000	
m5n.12xlarge [2]	9500		1187.5		40000	
m5n.16xlarge [2]	13600		1700,0		60000	
m5n.24xlarge [2]	19000		2375,0		80000	
m5n.metal [2]	19000		2375,0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m5zn.large [1]	800	3170	100,00	396,25	3333	13333
m5zn.xlarge [1]	1564	3170	195,50	396,25	6667	13333
m5zn.2xlarge [2]	3170		396,25		13333	
m5zn.3xlarge [2]	4750		593,75		20000	
m5zn.6xlarge [2]	9500		1187.5		40000	
m5zn.12xlarge [2]	19000		2375,0		80000	
m5zn.metal [2]	19000		2375,0		80000	
m6a.large [1]	650	10000	81,25	1250,00	3600	40000
m6a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m6a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m6a.8xlarge [2]	10000		1250,0		40000	
m6a.12xlarge [2]	15000		1875,0		60000	
m6a.16xlarge [2]	20000		2500,0		80000	
m6a.24xlarge [2]	30000		3750,0		120000	
m6a.32xlarge [2]	40000		5000,0		160000	
m6a.48xlarge [2]	40000		5000,0		240000	
m6a.metal [2]	40000		5000,0		240000	
m6g.medium [1]	315	4750	39,38	593,75	2500	20000
m6g.large [1]	630	4750	78,75	593,75	3600	20000
m6g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
m6g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m6g.4xlarge [2]	4750		593,75		20000	
m6g.8xlarge [2]	9500		1187.5		40000	
m6g.12xlarge [2]	14250		1781,25		50000	
m6g.16xlarge [2]	19000		2375,0		80000	
m6g.metal [2]	19000		2375,0		80000	
m6gd.medium [1]	315	4750	39,38	593,75	2500	20000
m6gd.large [1]	630	4750	78,75	593,75	3600	20000
m6gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
m6gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
m6gd.4xlarge [2]	4750		593,75		20000	
m6gd.8xlarge [2]	9500		1187.5		40000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m6gd.12xlarge [2]	14250		1781,25		50000	
m6gd.16xlarge [2]	19000		2375,0		80000	
m6gd.metal [2]	19000		2375,0		80000	
m6i.large [1]	650	10000	81,25	1250,00	3600	40000
m6i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m6i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6i.8xlarge [2]	10000		1250,0		40000	
m6i.12xlarge [2]	15000		1875,0		60000	
m6i.16xlarge [2]	20000		2500,0		80000	
m6i.24xlarge [2]	30000		3750,0		120000	
m6i.32xlarge [2]	40000		5000,0		160000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m6i.metal [2]	40000		5000,0		160000	
m6id.large [1]	650	10000	81,25	1250,00	3600	40000
m6id.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m6id.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6id.8xlarge [2]	10000		1250,0		40000	
m6id.12xlarge [2]	15000		1875,0		60000	
m6id.16xlarge [2]	20000		2500,0		80000	
m6id.24xlarge [2]	30000		3750,0		120000	
m6id.32xlarge [2]	40000		5000,0		160000	
m6id.metal [2]	40000		5000,0		160000	
m6idn.large [1]	1562	25000	195,31	3125,00	6250	100000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m6idn.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
m6idn.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
m6idn.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
m6idn.8xlarge [2]	25000		3125,0		100000	
m6idn.12xlarge [2]	37500		4687,5		150000	
m6idn.16xlarge [2]	50000		6250,0		200000	
m6idn.24xlarge [2]	75000		9375,0		300000	
m6idn.32xlarge [2]	100000		12500,0		400000	
m6idn.metal [2]	100000		12500,0		400000	
m6in.large [1]	1562	25000	195,31	3125,00	6250	100000
m6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
m6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
m6in.8xlarge [2]	25000		3125,0		100000	
m6in.12xlarge [2]	37500		4687,5		150000	
m6in.16xlarge [2]	50000		6250,0		200000	
m6in.24xlarge [2]	75000		9375,0		300000	
m6in.32xlarge [2]	100000		12500,0		400000	
m6in.metal [2]	100000		12500,0		400000	
m7a.medium [1]	325	10000	40,62	1250,00	2500	40000
m7a.large [1]	650	10000	81,25	1250,00	3600	40000
m7a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m7a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7a.8xlarge [2]	10000		1250,0		40000	
m7a.12xlarge [2]	15000		1875,0		60000	
m7a.16xlarge [2]	20000		2500,0		80000	
m7a.24xlarge [2]	30000		3750,0		120000	
m7a.32xlarge [2]	40000		5000,0		160000	
m7a.48xlarge [2]	40000		5000,0		240000	
m7a.metal-48xl [2]	40000		5000,0		240000	
m7g.medium [1]	315	10000	39,38	1250,00	2500	40000
m7g.large [1]	630	10000	78,75	1250,00	3600	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m7g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7g.8xlarge [2]	10000		1250,0		40000	
m7g.12xlarge [2]	15000		1875,0		60000	
m7g.16xlarge [2]	20000		2500,0		80000	
m7g.metal [2]	20000		2500,0		80000	
m7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
m7gd.large [1]	630	10000	78,75	1250,00	3600	40000
m7gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7gd.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7gd.8xlarge [2]	10000		1250,0		40000	
m7gd.12xlarge [2]	15000		1875,0		60000	
m7gd.16xlarge [2]	20000		2500,0		80000	
m7gd.metal [2]	20000		2500,0		80000	
m7i.large [1]	650	10000	81,25	1250,00	3600	40000
m7i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7i.8xlarge [2]	10000		1250,0		40000	
m7i.12xlarge [2]	15000		1875,0		60000	
m7i.16xlarge [2]	20000		2500,0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m7i.24xlarge [2]	30000		3750,0		120000	
m7i.48xlarge [2]	40000		5000,0		240000	
m7i.metal-24xl [2]	30000		3750,0		120000	
m7i.metal-48xl [2]	40000		5000,0		240000	
m7i-flex.large [1]	312	10000	39,06	1250,00	2500	40000
m7i-flex.xlarge [1]	625	10000	78,12	1250,00	3600	40000
m7i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6000	40000
m7i-flex.4xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7i-flex.8xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7i-flex.12xlarge 1	7500	15000	937,50	1875,00	30000	60000
m7i-flex.16xlarge 1	10000	20000	1250,00	2500,00	40000	80000
m8a.medio 1	325	10000	40,62	1250,00	2500	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m8a. grande 1	650	10000	81,25	1250,00	3600	40000
m8a.x grande 1	1250	10000	156,25	1250,00	6000	40000
m8a.2x grande 1	2500	10000	312,50	1250,00	12000	40000
m8a.4x grande 1	5000	10000	625,00	1250,00	20000	40000
m8a.8x grande 2	10000		1250,0		40000	
m8a.12x grande 2	15000		1875,0		60000	
m8a.16x grande 2	20000		2500.0		80000	
m8a.24x grande 2	30000		3750,0		120000	
m8a.48x grande 2	60000		7500,0		240000	
m8a. Metal-24xl 2	30000		3750,0		120000	
m8a.metal lo-48xl 2	60000		7500,0		240000	
m8azn.medio 1	625	15000	78,12	1875,00	2500	60000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m8azn.grande 1	1250	15000	156,25	1875,00	5000	60000
m8azn.xlarge 1	2500	15000	312,50	1875,00	10000	60000
m8azn. 3x grande 1	7500	15000	937,50	1875,00	30000	60000
m8azn. 6x grande 2	15000		1875,0		60000	
m8azn. 12 x grande 2	30000		3750,0		120000	
m8azn. 24 x grande 2	60000		7500,0		240000	
m8azn.metallo-12xl 2	30000		3750,0		120000	
m8azn.metallo-24xl 2	60000		7500,0		240000	
m8g.medium [1]	315	10000	39,38	1250,00	2500	40000
m8g.large 1	630	10000	78,75	1250,00	3600	40000
m8g.xlarge 1	1250	10000	156,25	1250,00	6000	40000
m8g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m8g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m8g.8xlarge [2]	10000		1250,0		40000	
m8g.12xlarge [2]	15000		1875,0		60000	
m8g.16xlarge [2]	20000		2500,0		80000	
m8g.24xlarge [2]	30000		3750,0		120000	
m8g.48xlarge [2]	40000		5000,0		240000	
m8g.metal-24xl [2]	30000		3750,0		120000	
m8g.metal-48xl [2]	40000		5000,0		240000	
8 gb. Medio 1	1562	25000	195,31	3125,00	7500	120000
8 gb. Grande 1	3125	25000	390,62	3125,00	15000	120000
8 gb.xlarge 1	6250	25000	781,25	3125,00	30000	120000
8 gb. 2 x grande 1	12500	25000	1562,50	3125,00	60000	120000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
8 gb. 4x large 2	25000		3125,0		120000	
8 gb. 8 x large 2	50000		6250,0		240000	
8 gb. 12 x grande 2	75000		9375,0		360000	
8 gb. 16 x large 2	100000		12500,0		480000	
8 gb. 24 x large 2	150000		18750,0		720000	
8 gb. 48 x large 2	300000		37500,0		1440000	
8 gb. Metal-24xl 2	150000		18750,0		720000	
8 gb. Metal-48xl 2	300000		37500,0		1440000	
8 mg. Medio 1	315	10000	39,38	1250,00	2500	40000
8 mg. Grande 1	630	10000	78,75	1250,00	3600	40000
m8gd.xlarge 1	1250	10000	156,25	1250,00	6000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
8 m g. 2 x grande 1	2500	10000	312,50	1250,00	12000	40000
m 8 g. 4 x grande 1	5000	10000	625,00	1250,00	20000	40000
m 8 g. 8 x grande 2	10000		1250,0		40000	
m 8 g. 12 x grande 2	15000		1875,0		60000	
m 8 g. 16 x grande 2	20000		2500.0		80000	
m8gd.24xlarge [2]	30000		3750,0		120000	
m8gd.48xlarge [2]	40000		5000,0		240000	
m8gd.metal-24xl [2]	30000		3750,0		120000	
m8gd.metal-48xl [2]	40000		5000,0		240000	
8 mg. Medio 1	760	10000	95,00	1250,00	2500	40000
8 mg. grande 1	1250	10000	156,25	1250,00	5000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m8gn.xlarge 1	2500	10000	312,50	1250,00	10000	40000
m 8 g n. 2 x grande 1	5000	10000	625,00	1250,00	20000	40000
m 8 g n. 4 x grande 2	10000		1250,0		40000	
m 8 g n. 8 x grande 2	20000		2500,0		80000	
m 8 g n. 12 x grande 2	30000		3750,0		120000	
m8 g n. 16 x grande 2	40000		5000,0		160000	
m 8 g n. 24 x grande 2	60000		7500,0		240000	
m 8 g n. 48 x grande 2	120000		15000,0		480000	
m8gn.metal-24xl 2	60000		7500,0		240000	
m8gn.metallo-48xl 2	120000		15000,0		480000	
m8i. grande 1	650	10000	81,25	1250,00	3600	40000
m8i.x grande 1	1250	10000	156,25	1250,00	6000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m8i.2x grande 1	2500	10000	312,50	1250,00	12000	40000
m8i.4x grande 1	5000	10000	625,00	1250,00	20000	40000
m8i.8x grande 2	10000		1250,0		40000	
m8i.12x grande 2	15000		1875,0		60000	
m8i.16x grande 2	20000		2500.0		80000	
m8i.24x grande 2	30000		3750,0		120000	
m8i.32x grande 2	40000		5000,0		160000	
m8i.48x grande 2	60000		7500,0		240000	
m8i.96x grande 2	80000		10000,0		480000	
m8i. Metal-48x l 2	60000		7500,0		240000	
m8i. Metal-96x l 2	80000		10000,0		480000	
m8id.large 1	650	10000	81,25	1250.00	3600	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m8id.xlarge 1	1250	10000	156,25	1250,00	6000	40000
m8 id.2x grande 1	2500	10000	312,50	1250,00	12000	40000
m8 id.4x grande 1	5000	10000	625,00	1250,00	20000	40000
m8 id.8x grande 2	10000		1250,0		40000	
m8 id.12 x grande 2	15000		1875,0		60000	
m8 id.16x grande 2	20000		2500.0		80000	
m8 id.24x grande 2	30000		3750,0		120000	
m8 id.32x grande 2	40000		5000.0		160000	
m8 id.48 x grande 2	60000		7500,0		240000	
m8 id.96 x grande 2	80000		10000,0		480000	
m8id.metallo-48xl 2	60000		7500,0		240000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m8id.metallo-96xl 2	80000		10000,0		480000	
m8i-flex.large 1	315	10000	39,38	1250,00	2500	40000
m8i-flex.xlarge 1	630	10000	78,75	1250,00	3600	40000
m8i-flex.2xlarge 1	1250	10000	156,25	1250,00	6000	40000
m8i-flex.4xlarge 1	2500	10000	312,50	1250,00	12000	40000
m8i-flex.8xlarge 1	5000	10000	625,00	1250,00	20000	40000
m8i-flex.12xlarge 1	7500	15000	937,50	1875,00	30000	60000
m8i-flex.16xlarge 1	10000	20000	1250,00	2500,00	40000	80000
8 min. Grande 1	650	10000	81,25	1250,00	3600	40000
m 8 pollici x grande 1	1250	10000	156,25	1250,00	6000	40000
m 8 pollici 2 x grande 1	2500	10000	312,50	1250,00	12000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m 8 pollici. 4 x grande 1	5000	10000	625,00	1250,00	20000	40000
m 8 pollici x grande 2	10000		1250,0		40000	
m 8 pollici 12 x grande 2	15000		1875,0		60000	
m 8 pollici 16 x grande 2	20000		2500.0		80000	
8 pollici 24 x grande 2	30000		3750,0		120000	
m 8 pollici 32 x grande 2	40000		5000,0		160000	
m 8 pollici 48 x grande 2	60000		7500,0		240000	
m 8 pollici 96 x grande 2	120000		15000,0		480000	
metallo', 8 pollici, 48 x 2	60000		7500,0		240000	
Metallo da 8 pollici, 96 x 2	120000		15000,0		480000	
m8idn.grande 1	650	10000	81,25	1250.00	3600	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m8idn.xlarge 1	1250	10000	156,25	1250,00	6000	40000
m8idn.2xgrande 1	2500	10000	312,50	1250,00	12000	40000
m8idn.4xgrande 1	5000	10000	625,00	1250,00	20000	40000
m8idn.8xgrande 2	10000		1250,0		40000	
m8idn.12xgrande 2	15000		1875,0		60000	
m8idn.16xgrande 2	20000		2500.0		80000	
m8idn.24xgrande 2	30000		3750,0		120000	
m8idn.32xgrande 2	40000		5000,0		160000	
m8idn.48xgrande 2	60000		7500,0		240000	
m8idn.96xlarge 2	120000		15000,0		480000	
m8idn.metallo-48xl 2	60000		7500,0		240000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m8idn.metallo-96xl 2	120000		15000,0		480000	
mio. Grande 1	650	10000	81,25	1250,00	3600	40000
m8ine.xlarge 1	1250	10000	156,25	1250,00	6000	40000
m8 min. 2 x grande 1	2500	10000	312,50	1250,00	12000	40000
m8 in. 4 x grande 1	5000	10000	625,00	1250,00	20000	40000
m8 in. 8 x grande 2	10000		1250,0		40000	
m8 in. 12 x grande 2	15000		1875,0		60000	
8 libbre di grandi dimensioni 1	1563	25000	195,38	3125,00	7500	120000
m8ib.xlarge 1	3125	25000	390,62	3125,00	15000	120000
m8ib.2x grande 1	6250	25000	781,25	3125,00	30000	120000
m8ib.4x grande 1	12500	25000	1562,50	3125,00	60000	120000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m8ib.8x grande 2	25000		3125.0		120000	
m8ib.12x grande 2	37500		4687,5		180000	
m8ib.16x grande 2	50000		6250,0		240000	
m8ib.24x grande 2	75000		9375,0		360000	
m8ib.32x grande 2	100000		12500,0		480000	
m8ib.48x grande 2	150000		18750,0		720000	
m8ib.96x grande 2	300000		37500,0		1440000	
m8ib.metallo-48xl 2	150000		18750,0		720000	
m8ib.metallo-96xl 2	300000		37500,0		1440000	
m8idb.grande 1	1563	25000	195,38	3125,00	7500	120000
m8idb.xlarge 1	3125	25000	390,62	3125,00	15000	120000
m8idb.2x grande 1	6250	25000	781,25	3125,00	30000	120000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m8idb.4x grande 1	12500	25000	1562,50	3125,00	60000	120000
m8idb.8x grande 2	25000		3125.0		120000	
m8idb.12xlarge 2	37500		4687,5		180000	
m8idb.16x grande 2	50000		6250,0		240000	
m8idb.24x grande 2	75000		9375,0		360000	
m8idb.32xlarge 2	100000		12500,0		480000	
m8idb.48x grande 2	150000		18750,0		720000	
m8idb.96xlarge 2	300000		37500,0		1440000	
m8idb.metallo-48xl 2	150000		18750,0		720000	
m8idb.metallo-96xl 2	300000		37500,0		1440000	
9 g. Medio 1	380	12000	47,50	1500,00	2500	48000
9 g. Grande 1	760	12000	95,00	1500,00	3600	48000
9g. x grande 1	1500	12000	187,50	1500,00	6000	48000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
9 m. 2 x grande 1	3000	12000	375,00	1500,00	12000	48000
9g. 4x grande 1	6000	12000	750,00	1500,00	24000	48000
m 9 g. 8 x grande 2	12000		1500,0		48000	
9 g. 12 x grande 2	18000		2250,0		72000	
9g. 16 x grande 2	24000		3000,0		96000	
9 g. 24 x grande 2	36000		4500,0		144000	
m 9 g. 48 x grande 2	72000		9000,0		288000	
9 g. Metallo - 48 xl 2	72000		9000,0		288000	
9 mg. Medio 1	380	12000	47,50	1500,00	2500	48000
9 mg. Grande 1	760	12000	95,00	1500,00	3600	48000
m9gd.xlarge 1	1500	12000	187,50	1500,00	6000	48000
m 9 g. 2 x grande 1	3000	12000	375,00	1500,00	12000	48000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
m 9 g. 4 x grande 1	6000	12000	750,00	1500,00	24000	48000
m 9 g. 8 x grande 2	12000		1500,0		48000	
m 9 g. 12 x grande 2	18000		2250,0		72000	
m 9 g. 16 x grande 2	24000		3000,0		96000	
m 9 g. 24 x grande 2	36000		4500,0		144000	
m 9 g. 48 x grande 2	72000		9000,0		288000	
m9gd.metallo-48xl 2	72000		9000,0		288000	
mac1.metal 2	14000		1750,0		80000	
mac2.metal 2	10000		1250,0		55000	
mac2-m1ultra.metal 2	10000		1250,0		55000	
mac2-m2.metal 2	8000		1000,0		55000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
mac2-m2pro.metal [2]	8000		1000,0		55000	
mac-m3 ultrametal 2	10000		1250,0		55000	
mac-m4.metal [2]	8000		1000,0		55000	
mac-m4pro.metal [2]	8000		1000,0		55000	
mac-m4 max.metal 2	10000		1250,0		55000	
t3.nano [1]	43	2085	5,38	260,62	250	11800
t3.micro [1]	87	2085	10,88	260,62	500	11800
t3.small [1]	174	2085	21,75	260,62	1000	11800
t3.medium [1]	347	2085	43,38	260,62	2000	11800
t3.large [1]	695	2780	86,88	347,50	4000	15700
t3.xlarge [1]	695	2780	86,88	347,50	4000	15700
t3.2xlarge [1]	695	2780	86,88	347,50	4000	15700
t3a.nano [1]	45	2085	5,62	260,62	250	11800
t3a.micro [1]	90	2085	11,25	260,62	500	11800
t3a.small [1]	175	2085	21,88	260,62	1000	11800

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
t3a.medium [1]	350	2085	43,75	260,62	2000	11800
t3a.large [1]	695	2780	86,88	347,50	4000	15700
t3a.xlarge [1]	695	2780	86,88	347,50	4000	15700
t3a.2xlarge [1]	695	2780	86,88	347,50	4000	15700
t4g.nano [1]	43	2085	5,38	260,62	250	11800
t4g.micro [1]	87	2085	10,88	260,62	500	11800
t4g.small [1]	174	2085	21,75	260,62	1000	11800
t4g.medium [1]	347	2085	43,38	260,62	2000	11800
t4g.large [1]	695	2780	86,88	347,50	4000	15700
t4g.xlarge [1]	695	2780	86,88	347,50	4000	15700
t4g.2xlarge [1]	695	2780	86,88	347,50	4000	15700

[1] Questi tipi di istanze possono sostenere le prestazioni massime per 30 minuti almeno una volta ogni 24 ore, dopodiché tornano alle prestazioni di base.

[2] Queste istanze possono mantenere le prestazioni dichiarate a tempo indeterminato. Se il carico di lavoro richiede prestazioni massime sostenute per un periodo superiore a 30 minuti, utilizza una di queste istanze.

Calcolo ottimizzato

> **Note**
>
> I tipi di istanza C8a, C8g, C8gd, C8i, C8id, C9g, C9gd supportano ponderazioni configurabili della larghezza di banda. C8i-flex Con questi tipi di istanze, puoi ottimizzare la larghezza di banda di un'istanza per le prestazioni di rete o per le prestazioni di Amazon EBS. La tabella seguente mostra le prestazioni di banda larga predefinite di Amazon EBS per questi tipi di istanze. Per ulteriori informazioni, consulta Configurazione della ponderazione della larghezza di banda dell'istanza EC2.

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c4.large [2]	500		62,5		4000	
c4.xlarge [2]	750		93,75		6000	
c4.2xlarge [2]	1000		125.0		8000	
c4.4xlarge [2]	2000		250,0		16000	
c4.8xlarge [2]	4000		500,0		32000	
c5.large [1]	650	4750	81,25	593,75	4000	20000
c5.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5.4xlarge [2]	4750		593,75		20000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c5.9xlarge [2]	9500		1187.5		40000	
c5.12xlarge [2]	9500		1187.5		40000	
c5.18xlarge [2]	19000		2375,0		80000	
c5.24xlarge [2]	19000		2375,0		80000	
c5.metal [2]	19000		2375,0		80000	
c5a.large [1]	200	3170	25,00	396,25	800	13300
c5a.xlarge [1]	400	3170	50,00	396,25	1600	13300
c5a.2xlarge [1]	800	3170	100,00	396,25	3200	13300
c5a.4xlarge [1]	1580	3170	197,50	396,25	6600	13300
c5a.8xlarge [2]	3170		396,25		13300	
c5a.12xlarge [2]	4750		593,75		20000	
c5a.16xlarge [2]	6300		787,5		26700	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c5a.24xlarge [2]	9500		1187.5		40000	
c5ad.large [1]	200	3170	25,00	396,25	800	13300
c5ad.xlarge [1]	400	3170	50,00	396,25	1600	13300
c5ad.2xlarge [1]	800	3170	100,00	396,25	3200	13300
c5ad.4xlarge [1]	1580	3170	197,50	396,25	6600	13300
c5ad.8xlarge [2]	3170		396,25		13300	
c5ad.12xlarge [2]	4750		593,75		20000	
c5ad.16xlarge [2]	6300		787,5		26700	
c5ad.24xlarge [2]	9500		1187.5		40000	
c5d.large [1]	650	4750	81,25	593,75	4000	20000
c5d.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5d.2xlarge [1]	2300	4750	287,50	593,75	10000	20000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c5d.4xlarge [2]	4750		593,75		20000	
c5d.9xlarge [2]	9500		1187.5		40000	
c5d.12xlarge [2]	9500		1187.5		40000	
c5d.18xlarge [2]	19000		2375,0		80000	
c5d.24xlarge [2]	19000		2375,0		80000	
c5d.metal [2]	19000		2375,0		80000	
c5n.large [1]	650	4750	81,25	593,75	4000	20000
c5n.xlarge [1]	1150	4750	143,75	593,75	6000	20000
c5n.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5n.4xlarge [2]	4750		593,75		20000	
c5n.9xlarge [2]	9500		1187.5		40000	
c5n.18xlarge [2]	19000		2375,0		80000	
c5n.metal [2]	19000		2375,0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c6a.large [1]	650	10000	81,25	1250,00	3600	40000
c6a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c6a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6a.8xlarge [2]	10000		1250,0		40000	
c6a.12xlarge [2]	15000		1875,0		60000	
c6a.16xlarge [2]	20000		2500,0		80000	
c6a.24xlarge [2]	30000		3750,0		120000	
c6a.32xlarge [2]	40000		5000,0		160000	
c6a.48xlarge [2]	40000		5000,0		240000	
c6a.metal [2]	40000		5000,0		240000	
c6g.medium [1]	315	4750	39,38	593,75	2500	20000
c6g.large [1]	630	4750	78,75	593,75	3600	20000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c6g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
c6g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
c6g.4xlarge [2]	4750		593,75		20000	
c6g.8xlarge [2]	9500		1187.5		40000	
c6g.12xlarge [2]	14250		1781,25		50000	
c6g.16xlarge [2]	19000		2375,0		80000	
c6g.metal [2]	19000		2375,0		80000	
c6gd.medium [1]	315	4750	39,38	593,75	2500	20000
c6gd.large [1]	630	4750	78,75	593,75	3600	20000
c6gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
c6gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
c6gd.4xlarge [2]	4750		593,75		20000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c6gd.8xlarge [2]	9500		1187.5		40000	
c6gd.12xlarge [2]	14250		1781,25		50000	
c6gd.16xlarge [2]	19000		2375,0		80000	
c6gd.metal [2]	19000		2375,0		80000	
c6gn.medium [1]	760	9500	95,00	1187,50	2500	40000
c6gn.large [1]	1235	9500	154,38	1187,50	5000	40000
c6gn.xlarge [1]	2375	9500	296,88	1187,50	10000	40000
c6gn.2xlarge [1]	4750	9500	593,75	1187,50	20000	40000
c6gn.4xlarge [2]	9500		1187.5		40000	
c6gn.8xlarge [2]	19000		2375,0		80000	
c6gn.12xlarge [2]	28500		3562,5		120000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c6gn.16xlarge [2]	38000		4750,0		160000	
c6i.large [1]	650	10000	81,25	1250,00	3600	40000
c6i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c6i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6i.8xlarge [2]	10000		1250,0		40000	
c6i.12xlarge [2]	15000		1875,0		60000	
c6i.16xlarge [2]	20000		2500,0		80000	
c6i.24xlarge [2]	30000		3750,0		120000	
c6i.32xlarge [2]	40000		5000,0		160000	
c6i.metal [2]	40000		5000,0		160000	
c6id.large [1]	650	10000	81,25	1250,00	3600	40000
c6id.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c6id.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6id.8xlarge [2]	10000		1250,0		40000	
c6id.12xlarge [2]	15000		1875,0		60000	
c6id.16xlarge [2]	20000		2500,0		80000	
c6id.24xlarge [2]	30000		3750,0		120000	
c6id.32xlarge [2]	40000		5000,0		160000	
c6id.metal [2]	40000		5000,0		160000	
c6in.large [1]	1562	25000	195,31	3125,00	6250	100000
c6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
c6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
c6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c6in.8xlarge [2]	25000		3125,0		100000	
c6in.12xlarge [2]	37500		4687,5		150000	
c6in.16xlarge [2]	50000		6250,0		200000	
c6in.24xlarge [2]	75000		9375,0		300000	
c6in.32xlarge [2]	100000		12500,0		400000	
c6in.metal [2]	100000		12500,0		400000	
c7a.medium [1]	325	10000	40,62	1250,00	2500	40000
c7a.large [1]	650	10000	81,25	1250,00	3600	40000
c7a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7a.8xlarge [2]	10000		1250,0		40000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c7a.12xlarge [2]	15000		1875,0		60000	
c7a.16xlarge [2]	20000		2500,0		80000	
c7a.24xlarge [2]	30000		3750,0		120000	
c7a.32xlarge [2]	40000		5000,0		160000	
c7a.48xlarge [2]	40000		5000,0		240000	
c7a.metal-48xl [2]	40000		5000,0		240000	
c7g.medium [1]	315	10000	39,38	1250,00	2500	40000
c7g.large [1]	630	10000	78,75	1250,00	3600	40000
c7g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7g.8xlarge [2]	10000		1250,0		40000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c7g.12xlarge [2]	15000		1875,0		60000	
c7g.16xlarge [2]	20000		2500,0		80000	
c7g.metal [2]	20000		2500,0		80000	
c7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
c7gd.large [1]	630	10000	78,75	1250,00	3600	40000
c7gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7gd.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7gd.8xlarge [2]	10000		1250,0		40000	
c7gd.12xlarge [2]	15000		1875,0		60000	
c7gd.16xlarge [2]	20000		2500,0		80000	
c7gd.metal [2]	20000		2500,0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c7gn.medium [1]	521	10000	65,12	1250,00	2083	40000
c7gn.large [1]	1042	10000	130,25	1250,00	4167	40000
c7gn.xlarge [1]	2083	10000	260,38	1250,00	8333	40000
c7gn.2xlarge [1]	4167	10000	520,88	1250,00	16667	40000
c7gn.4xlarge [1]	8333	10000	1041,62	1250,00	33333	40000
c7gn.8xlarge [1]	16667	20000	2083,38	2500,00	66667	80000
c7gn.12xlarge [1]	25000	30000	3125,00	3750,00	100000	120000
c7gn.16xlarge [1]	33333	40000	4166,62	5000,00	133333	160000
c7gn.metal [1]	33333	40000	4166,62	5000,00	133333	160000
c7i.large [1]	650	10000	81,25	1250,00	3600	40000
c7i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c7i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7i.8xlarge [2]	10000		1250,0		40000	
c7i.12xlarge [2]	15000		1875,0		60000	
c7i.16xlarge [2]	20000		2500,0		80000	
c7i.24xlarge [2]	30000		3750,0		120000	
c7i.48xlarge [2]	40000		5000,0		240000	
c7i.metal-24xl [2]	30000		3750,0		120000	
c7i.metal-48xl [2]	40000		5000,0		240000	
c7i-flex.large [1]	312	10000	39,06	1250,00	2500	40000
c7i-flex.xlarge [1]	625	10000	78,12	1250,00	3600	40000
c7i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c7i-flex.4xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7i-flex.8xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7i-flex.12xlarge 1	7500	15000	937,50	1875,00	30000	60000
c7i-flex.16xlarge 1	10000	20000	1250,00	2500,00	40000	80000
c8a.medio 1	325	10000	40,62	1250,00	2500	40000
c8a.grande 1	650	10000	81,25	1250,00	3600	40000
c8a.xlarge 1	1250	10000	156,25	1250,00	6000	40000
c8a.2xgrande 1	2500	10000	312,50	1250,00	12000	40000
c8a.4x grande 1	5000	10000	625,00	1250,00	20000	40000
c8a.8xgrande 2	10000		1250,0		40000	
c8a.12xgrande 2	15000		1875,0		60000	
c8a.16xgrande 2	20000		2500.0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c8a.24x grande 2	30000		3750,0		120000	
c8a.48x grande 2	60000		7500,0		240000	
c8a.metal lo-24xl 2	30000		3750,0		120000	
c8a.metal lo-48xl 2	60000		7500,0		240000	
c8g.medium [1]	315	10000	39,38	1250,00	2500	40000
c8g.large [1]	630	10000	78,75	1250,00	3600	40000
c8g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c8g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c8g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c8g.8xlarge [2]	10000		1250,0		40000	
c8g.12xlarge [2]	15000		1875,0		60000	
c8g.16xlarge [2]	20000		2500,0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c8g.24xlarge [2]	30000		3750,0		120000	
c8g.48xlarge [2]	40000		5000,0		240000	
c8g.metal-24xl [2]	30000		3750,0		120000	
c8g.metal-48xl [2]	40000		5000,0		240000	
c8 gb. Medio 1	1562	25000	195,31	3125,00	7500	120000
c8 gb. grande 1	3125	25000	390,62	3125,00	15000	120000
c8 gb.xlarge 1	6250	25000	781,25	3125,00	30000	120000
c 8 gb. 2 x grande 1	12500	25000	1562,50	3125,00	60000	120000
c 8 gb. 4x large 2	25000		3125.0		120000	
c 8 gb. 8x large 2	50000		6250,0		240000	
c 8 gb. 12 x large 2	75000		9375,0		360000	
c 8 gb. 16 x large 2	100000		12500,0		480000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c 8 gb. 24 x large 2	150000		18750,0		720000	
c 8 gb. 48 x large 2	300000		37500,0		1440000	
c8gb.metal-24xl 2	150000		18750,0		720000	
c8gb.metallo-48xl 2	300000		37500,0		1440000	
c8gd.medium [1]	315	10000	39,38	1250,00	2500	40000
c8gd.large [1]	630	10000	78,75	1250,00	3600	40000
c8gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c8 g. 2 x grande 1	2500	10000	312,50	1250,00	12000	40000
c8g. 4x grande 1	5000	10000	625,00	1250,00	20000	40000
c8 g. 8 x grande 2	10000		1250,0		40000	
c8 g. 12 x grande 2	15000		1875,0		60000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c8 g. 16 x grande 2	20000		2500.0		80000	
c8gd.24xlarge [2]	30000		3750,0		120000	
c8gd.48xlarge [2]	40000		5000,0		240000	
c8gd.metal-24xl [2]	30000		3750,0		120000	
c8gd.metal-48xl [2]	40000		5000,0		240000	
c8gn.medium [1]	760	10000	95,00	1250,00	2500	40000
c8gn.large [1]	1250	10000	156,25	1250,00	5000	40000
c8gn.xlarge [1]	2500	10000	312,50	1250,00	10000	40000
c 8 g n. 2 x grande 1	5000	10000	625,00	1250,00	20000	40000
c 8 g n. 4 x grande 2	10000		1250,0		40000	
c8gn.8x grande 2	20000		2500.0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c8gn.12x grande 2	30000		3750,0		120000	
c8 gn.16x grande 2	40000		5000,0		160000	
c8gn.24xlarge [2]	60000		7500,0		240000	
c8gn.48xlarge [2]	120000		15000,0		480000	
c8gn.metal-24xl [2]	60000		7500,0		240000	
c8gn.metal-48xl [2]	120000		15000,0		480000	
c8i.large [1]	650	10000	81,25	1250,00	3600	40000
c8i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
c8i.2x grande 1	2500	10000	312,50	1250,00	12000	40000
c8i.4x grande 1	5000	10000	625,00	1250,00	20000	40000
c8i.8x grande 2	10000		1250,0		40000	
c8i.12x grande 2	15000		1875,0		60000	
c8i.16x grande 2	20000		2500.0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c8i.24x grande 2	30000		3750,0		120000	
c8i.32x grande 2	40000		5000,0		160000	
c8i.48x grande 2	60000		7500,0		240000	
c8i.96xlarge [2]	80000		10000,0		480000	
c8i.metal lo-48xl 2	60000		7500,0		240000	
c8i.metal -96xl [2]	80000		10000,0		480000	
c8id.grande 1	650	10000	81,25	1250,00	3600	40000
c8id.xlarge 1	1250	10000	156,25	1250,00	6000	40000
c8id.2x grande 1	2500	10000	312,50	1250,00	12000	40000
c8id.4x grande 1	5000	10000	625,00	1250,00	20000	40000
c8id.8x grande 2	10000		1250,0		40000	
c8id.12x grande 2	15000		1875,0		60000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c8 id.16x grande 2	20000		2500.0		80000	
c8id.24x grande 2	30000		3750,0		120000	
c8id.32x grande 2	40000		5000,0		160000	
c8id.48x grande 2	60000		7500,0		240000	
c8 id.96 x grande 2	80000		10000,0		480000	
c8id.metallo-48xl 2	60000		7500,0		240000	
c8id.metallo-96xl 2	80000		10000,0		480000	
c8i-flex.large 1	315	10000	39,38	1250,00	2500	40000
c8i-flex.xlarge 1	630	10000	78,75	1250,00	3600	40000
c8i-flex.2xlarge 1	1250	10000	156,25	1250,00	6000	40000
c8i-flex.4xlarge 1	2500	10000	312,50	1250,00	12000	40000
c8i-flex.8xlarge 1	5000	10000	625,00	1250,00	20000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c8i-flex. 12xlarge 1	7500	15000	937,50	1875,00	30000	60000
c8i-flex. 16xlarge 1	10000	20000	1250,00	2500,00	40000	80000
8 pollici grande 1	650	10000	81,25	1250,00	3600	40000
c8in.xlarge 1	1250	10000	156,25	1250,00	6000	40000
c 8 pollici 2 x grande 1	2500	10000	312,50	1250,00	12000	40000
c8 pollici. 4 x grande 1	5000	10000	625,00	1250,00	20000	40000
c 8 pollici x grande 2	10000		1250,0		40000	
c8 pollici. 12 x grande 2	15000		1875,0		60000	
c 8 pollici 16 x grande 2	20000		250,0		80000	
c8 pollici 24 x grande 2	30000		3750,0		120000	
c 8 pollici 32 x grande 2	40000		5000,0		160000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c8 pollici 48 x grande 2	60000		7500,0		240000	
c 8 pollici 96 x grande 2	120000		15000,0		480000	
Metallo da 8 pollici, 48 x L 2	60000		7500,0		240000	
Metallo da 8 pollici, 96 x L 2	120000		15000,0		480000	
c8ine. Large 1	650	10000	81,25	1250,00	3600	40000
c8ine.xlarge 1	1250	10000	156,25	1250,00	6000	40000
c8 in. 2 x grande 1	2500	10000	312,50	1250,00	12000	40000
c8 in. 4 x grande 1	5000	10000	625,00	1250,00	20000	40000
c8 in. 8 x grande 2	10000		1250,0		40000	
c8 in. 12 x grande 2	15000		1875,0		60000	
c8ib. grande 1	1563	25000	195,38	3125,00	7500	120000
c8ib.xlarge 1	3125	25000	390,62	3125,00	15000	120000
c8ib.2x grande 1	6250	25000	781,25	3125,00	30000	120000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c8ib.4x grande 1	12500	25000	1562,50	3125,00	60000	120000
c8ib.8x grande 2	25000		3125.0		120000	
c8ib.12x grande 2	37500		4687,5		180000	
c8ib.16x grande 2	50000		6250,0		240000	
c8ib.24x grande 2	75000		9375,0		360000	
c8ib.32x grande 2	100000		12500,0		480000	
c8ib.48x grande 2	150000		18750,0		720000	
c8ib.96x grande 2	300000		37500,0		1440000	
c8ib.metallo-48xl 2	150000		18750,0		720000	
c8ib.metallo-96xl 2	300000		37500,0		1440000	
cm 9 g. Medio 1	380	12000	47,50	1500,00	2500	48000
9c. Grande 1	760	12000	95,00	1500,00	3600	48000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c9g.x grande 1	1500	12000	187,50	1500,00	6000	48000
cm 9 g. 2 x grande 1	3000	12000	375,00	1500,00	12000	48000
cm 9 g. 4 x grande 1	6000	12000	750,00	1500,00	24000	48000
cm 9 g. 8 x grande 2	12000		1500,0		48000	
cm 9 g. 12 x grande 2	18000		2250,0		72000	
cm 9 g. 16 x grande 2	24000		3000,0		96000	
cm 9 g. 24 x grande 2	36000		4500,0		144000	
cm 9 g. 48 x grande 2	72000		9000,0		288000	
c9g. Metallo-48xl 2	72000		9000,0		288000	
c9gr. Medio 1	380	12000	47,50	1500,00	2500	48000
c9gd. grande 1	760	12000	95,00	1500,00	3600	48000
c9gd.xlarge 1	1500	12000	187,50	1500,00	6000	48000
c9g. 2x grande 1	3000	12000	375,00	1500,00	12000	48000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	MB/sThroughput di I/O base (, 128 KiB)	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
c9g. 4x grande 1	6000	12000	750,00	1500,00	24000	48000
c9g. 8x grande 2	12000		1500,0		48000	
c9g. 12x grande 2	18000		2250,0		72000	
c9g. 16x grande 2	24000		3000,0		96000	
cm 9 g. 24 x grande 2	36000		4500,0		144000	
c9g. 48x grande 2	72000		9000,0		288000	
c9gd.metallo-48xl 2	72000		9000,0		288000	

[1] Questi tipi di istanze possono sostenere le prestazioni massime per 30 minuti almeno una volta ogni 24 ore, dopodiché tornano alle prestazioni di base.

[2] Queste istanze possono mantenere le prestazioni dichiarate a tempo indeterminato. Se il carico di lavoro richiede prestazioni massime sostenute per un periodo superiore a 30 minuti, utilizza una di queste istanze.

Memoria ottimizzata

> **Note**
>
> - I tipi di istanza R8a, R8g, R8gd, R8i, R8id, R9g, R9gd, X8g, X8aedz R8i-flex, X8i supportano ponderazioni configurabili della larghezza di banda. Con questi tipi di istanze,

puoi ottimizzare la larghezza di banda di un'istanza per le prestazioni di rete o per le prestazioni di Amazon EBS. La tabella seguente mostra le prestazioni di banda larga predefinite di Amazon EBS per questi tipi di istanze. Per ulteriori informazioni, consulta Configurazione della ponderazione della larghezza di banda dell'istanza EC2.

- Per ottenere le massime prestazioni IOPS con le istanze U7i BlockExpress , si consiglia di utilizzare i volumi io2.

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r4.large [2]	425		53,125		3000	
r4.xlarge [2]	850		106,25		6000	
r4.2xlarge [2]	1700		212,5		12000	
r4.4xlarge [2]	3500		437,5		18750	
r4.8xlarge [2]	7000		875,0		37500	
r4.16xlarge [2]	14000		1750,0		75000	
r5.large [1]	650	4750	81,25	593,75	3600	18750
r5.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5.4xlarge [2]	4750		593,75		18750	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r5.8xlarge [2]	6800		850,0		30000	
r5.12xlarge [2]	9500		1187.5		40000	
r5.16xlarge [2]	13600		1700,0		60000	
r5.24xlarge [2]	19000		2375,0		80000	
r5.metal [2]	19000		2375,0		80000	
r5a.large [1]	650	2880	81,25	360,00	3600	16000
r5a.xlarge [1]	1085	2880	135,62	360,00	6000	16000
r5a.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
r5a.4xlarge [2]	2880		360,0		16000	
r5a.8xlarge [2]	4750		593,75		20000	
r5a.12xlarge [2]	6780		847,5		30000	
r5a.16xlarge [2]	9500		1187.5		40000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r5a.24xlarge [2]	13570		1696,25		60000	
r5ad.large [1]	650	2880	81,25	360,00	3600	16000
r5ad.xlarge [1]	1085	2880	135,62	360,00	6000	16000
r5ad.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
r5ad.4xlarge [2]	2880		360,0		16000	
r5ad.8xlarge [2]	4750		593,75		20000	
r5ad.12xlarge [2]	6780		847,5		30000	
r5ad.16xlarge [2]	9500		1187.5		40000	
r5ad.24xlarge [2]	13570		1696,25		60000	
r5b.large [1]	1250	10000	156,25	1250,00	5417	43333
r5b.xlarge [1]	2500	10000	312,50	1250,00	10833	43333
r5b.2xlarge [1]	5000	10000	625,00	1250,00	21667	43333

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r5b.4xlarge [2]	10000		1250,0		43333	
r5b.8xlarge [2]	20000		2500,0		86667	
r5b.12xlarge [2]	30000		3750,0		130000	
r5b.16xlarge [2]	40000		5000,0		173333	
r5b.24xlarge [2]	60000		7500,0		260000	
r5b.metal [2]	60000		7500,0		260000	
r5d.large [1]	650	4750	81,25	593,75	3600	18750
r5d.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5d.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5d.4xlarge [2]	4750		593,75		18750	
r5d.8xlarge [2]	6800		850,0		30000	
r5d.12xlarge [2]	9500		1187.5		40000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r5d.16xlarge [2]	13600		1700,0		60000	
r5d.24xlarge [2]	19000		2375,0		80000	
r5d.metal [2]	19000		2375,0		80000	
r5dn.large [1]	650	4750	81,25	593,75	3600	18750
r5dn.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5dn.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5dn.4xlarge [2]	4750		593,75		18750	
r5dn.8xlarge [2]	6800		850,0		30000	
r5dn.12xlarge [2]	9500		1187.5		40000	
r5dn.16xlarge [2]	13600		1700,0		60000	
r5dn.24xlarge [2]	19000		2375,0		80000	
r5dn.metal [2]	19000		2375,0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r5n.large [1]	650	4750	81,25	593,75	3600	18750
r5n.xlarge [1]	1150	4750	143,75	593,75	6000	18750
r5n.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5n.4xlarge [2]	4750		593,75		18750	
r5n.8xlarge [2]	6800		850,0		30000	
r5n.12xlarge [2]	9500		1187.5		40000	
r5n.16xlarge [2]	13600		1700,0		60000	
r5n.24xlarge [2]	19000		2375,0		80000	
r5n.metal [2]	19000		2375,0		80000	
r6a.large [1]	650	10000	81,25	1250,00	3600	40000
r6a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r6a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r6a.8xlarge [2]	10000		1250,0		40000	
r6a.12xlarge [2]	15000		1875,0		60000	
r6a.16xlarge [2]	20000		2500,0		80000	
r6a.24xlarge [2]	30000		3750,0		120000	
r6a.32xlarge [2]	40000		5000,0		160000	
r6a.48xlarge [2]	40000		5000,0		240000	
r6a.metal [2]	40000		5000,0		240000	
r6g.medium [1]	315	4750	39,38	593,75	2500	20000
r6g.large [1]	630	4750	78,75	593,75	3600	20000
r6g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
r6g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
r6g.4xlarge [2]	4750		593,75		20000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r6g.8xlarge [2]	9500		1187.5		40000	
r6g.12xlarge [2]	14250		1781,25		50000	
r6g.16xlarge [2]	19000		2375,0		80000	
r6g.metal [2]	19000		2375,0		80000	
r6gd.medium [1]	315	4750	39,38	593,75	2500	20000
r6gd.large [1]	630	4750	78,75	593,75	3600	20000
r6gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
r6gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
r6gd.4xlarge [2]	4750		593,75		20000	
r6gd.8xlarge [2]	9500		1187.5		40000	
r6gd.12xlarge [2]	14250		1781,25		50000	
r6gd.16xlarge [2]	19000		2375,0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r6gd.metal [2]	19000		2375,0		80000	
r6i.large [1]	650	10000	81,25	1250,00	3600	40000
r6i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r6i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r6i.8xlarge [2]	10000		1250,0		40000	
r6i.12xlarge [2]	15000		1875,0		60000	
r6i.16xlarge [2]	20000		2500,0		80000	
r6i.24xlarge [2]	30000		3750,0		120000	
r6i.32xlarge [2]	40000		5000,0		160000	
r6i.metal [2]	40000		5000,0		160000	
r6id.large [1]	650	10000	81,25	1250,00	3600	40000
r6id.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r6id.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r6id.8xlarge [2]	10000		1250,0		40000	
r6id.12xlarge [2]	15000		1875,0		60000	
r6id.16xlarge [2]	20000		2500,0		80000	
r6id.24xlarge [2]	30000		3750,0		120000	
r6id.32xlarge [2]	40000		5000,0		160000	
r6id.metal [2]	40000		5000,0		160000	
r6idn.large [1]	1562	25000	195,31	3125,00	6250	100000
r6idn.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
r6idn.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
r6idn.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r6idn.8xlarge [2]	25000		3125,0		100000	
r6idn.12xlarge [2]	37500		4687,5		150000	
r6idn.16xlarge [2]	50000		6250,0		200000	
r6idn.24xlarge [2]	75000		9375,0		300000	
r6idn.32xlarge [2]	100000		12500,0		400000	
r6idn.metal [2]	100000		12500,0		400000	
r6in.large [1]	1562	25000	195,31	3125,00	6250	100000
r6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
r6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
r6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
r6in.8xlarge [2]	25000		3125,0		100000	
r6in.12xlarge [2]	37500		4687,5		150000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r6in.16xlarge [2]	50000		6250,0		200000	
r6in.24xlarge [2]	75000		9375,0		300000	
r6in.32xlarge [2]	100000		12500,0		400000	
r6in.metal [2]	100000		12500,0		400000	
r7a.medium [1]	325	10000	40,62	1250,00	2500	40000
r7a.large [1]	650	10000	81,25	1250,00	3600	40000
r7a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7a.8xlarge [2]	10000		1250,0		40000	
r7a.12xlarge [2]	15000		1875,0		60000	
r7a.16xlarge [2]	20000		2500,0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r7a.24xlarge [2]	30000		3750,0		120000	
r7a.32xlarge [2]	40000		5000,0		160000	
r7a.48xlarge [2]	40000		5000,0		240000	
r7a.metal-48xl [2]	40000		5000,0		240000	
r7g.medium [1]	315	10000	39,38	1250,00	2500	40000
r7g.large [1]	630	10000	78,75	1250,00	3600	40000
r7g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7g.8xlarge [2]	10000		1250,0		40000	
r7g.12xlarge [2]	15000		1875,0		60000	
r7g.16xlarge [2]	20000		2500,0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r7g.metal [2]	20000		2500,0		80000	
r7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
r7gd.large [1]	630	10000	78,75	1250,00	3600	40000
r7gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7gd.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7gd.8xlarge [2]	10000		1250,0		40000	
r7gd.12xlarge [2]	15000		1875,0		60000	
r7gd.16xlarge [2]	20000		2500,0		80000	
r7gd.metal [2]	20000		2500,0		80000	
r7i.large [1]	650	10000	81,25	1250,00	3600	40000
r7i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r7i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7i.8xlarge [2]	10000		1250,0		40000	
r7i.12xlarge [2]	15000		1875,0		60000	
r7i.16xlarge [2]	20000		2500,0		80000	
r7i.24xlarge [2]	30000		3750,0		120000	
r7i.48xlarge [2]	40000		5000,0		240000	
r7i.metal-24xl [2]	30000		3750,0		120000	
r7i.metal-48xl [2]	40000		5000,0		240000	
r7iz.large [1]	792	10000	99,00	1250,00	3600	40000
r7iz.xlarge [1]	1584	10000	198,00	1250,00	6667	40000
r7iz.2xlarge [1]	3168	10000	396,00	1250,00	13333	40000
r7iz.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r7iz.8xlarge [2]	10000		1250,0		40000	
r7iz.12xlarge [2]	19000		2375,0		76000	
r7iz.16xlarge [2]	20000		2500,0		80000	
r7iz.32xlarge [2]	40000		5000,0		160000	
r7iz.metal-16xl [2]	20000		2500,0		80000	
r7iz.metal-32xl [2]	40000		5000,0		160000	
r8a.medium [1]	325	10000	40,62	1250,00	2500	40000
r8a.large [1]	650	10000	81,25	1250,00	3600	40000
r8a.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r8a.2xgrande 1	2500	10000	312,50	1250,00	12000	40000
r8a.4xgrande 1	5000	10000	625,00	1250,00	20000	40000
r8a.8xgrande 2	10000		1250,0		40000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r8a.12x grande 2	15000		1875,0		60000	
r8a.16x grande 2	20000		2500.0		80000	
r8a.24x grande 2	30000		3750,0		120000	
r8a.48x grande 2	60000		7500,0		240000	
r8a.metal -24xl [2]	30000		3750,0		120000	
R8a. Metal-48xl 2	60000		7500,0		240000	
r8g.medium [1]	315	10000	39,38	1250,00	2500	40000
r8g.large [1]	630	10000	78,75	1250,00	3600	40000
r8g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r8g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r8g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r8g.8xlarge [2]	10000		1250,0		40000	
r8g.12xlarge [2]	15000		1875,0		60000	
r8g.16xlarge [2]	20000		2500,0		80000	
r8g.24xlarge [2]	30000		3750,0		120000	
r8g.48xlarge [2]	40000		5000,0		240000	
r8g.metal-24xl [2]	30000		3750,0		120000	
r8g.metal-48xl [2]	40000		5000,0		240000	
r8gb.medium [1]	1562	25000	195,31	3125,00	7500	120000
r8gb.large [1]	3125	25000	390,62	3125,00	15000	120000
r8gb.xlarge [1]	6250	25000	781,25	3125,00	30000	120000
r8gb.2xlarge [1]	12500	25000	1562,50	3125,00	60000	120000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r8gb.4xlarge [2]	25000		3125,0		120000	
r8gb.8xlarge [2]	50000		6250,0		240000	
r8gb.12xlarge [2]	75000		9375,0		360000	
r8gb.16xlarge [2]	100000		12500,0		480000	
r8gb.24xlarge [2]	150000		18750,0		720000	
r8 gb. 48 x large 2	300000		37500,0		1440000	
r8gb.metal-24xl [2]	150000		18750,0		720000	
r8 gb. Metal-48xl 2	300000		37500,0		1440000	
r8gd.medium [1]	315	10000	39,38	1250,00	2500	40000
r8gd.large [1]	630	10000	78,75	1250,00	3600	40000
r8gd.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r8 g. 2 x grande 1	2500	10000	312,50	1250,00	12000	40000
r8gd.4x grande 1	5000	10000	625,00	1250,00	20000	40000
r8 g. 8 x grande 2	10000		1250,0		40000	
r8gd.12x grande 2	15000		1875,0		60000	
r8gd.16x grande 2	20000		2500.0		80000	
r8gd.24xlarge [2]	30000		3750,0		120000	
r8gd.48xlarge [2]	40000		5000,0		240000	
r8gd.metal-24xl [2]	30000		3750,0		120000	
r8gd.metal-48xl [2]	40000		5000,0		240000	
r8gn.medium [1]	760	10000	95,00	1250,00	2500	40000
r8gn.large [1]	1250	10000	156,25	1250,00	5000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r8gn.xlarge [1]	2500	10000	312,50	1250,00	10000	40000
r8gn.2xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r8gn.4xlarge [2]	10000		1250,0		40000	
r8gn.8xlarge [2]	20000		2500,0		80000	
r8gn.12xlarge [2]	30000		3750,0		120000	
r8gn.16xlarge [2]	40000		5000,0		160000	
r8gn.24xlarge [2]	60000		7500,0		240000	
r8gn.48xlarge [2]	120000		15000,0		480000	
r8gn.metal-24xl [2]	60000		7500,0		240000	
r8gn.metal-48xl [2]	120000		15000,0		480000	
r8i.large [1]	650	10000	81,25	1250,00	3600	40000
r8i.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r8i.2x grande 1	2500	10000	312,50	1250,00	12000	40000
r8i.4x grande 1	5000	10000	625,00	1250,00	20000	40000
r8i.8x grande 2	10000		1250,0		40000	
r8i.12x grande 2	15000		1875,0		60000	
r8i.16x grande 2	20000		2500.0		80000	
r8i.24x grande 2	30000		3750,0		120000	
r8i.32x grande 2	40000		5000,0		160000	
r8i.48x grande 2	60000		7500,0		240000	
r8i.96xlarge [2]	80000		10000,0		480000	
r8i.metallo-48xl 2	60000		7500,0		240000	
r8i.metal-96xl [2]	80000		10000,0		480000	
r8id.grande 1	650	10000	81,25	1250.00	3600	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r8id.xlarge 1	1250	10000	156,25	1250,00	6000	40000
r8id.2x grande 1	2500	10000	312,50	1250,00	12000	40000
r8id.4xgrande 1	5000	10000	625,00	1250,00	20000	40000
r8id.8x grande 2	10000		1250.0		40000	
r8id.12x grande 2	15000		1875,0		60000	
r8id.16x grande 2	20000		2500.0		80000	
r8id.24xlarge 2	30000		3750,0		120000	
r8id.32x grande 2	40000		5000.0		160000	
r8id.48x grande 2	60000		7500,0		240000	
r8id.96x grande 2	80000		10000,0		480000	
r8id.metallo-48xl 2	60000		7500,0		240000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r8id.metallo-96xl 2	80000		10000,0		480000	
r8i-flex.large [1]	315	10000	39,38	1250,00	2500	40000
r8i-flex.xlarge [1]	630	10000	78,75	1250,00	3600	40000
r8i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6000	40000
r8i-flex.4xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r8i-flex.8xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r8i-flex.12xlarge [1]	7500	15000	937,50	1875,00	30000	60000
r8i-flex.16xlarge [1]	10000	20000	1250,00	2500,00	40000	80000
R 8 pollici grande 1	650	10000	81,25	1250,00	3600	40000
r8in.xlarge 1	1250	10000	156,25	1250,00	6000	40000
R 8 pollici. 2 x grande 1	2500	10000	312,50	1250,00	12000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r 8 pollici. 4x grande 1	5000	10000	625,00	1250,00	20000	40000
R 8 pollici x grande 2	10000		1250,0		40000	
R 8 pollici 12 x grande 2	15000		1875,0		60000	
R 8 pollici 16 x grande 2	20000		2500.0		80000	
R 8 pollici 24 x grande 2	30000		3750,0		120000	
R 8 pollici 32 x grande 2	40000		5000,0		160000	
R 8 pollici 48 x grande 2	60000		7500,0		240000	
R 8 pollici 96 x grande 2	120000		15000,0		480000	
R8in.Metal-48xl 2	60000		7500,0		240000	
R8in.Metal-96xl 2	120000		15000,0		480000	
r8idn.grande 1	650	10000	81,25	1250.00	3600	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r8idn.xlarge 1	1250	10000	156,25	1250,00	6000	40000
r8idn.2xgrande 1	2500	10000	312,50	1250,00	12000	40000
r8idn.4xgrande 1	5000	10000	625,00	1250,00	20000	40000
r8idn.8xgrande 2	10000		1250,0		40000	
r8idn.12xgrande 2	15000		1875,0		60000	
r8idn.16xgrande 2	20000		2500.0		80000	
r8idn.24xlarge 2	30000		3750,0		120000	
r8idn.32xgrande 2	40000		5000,0		160000	
r8idn.48xgrande 2	60000		7500,0		240000	
r8idn.96xgrande 2	120000		15000,0		480000	
r8idn.metallo-48xl 2	60000		7500,0		240000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r8idn.metallo-96xl 2	120000		15000,0		480000	
r8ib. grande 1	1563	25000	195,38	3125,00	7500	120000
r8ib.xlarge 1	3125	25000	390,62	3125,00	15000	120000
r8ib.2x grande 1	6250	25000	781,25	3125,00	30000	120000
r8ib.4x grande 1	12500	25000	1562,50	3125,00	60000	120000
r8ib.8x grande 2	25000		3125.0		120000	
r8ib.12x grande 2	37500		4687,5		180000	
r8ib.16x grande 2	50000		6250,0		240000	
r8ib.24x grande 2	75000		9375,0		360000	
r8ib.32x grande 2	100000		12500,0		480000	
r8ib.48x grande 2	150000		18750,0		720000	
r8ib.96x grande 2	300000		37500,0		1440000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
R8ib.metallo-48xl 2	150000		18750,0		720000	
r8ib.metallo-96xl 2	300000		37500,0		1440000	
r8idb.grande 1	1563	25000	195,38	3125,00	7500	120000
r8idb.xlarge 1	3125	25000	390,62	3125,00	15000	120000
r8idb.2xgrande 1	6250	25000	781,25	3125,00	30000	120000
r8idb.4xgrande 1	12500	25000	1562,50	3125,00	60000	120000
r8idb.8xlarge 2	25000		3125.0		120000	
r8idb.12xlarge 2	37500		4687,5		180000	
r8idb.16xlarge 2	50000		6250,0		240000	
r8idb.24xlarge 2	75000		9375,0		360000	
r8idb.32xlarge 2	100000		12500,0		480000	
r8idb.48xlarge 2	150000		18750,0		720000	
r8idb.96xlarge 2	300000		37500,0		1440000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r8idb.metallo-48xl 2	150000		18750,0		720000	
r8idb.metallo-96xl 2	300000		37500,0		1440000	
r9g. Medio 1	380	12000	47,50	1500,00	2500	48000
r9g. Grande 1	760	12000	95,00	1500,00	3600	48000
r9g.x grande 1	1500	12000	187,50	1500,00	6000	48000
r 9 g. 2 x grande 1	3000	12000	375,00	1500,00	12000	48000
r 9 g. 4 x grande 1	6000	12000	750,00	1500,00	24000	48000
r 9 g. 8 x grande 2	12000		1500,0		48000	
r 9 g. 12 x grande 2	18000		2250,0		72000	
r 9 g. 16 x grande 2	24000		3000,0		96000	
r 9 g. 24 x grande 2	36000		4500,0		144000	
r 9 g. 48 x grande 2	72000		9000,0		288000	
R9g. Metal-48xl 2	72000		9000,0		288000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
r9gd.medio 1	380	12000	47,50	1500,00	2500	48000
r9gd. grande 1	760	12000	95,00	1500,00	3600	48000
r9gd.xlarge 1	1500	12000	187,50	1500,00	6000	48000
r9gd.2x grande 1	3000	12000	375,00	1500,00	12000	48000
r9gd.4x grande 1	6000	12000	750,00	1500,00	24000	48000
r9gd.8x grande 2	12000		1500,0		48000	
r 9 g. 12 x grande 2	18000		2250,0		72000	
r9gd.16x grande 2	24000		3000,0		96000	
r9gd.24x grande 2	36000		4500,0		144000	
r9gd.48x grande 2	72000		9000,0		288000	
r9gd.metallo-48xl 2	72000		9000,0		288000	
u-3tb1.56xlarge [2]	19000		2375,0		80000	
u-6tb1.56xlarge [2]	38000		4750,0		160000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
u-6tb1.112xlarge [2]	38000		4750,0		160000	
u-6tb1.metal [2]	38000		4750,0		160000	
u-9tb1.112xlarge [2]	38000		4750,0		160000	
u-9tb1.metal [2]	38000		4750,0		160000	
u-12tb1.112xlarge [2]	38000		4750,0		160000	
u-12tb1.metal [2]	38000		4750,0		160000	
u-18tb1.112xlarge [2]	38000		4750,0		160000	
u-18tb1.metal [2]	38000		4750,0		160000	
u-24tb1.112xlarge [2]	38000		4750,0		160000	
u-24tb1.metal [2]	38000		4750,0		160000	
u7i-6tb.112xlarge [2]	100000		12500,0		560000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
u7i-8tb.112xlarge [2]	100000		12500,0		560000	
u7i-12tb.224xlarge [2]	100000		12500,0		560000	
u7in-16tb.224xlarge [2]	100000		12500,0		560000	
u7in-24tb.224xlarge [2]	100000		12500,0		560000	
u7in-32tb.224xlarge [2]	100000		12500,0		560000	
u7inh-32tb.480xlarge [2]	160000		20000,0		840000	
x1.16xlarge [2]	7000		875,0		40000	
x1.32xlarge [2]	14000		1750,0		80000	
x1e.xlarge [2]	500		62,5		3700	
x1e.2xlarge [2]	1000		125,0		7400	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
x1e.4xlarge [2]	1750		218,75		10000	
x1e.8xlarge [2]	3500		437,5		20000	
x1e.16xlarge [2]	7000		875,0		40000	
x1e.32xlarge [2]	14000		1750,0		80000	
x2gd.medium [1]	315	4750	39,38	593,75	2500	20000
x2gd.large [1]	630	4750	78,75	593,75	3600	20000
x2gd.xlarge [1]	1188	4750	148,50	593,75	6000	20000
x2gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
x2gd.4xlarge [2]	4750		593,75		20000	
x2gd.8xlarge [2]	9500		1187.5		40000	
x2gd.12xlarge [2]	14250		1781,25		60000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
x2gd.16xlarge [2]	19000		2375,0		80000	
x2gd.metal [2]	19000		2375,0		80000	
x2idn.16xlarge [2]	40000		5000,0		173333	
x2idn.24xlarge [2]	60000		7500,0		260000	
x2idn.32xlarge [2]	80000		10000,0		260000	
x2idn.metal [2]	80000		10000,0		260000	
x2iedn.xlarge [1]	2500	20000	312,50	2500,00	8125	65000
x2iedn.2xlarge [1]	5000	20000	625,00	2500,00	16250	65000
x2iedn.4xlarge [1]	10000	20000	1250,00	2500,00	32500	65000
x2iedn.8xlarge [2]	20000		2500,0		65000	
x2iedn.16xlarge [2]	40000		5000,0		130000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
x2iedn.24xlarge [2]	60000		7500,0		195000	
x2iedn.32xlarge [2]	80000		10000,0		260000	
x2iedn.metal [2]	80000		10000,0		260000	
x2iezn.2xlarge [2]	3170		396,25		13333	
x2iezn.4xlarge [2]	4750		593,75		20000	
x2iezn.6xlarge [2]	9500		1187.5		40000	
x2iezn.8xlarge [2]	12000		1500,0		55000	
x2iezn.12xlarge [2]	19000		2375,0		80000	
x2iezn.metal [2]	19000		2375,0		80000	
x8g.medium [1]	315	10000	39,38	1250,00	2500	40000
x8g.large [1]	630	10000	78,75	1250,00	3600	40000
x8g.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
x8g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
x8g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
x8g.8xlarge [2]	10000		1250,0		40000	
x8g.12xlarge [2]	15000		1875,0		60000	
x8g.16xlarge [2]	20000		2500,0		80000	
x8g.24xlarge [2]	30000		3750,0		120000	
x8g.48xlarge [2]	40000		5000,0		240000	
x8g.metal-24xl [2]	30000		3750,0		120000	
x8g.metal-48xl [2]	40000		5000,0		240000	
x8aedz.grande 1	1250	15000	156,25	1875,00	5000	60000
x8aedz.xlarge 1	2500	15000	312,50	1875,00	10000	60000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
x8aedz.3x grande 1	7500	15000	937,50	1875,00	30000	60000
x8aedz.6x grande 2	15000		1875,0		60000	
x8aedz.12x grande 2	30000		3750,0		120000	
x8aedz.24x grande 2	60000		7500,0		240000	
x8aedz.metallo-12xl 2	30000		3750,0		120000	
x8aedz.metallo-24xl 2	60000		7500,0		240000	
x8i. Grande 1	650	10000	81,25	1250,00	3600	40000
x8i.x grande 1	1250	10000	156,25	1250,00	6000	40000
x 8i.2 x grande 1	2500	10000	312,50	1250,00	12000	40000
x8i.4x grande 1	5000	10000	625,00	1250,00	20000	40000
x8i.8x grande 2	10000		1250,0		40000	
x8i.12x grande 2	15000		1875,0		60000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
x8i.16xgrande 2	20000		2500.0		80000	
x8i.24xgrande 2	30000		3750,0		120000	
x8i.32xgrande 2	40000		5000,0		160000	
x8i.48xgrande 2	60000		7500,0		240000	
x8i.64xgrande 2	70000		8750,0		320000	
x8i.96xgrande 2	80000		10000,0		480000	
x8i.metallo-48xl 2	60000		7500,0		240000	
x8i.metallo-96xl 2	80000		10000,0		480000	
z1d.large [1]	800	3170	100,00	396,25	3333	13333
z1d.xlarge [1]	1580	3170	197,50	396,25	6667	13333
z1d.2xlarge [2]	3170		396,25		13333	
z1d.3xlarge [2]	4750		593,75		20000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Throughput di base (, 128 KiB) MB/s I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
z1d.6xlarge [2]	9500		1187.5		40000	
z1d.12xlarge [2]	19000		2375,0		80000	
z1d.metal [2]	19000		2375,0		80000	

[1] Questi tipi di istanze possono sostenere le prestazioni massime per 30 minuti almeno una volta ogni 24 ore, dopodiché tornano alle prestazioni di base.

[2] Queste istanze possono mantenere le prestazioni dichiarate a tempo indeterminato. Se il carico di lavoro richiede prestazioni massime sostenute per un periodo superiore a 30 minuti, utilizza una di queste istanze.

Archiviazione ottimizzata

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
d2.xlarge [2]	750		93,75		6000	
d2.2xlarge [2]	1000		125.0		8000	
d2.4xlarge [2]	2000		250,0		16000	
d2.8xlarge [2]	4000		500,0		32000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
d3.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3.2xlarge [1]	1700	2800	212,50	350,00	10000	15000
d3.4xlarge [2]	2800		350,0		15000	
d3.8xlarge [2]	5000		625,0		30000	
d3en.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3en.2xlarge [1]	1700	2800	212,50	350,00	10000	15000
d3en.4xlarge [2]	2800		350,0		15000	
d3en.6xlarge [2]	4000		500,0		25000	
d3en.8xlarge [2]	5000		625,0		30000	
d3en.12xlarge [2]	7000		875,0		40000	
h1.2xlarge [2]	1750		218,75		12000	
h1.4xlarge [2]	3500		437,5		20000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
h1.8xlarge [2]	7000		875,0		40000	
h1.16xlarge [2]	14000		1750,0		80000	
i3.large [2]	425		53,125		3000	
i3.xlarge [2]	850		106,25		6000	
i3.2xlarge [2]	1700		212,5		12000	
i3.4xlarge [2]	3500		437,5		16000	
i3.8xlarge [2]	7000		875,0		32500	
i3.16xlarge [2]	14000		1750,0		65000	
i3.metal [2]	19000		2375,0		80000	
i3en.large [1]	576	4750	72,10	593,75	3000	20000
i3en.xlarge [1]	1153	4750	144,20	593,75	6000	20000
i3en.2xlarge [1]	2307	4750	288,39	593,75	12000	20000
i3en.3xlarge [1]	3800	4750	475,00	593,75	15000	20000
i3en.6xlarge [2]	4750		593,75		20000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
i3en.12xlarge [2]	9500		1187.5		40000	
i3en.24xlarge [2]	19000		2375,0		80000	
i3en.metal [2]	19000		2375,0		80000	
i4g.large [1]	625	10000	78,12	1250,00	2500	40000
i4g.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i4g.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i4g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
i4g.8xlarge [2]	10000		1250,0		40000	
i4g.16xlarge [2]	20000		2500,0		80000	
i4i.large [1]	625	10000	78,12	1250,00	2500	40000
i4i.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i4i.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i4i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
i4i.8xlarge [2]	10000		1250,0		40000	
i4i.12xlarge [2]	15000		1875,0		60000	
i4i.16xlarge [2]	20000		2500,0		80000	
i4i.24xlarge [2]	30000		3750,0		120000	
i4i.32xlarge [2]	40000		5000,0		160000	
i4i.metal [2]	40000		5000,0		160000	
i7i.large [1]	625	10000	78,12	1250,00	2500	40000
i7i.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i7i.2x grande 1	2500	10000	312,50	1250,00	10000	40000
i7i.4x grande 1	5000	10000	625,00	1250,00	20000	40000
i7i.8x grande 2	10000		1250,0		40000	
i7i.12xlarge 2	15000		1875,0		60000	
i7i.16x grande 2	20000		2500.0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
i7i.24x grande [2]	30000		3750,0		120000	
i7i.48xlarge [2]	60000		7500,0		240000	
i7i.metal-24xl [2]	30000		3750,0		120000	
i7i.metal-48xl [2]	60000		7500,0		240000	
i7ie.large [1]	625	10000	78,12	1250,00	2500	40000
i7ie.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i7ie.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i7ie.3xlarge [1]	3750	10000	468,75	1250,00	15000	40000
i7ie.6xlarge [1]	7500	10000	937,50	1250,00	30000	40000
i7ie.12xlarge [2]	15000		1875,0		60000	
i7ie.18xlarge [2]	22500		2812,5		90000	
i7ie.24xlarge [2]	30000		3750,0		120000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
i7ie.48xlarge [2]	60000		7500,0		240000	
i7ie.metal-24xl [2]	30000		3750,0		120000	
i7ie.metal-48xl [2]	60000		7500,0		240000	
i8g.large [1]	625	10000	78,12	1250,00	2500	40000
i8g.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i8g.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i8g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
i8g.8xlarge [2]	10000		1250,0		40000	
i8g.12xlarge [2]	15000		1875,0		60000	
i8g.16xlarge [2]	20000		2500,0		80000	
i8g.24xlarge [2]	30000		3750,0		120000	
i8 g. 48 x grande 2	60000		7500,0		240000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
i8g.metal-24xl [2]	30000		3750,0		120000	
i8 g. Metallo-48 XL 2	60000		7500,0		240000	
i8ge.large [1]	625	10000	78,12	1250,00	2500	40000
i8ge.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i8ge.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i8ge.3xlarge [1]	3750	10000	468,75	1250,00	15000	40000
i8ge.6xlarge [1]	7500	10000	937,50	1250,00	30000	40000
i8ge.12xlarge [2]	15000		1875,0		60000	
i8ge.18xlarge [2]	22500		2812,5		90000	
i8ge.24xlarge [2]	30000		3750,0		120000	
i8ge.48xlarge [2]	60000		7500,0		240000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
i8ge.metal-24xl [2]	30000		3750,0		120000	
i8ge.metal-48xl [2]	60000		7500,0		240000	
im4gn.large [1]	1250	10000	156,25	1250,00	5000	40000
im4gn.xlarge [1]	2500	10000	312,50	1250,00	10000	40000
im4gn.2xlarge [1]	5000	10000	625,00	1250,00	20000	40000
im4gn.4xlarge [2]	10000		1250,0		40000	
im4gn.8xlarge [2]	20000		2500,0		80000	
im4gn.16xlarge [2]	40000		5000,0		160000	
is4gen.medium [1]	625	10000	78,12	1250,00	2500	40000
is4gen.large [1]	1250	10000	156,25	1250,00	5000	40000
is4gen.xlarge [1]	2500	10000	312,50	1250,00	10000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
is4gen.2xlarge [1]	5000	10000	625,00	1250,00	20000	40000
is4gen.4xlarge [2]	10000		1250,0		40000	
is4gen.8xlarge [2]	20000		2500,0		80000	

[1] Questi tipi di istanze possono sostenere le prestazioni massime per 30 minuti almeno una volta ogni 24 ore, dopodiché tornano alle prestazioni di base.

[2] Queste istanze possono mantenere le prestazioni dichiarate a tempo indeterminato. Se il carico di lavoro richiede prestazioni massime sostenute per un periodo superiore a 30 minuti, utilizza una di queste istanze.

Elaborazione accelerata

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
dl1.24xlarge [2]	19000		2375,0		80000	
dl2q.24xlarge [2]	19000		2375,0		80000	
f2.6xlarge [2]	7500		937,5		30000	
f2.12xlarge [2]	15000		1875,0		60000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
f2.48xlarge [2]	60000		7500,0		240000	
g3.4xlarge [2]	3500		437,5		20000	
g3.8xlarge [2]	7000		875,0		40000	
g3.16xlarge [2]	14000		1750,0		80000	
g4ad.xlarge [1]	400	3170	50,00	396,25	1700	13333
g4ad.2xlarge [1]	800	3170	100,00	396,25	3400	13333
g4ad.4xlarge [1]	1580	3170	197,50	396,25	6700	13333
g4ad.8xlarge [2]	3170		396,25		13333	
g4ad.16xlarge [2]	6300		787,5		26667	
g4dn.xlarge [1]	950	3500	118,75	437,50	3000	20000
g4dn.2xlarge [1]	1150	3500	143,75	437,50	6000	20000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
g4dn.4xlarge [2]	4750		593,75		20000	
g4dn.8xlarge [2]	9500		1187.5		40000	
g4dn.12xlarge [2]	9500		1187.5		40000	
g4dn.16xlarge [2]	9500		1187.5		40000	
g4dn.metal [2]	19000		2375,0		80000	
g5.xlarge [1]	700	3500	87,50	437,50	3000	15000
g5.2xlarge [1]	850	3500	106,25	437,50	3500	15000
g5.4xlarge [2]	4750		593,75		20000	
g5.8xlarge [2]	16000		2000,0		65000	
g5.12xlarge [2]	16000		2000,0		65000	
g5.16xlarge [2]	16000		2000,0		65000	
g5.24xlarge [2]	19000		2375,0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
g5.48xlarge [2]	19000		2375,0		80000	
g5g.xlarge [1]	1188	4750	148,50	593,75	6000	20000
g5g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
g5g.4xlarge [2]	4750		593,75		20000	
g5g.8xlarge [2]	9500		1187.5		40000	
g5g.16xlarge [2]	19000		2375,0		80000	
g5g.metal [2]	19000		2375,0		80000	
g6.xlarge [1]	1000	5000	125,00	625,00	4000	20000
g6.2xlarge [1]	2000	5000	250,00	625,00	8000	20000
g6.4xlarge [2]	8000		1000,0		32000	
g6.8xlarge [2]	16000		2000,0		64000	
g6.12xlarge [2]	20000		2500,0		80000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
g6.16xlarge [2]	20000		2500,0		80000	
g6.24xlarge [2]	30000		3750,0		120000	
g6.48xlarge [2]	60000		7500,0		240000	
g6e.xlarge [1]	1000	5000	125,00	625,00	4000	20000
g6e.2xlarge [1]	2000	5000	250,00	625,00	8000	20000
g6e.4xlarge [2]	8000		1000,0		32000	
g6e.8xlarge [2]	16000		2000,0		64000	
g6e.12xlarge [2]	20000		2500,0		80000	
g6e.16xlarge [2]	20000		2500,0		80000	
g6e.24xlarge [2]	30000		3750,0		120000	
g6e.48xlarge [2]	60000		7500,0		240000	
g6f.large [1]	936	5000	117,00	625,00	3750	20000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
g6f.xlarge [1]	1000	5000	125,00	625,00	4000	20000
g6f.2xlarge [1]	2000	5000	250,00	625,00	8000	20000
g6f.4xlarge [2]	6000		750,0		24000	
gr6.4xlarge [2]	8000		1000,0		32000	
gr6.8xlarge [2]	16000		2000,0		64000	
gr6f.4xlarge [2]	8000		1000,0		32000	
g [7,2 x grande] [1]	4000	8000	500,00	1000,00	16000	32000
g [7.4 x grande] [2]	8000		1000,0		32000	
g [7,8 x grande] [2]	16000		2000,0		64000	
g 7.12 x grande 2	20000		2500.0		80000	
g [7,24 x grande] [2]	40000		5000,0		160000	
g [7,48 x grande] [2]	80000		10000,0		320000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
g7e.2x grande [1]	2000	5000	250,00	625,00	8000	20000
g7e.4x grande 2	8000		1000,0		32000	
g7e.8x grande 2	16000		2000,0		64000	
g7e.12x grande 2	25000		3125.0		100000	
g7e.24x grande 2	50000		6250,0		200000	
g7e.48x grande 2	100000		12500,0		400000	
inf1.xlarge [1]	1190	4750	148,75	593,75	4000	20000
inf1.2xlarge [1]	1190	4750	148,75	593,75	6000	20000
inf1.6xlarge [2]	4750		593,75		20000	
inf1.24xlarge [2]	19000		2375,0		80000	
inf2.xlarge [1]	1250	10000	156,25	1250,00	6000	40000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
inf2.8xlarge [2]	10000		1250,0		40000	
inf2.24xlarge [2]	30000		3750,0		120000	
inf2.48xlarge [2]	60000		7500,0		240000	
p3.2xlarge [2]	1750		218,75		10000	
p3.8xlarge [2]	7000		875,0		40000	
p3.16xlarge [2]	14000		1750,0		80000	
p3dn.24xlarge [2]	19000		2375,0		80000	
p4d.24xlarge [2]	19000		2375,0		80000	
p4de.24xlarge [2]	19000		2375,0		80000	
p5.4xlarge [2]	10000		1250,0		32500	
p5.48xlarge [2]	80000		10000,0		260000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
p5e.48xlarge [2]	80000		10000,0		260000	
p5en.48xlarge [2]	100000		12500,0		400000	
p6-b200.48xlarge [2]	100000		12500,0		400000	
p6-b300.48xgrande 2	100000		12500,0		400000	
p6e-gb200.36xlarge [2]	60000		7500,0		240000	
trn1.2xlarge [1]	5000	20000	625,00	2500,00	16250	65000
trn1.32xlarge [2]	80000		10000,0		260000	
trn1n.32xlarge [2]	80000		10000,0		260000	
trn 2,3 xgrande 2	5000		625,0		16250	
trn2.48xlarge [2]	80000		10000,0		260000	
trn2u.48xlarge [2]	80000		10000,0		260000	

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
vt1.3xlarge [1]	2375	4750	296,88	593,75	10000	20000
vt1.6xlarge [2]	4750		593,75		20000	
vt1.24xlarge [2]	19000		2375,0		80000	

[1] Questi tipi di istanze possono sostenere le prestazioni massime per 30 minuti almeno una volta ogni 24 ore, dopodiché tornano alle prestazioni di base.

[2] Queste istanze possono mantenere le prestazioni dichiarate a tempo indeterminato. Se il carico di lavoro richiede prestazioni massime sostenute per un periodo superiore a 30 minuti, utilizza una di queste istanze.

High-performance informatica

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
hpc6a.48xlarge [1]	87	2085	10,88	260,62	500	11000
hpc6id.32xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.12xlarge [1]	87	2085	10,88	260,62	500	11000

Dimensioni istanza	Larghezza di banda di base (Mbps)	Larghezza di banda massima (Mbps)	Produttività di base (MB/s, 128 KiB) I/O	Produttività massima (MB/s, 128 KiB) I/O	IOPS di base (16 KiB) I/O	IOPS massimo (16 KiB) I/O
hpc7a.24xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.48xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.96xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7g.4xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7g.8xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7g.16xlarge [1]	87	2085	10,88	260,62	500	11000
hpc8a.96xlarge 1	87	2085	10,88	260,62	500	11000

[1] Questi tipi di istanze possono sostenere le prestazioni massime per 30 minuti almeno una volta ogni 24 ore, dopodiché tornano alle prestazioni di base.

[2] Queste istanze possono mantenere le prestazioni dichiarate a tempo indeterminato. Se il carico di lavoro richiede prestazioni massime sostenute per un periodo superiore a 30 minuti, utilizza una di queste istanze.

Ottimizzazione EBS supportata

I seguenti tipi di istanza supportano l'ottimizzazione EBS, ma tale ottimizzazione non è abilitata per impostazione predefinita. Devi abilitare l'ottimizzazione EBS, a una tariffa oraria aggiuntiva, durante o dopo l'avvio per raggiungere il livello di prestazioni EBS descritto.

Dimensioni istanza	Larghezza di banda massima (Mbps)	Produttività massima (MB/s, 128 KiB) I/O	IOPS massimi (16 KiB) I/O
c1.xlarge	1000	125.0	8000
c3.xlarge	500	62,5	4000
c3.2xlarge	1000	125,0	8000
c3.4xlarge	2000	250,0	16000
i2.xlarge	500	62,5	4000
i2.2xlarge	1000	125,0	8000
i2.4xlarge	2000	250,0	16000
m1.large	500	62,5	4000
m1.xlarge	1000	125,0	8000
m2.2xlarge	500	62,5	4000
m2.4xlarge	1000	125,0	8000
m3.xlarge	500	62,5	4000
m3.2xlarge	1000	125,0	8000
r3.xlarge	500	62,5	4000
r3.2xlarge	1000	125,0	8000
r3.4xlarge	2000	250,0	16000

Note

Le istanze `i2.8xlarge`, `c3.8xlarge` e `r3.8xlarge` non dispongono di larghezza di banda EBS dedicata e pertanto non offrono la funzionalità di ottimizzazione EBS. In queste

istanze, il traffico di rete e il traffico Amazon EBS condividono la stessa interfaccia di rete da 10 gigabit.

Ottieni le massime prestazioni ottimizzate per Amazon EBS

Le prestazioni EBS di un'istanza sono limitate dai limiti di prestazioni del tipo di istanza o dalle prestazioni aggregate dei volumi collegati, a seconda di quale dei due valori sia inferiore. Per ottenere le massime prestazioni EBS, un'istanza deve disporre di volumi collegati che forniscano prestazioni combinate pari o superiori alle prestazioni massime dell'istanza. Ad esempio, per ottenere `80,000` IOPS per `r6i.16xlarge`, l'istanza deve disporre di almeno `5` volumi `gp2` forniti con `16,000` IOPS ciascuno (`5` volumi x `16,000` IOPS = `80,000` IOPS), oppure può disporre di `1` volumi `gp3` forniti con `80,000` IOPS. Consigliamo di scegliere un tipo di istanza ottimizzata per EBS in grado di fornire una quantità maggiore di throughput dedicato Amazon EBS rispetto alle esigenze dell'applicazione. In caso contrario, la connessione tra Amazon EBS e Amazon EC2 può trasformarsi un collo di bottiglia delle prestazioni.

Important

Quando si utilizzano ponderazioni di larghezza di banda configurabili, i limiti di larghezza di banda EBS per l'istanza potrebbero cambiare. Per le istanze con configurazione di ponderazione `VPC-1`, che aumenta la larghezza di banda della rete, potresti riscontrare una riduzione maggiore del previsto di IOPS per i volumi EBS per via del raggiungimento del limite di larghezza di banda EBS prima del limite di IOPS. Ciò è particolarmente evidente nelle taglie più grandi I/O . Testa sempre il tuo carico di lavoro specifico per assicurarti che soddisfi i requisiti di prestazioni con la ponderazione di larghezza di banda selezionata. Per ulteriori informazioni, consulta Configurazione della ponderazione della larghezza di banda dell'istanza EC2.

È possibile utilizzare i parametri `EBSIOBalance%` e `EBSByteBalance%` per determinare se le istanze sono dimensionate correttamente. Puoi visualizzare queste metriche nella CloudWatch console e impostare un allarme che viene attivato in base a una soglia specificata. Questi parametri sono espressi come percentuale. Le istanze con una percentuale costantemente bassa sono candidate per un aumento delle dimensioni. Le istanze la cui percentuale non scende mai al di sotto del 100% sono candidate per una riduzione delle dimensioni. Per ulteriori informazioni, consulta Monitora le tue istanze utilizzando CloudWatch.

Le istanze a memoria elevata sono progettate per l'esecuzione di database di grandi dimensioni in memoria, incluse le distribuzioni di produzione del database in memoria SAP HANA all'interno del cloud. Per massimizzare le prestazioni EBS, utilizza istanze a memoria elevata con un numero pari di volumi `io1` o `io2` con prestazioni di provisioning identiche. Ad esempio, per carichi di lavoro IOPS gravosi, utilizza quattro volumi `io1` o `io2` con capacità di IOPS allocata da 40.000 per ottenere il numero massimo di 160.000 istanze IOPS. Analogamente, per carichi di lavoro con throughput elevato, utilizza sei `io1` o più `io2` volumi con 48.000 IOPS predisposti per ottenere il throughput massimo di 4.750. MB/s Per ulteriori suggerimenti, consultare Configurazione dell'archiviazione per SAP HANA.

Considerazioni

- Le istanze G4dn, I3en, Inf1, M5a, M5ad, R5a, R5ad, T3, T3a e Z1d avviate dopo il 26 febbraio 2020 forniscono le prestazioni massime ottimizzate per EBS. Per ottenere le massime prestazioni da un'istanza avviata prima del 26 febbraio 2020, interromperla e avviarla.
- Le istanze C5, C5d, C5n, M5, M5d, M5n, M5dn, R5, R5d, R5n, R5dn e P3dn avviate dopo il 3 dicembre 2019 forniscono le prestazioni massime ottimizzate per EBS. Per ottenere le prestazioni massime da un'istanza avviata prima del 3 dicembre 2019, interromperla e avviarla.
- Le istanze `u-6tb1.metal`, `u-9tb1.metal` e `u-12tb1.metal` avviate dopo il 12 marzo 2020 forniscono le prestazioni massime ottimizzate per EBS. Le istanze di questi tipi avviate prima del 12 marzo 2020 potrebbero fornire prestazioni inferiori. Per ottenere le prestazioni massime da un'istanza avviata prima del 12 marzo 2020, contattare il team dell'account per aggiornare l'istanza senza costi aggiuntivi.

Trova EBS-optimized i tipi di istanze EC2

Puoi visualizzare i tipi di istanze che supportano l'ottimizzazione EBS in ciascuna regione.

Console

Per trovare i tipi di istanza EBS-optimized predefiniti

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instance Types (Tipi di istanza).
3. Aggiungi il filtro supporto di ottimizzazione EBS = default.
4. (Facoltativo) Scegli l'icona Preferenze e attiva le colonne pertinenti, ad esempio EBS Maximum IOPS e EBS Baseline IOPS.

5. (Facoltativo) Aggiungi filtri per approfondire l'ambito di specifici tipi di istanze di interesse.

AWS CLI

Per trovare i tipi di istanza predefiniti EBS-optimized

Utilizza il seguente comando: describe-instance-types.

```
aws ec2 describe-instance-types \
--filters Name=ebs-info.ebs-optimized-support,Values=default  \
--query 'InstanceTypes[].{InstanceType:InstanceType,
 "MaxBandwidth(Mb/s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,
 MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIops, "MaxThroughput(MB/
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--output=table
```

Per trovare tipi di istanza che supportano facoltativamente l'ottimizzazione di EBS

Utilizza il seguente comando: describe-instance-types.

```
aws ec2 describe-instance-types \
--filters Name=ebs-info.ebs-optimized-support,Values=supported \
--query 'InstanceTypes[].{InstanceType:InstanceType,
 "MaxBandwidth(Mb/s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,
 MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIops, "MaxThroughput(MB/
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--output=table
```

Di seguito è riportato un output di esempio per `eu-west-1`.

```
-------------------------------------------------------------------------
|                        DescribeInstanceTypes                          |
+--------------+----------------------+----------+-----------------------+
| InstanceType | MaxBandwidth(Mb/s)   | MaxIOPS  |  MaxThroughput(MB/s)  |
+--------------+----------------------+----------+-----------------------+
|  i2.2xlarge  |  1000                |  8000    |  125.0                |
|  m2.4xlarge  |  1000                |  8000    |  125.0                |
|  m2.2xlarge  |  500                 |  4000    |  62.5                 |
|  c1.xlarge   |  1000                |  8000    |  125.0                |
|  i2.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.xlarge   |  500                 |  4000    |  62.5                 |
|  m1.xlarge   |  1000                |  8000    |  125.0                |
```

```
|  r3.4xlarge  |  2000                |  16000   |  250.0                |
|  r3.2xlarge  |  1000                |  8000    |  125.0                |
|  c3.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.2xlarge  |  1000                |  8000    |  125.0                |
|  r3.xlarge   |  500                 |  4000    |  62.5                 |
|  i2.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.2xlarge  |  1000                |  8000    |  125.0                |
|  m1.large    |  500                 |  4000    |  62.5                 |
+--------------+----------------------+----------+-----------------------+
```

PowerShell

Per trovare i tipi di istanza EBS-optimized predefiniti

Utilizza il cmdlet Get-EC2InstanceType.

```
Get-EC2InstanceType `
    -Filter @{Name="ebs-info.ebs-optimized-support"; Values="default"} | `
    Select InstanceType, `
        @{Name="MaxBandwidth(Mb/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps)}}, `
        @{Name="MaxIOPS"; Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumIops)}}, `
        @{Name="MaxThroughput (MB/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps)}}
```

Per trovare tipi di istanza che supportano facoltativamente l'ottimizzazione di EBS

Utilizza il cmdlet Get-EC2InstanceType.

```
Get-EC2InstanceType `
    -Filter @{Name="ebs-info.ebs-optimized-support"; Values="supported"} | `
    Select InstanceType, `
        @{Name="MaxBandwidth(Mb/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps)}}, `
        @{Name="MaxIOPS"; Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumIops)}}, `
        @{Name="MaxThroughput (MB/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps)}}
```

Di seguito è riportato un output di esempio per `eu-west-1`.

```
InstanceType MaxBandwidth(Mb/s) MaxIOPS MaxThroughput (MB/s)
------------ ------------------ ------- --------------------
```

```
m2.4xlarge                1000    8000              125.000
i2.2xlarge                1000    8000              125.000
c1.xlarge                 1000    8000              125.000
m2.2xlarge                 500    4000               62.500
r3.2xlarge                1000    8000              125.000
m3.xlarge                  500    4000               62.500
r3.4xlarge                2000   16000              250.000
m1.xlarge                 1000    8000              125.000
i2.xlarge                  500    4000               62.500
c3.xlarge                  500    4000               62.500
c3.4xlarge                2000   16000              250.000
c3.2xlarge                1000    8000              125.000
i2.4xlarge                2000   16000              250.000
r3.xlarge                  500    4000               62.500
m3.2xlarge                1000    8000              125.000
m1.large                   500    4000               62.500
```

Abilita l'ottimizzazione di EBS per un'istanza Amazon EC2

Puoi abilitare manualmente l'ottimizzazione di EBS solo per i tipi di istanze di generazioni precedenti che supportano facoltativamente l'ottimizzazione di EBS. Se abiliti l'ottimizzazione EBS per questi tipi di istanze, è prevista una tariffa oraria aggiuntiva

Prerequisiti

- Verifica che il tipo di istanza richieda l'abilitazione dell'ottimizzazione di EBS. Per ulteriori informazioni, consulta Ottimizzazione EBS supportata.
- Per abilitare l'ottimizzazione EBS dopo il lancio, è necessario interrompere l'istanza.

> **Warning**
>
> Quando si arresta un'istanza, i dati sui volumi dell'archivio dell'istanza vengono persi. Per preservare questi dati, esegui il backup su uno storage persistente.

Console

Per abilitare l'ottimizzazione di Amazon EBS durante l'avvio

Nella procedura guidata di avvio dell'istanza, seleziona il tipo di istanza richiesto. Espandi la sezione Dettagli avanzati, quindi, EBS-optimized ad esempio, seleziona Abilita.

Se il tipo di istanza selezionato non supporta l'ottimizzazione Amazon EBS, il menu a discesa è disabilitato. Se il tipo di istanza è Amazon EBS-optimized per impostazione predefinita, Abilita è già selezionato.

Per abilitare l'ottimizzazione di Amazon EBS dopo l'avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza.
3. Arrestare l'istanza. Scegliere Actions (Operazioni), Instance State (Stato istanza), Stop instance (Arresta istanza).
4. Con l'istanza ancora selezionata, scegliere Actions (Operazioni), Instance settings (Impostazioni istanza), Change instance type (Cambia tipo di istanza).
5. Seleziona EBS-optimized e quindi scegli Applica.

   Se il tipo di istanza è Amazon EBS-optimized per impostazione predefinita o se non supporta l'ottimizzazione di Amazon EBS, la casella di controllo è disabilitata.
6. Riavvia l'istanza. Scegli Instance state (Stato istanza), Start instance (Avvia istanza).

AWS CLI

Per abilitare l'ottimizzazione di Amazon EBS durante l'avvio

Utilizza il comando run-instances con l'opzione `--ebs-optimized`.

Per abilitare l'ottimizzazione di Amazon EBS dopo l'avvio

1. Se l'istanza è in esecuzione, interrompila usando il comando stop-instances.

   ```
   aws ec2 stop-instances --instance-ids i-1234567890abcdef0
   ```
2. Abilita l'ottimizzazione di EBS utilizzando il comando modify-instance-attribute con l'opzione `--ebs-optimized`.

   ```
   aws ec2 modify-instance-attribute \
       --instance-id i-1234567890abcdef0 \
       --ebs-optimized
   ```

PowerShell

Per abilitare l'ottimizzazione di Amazon EBS durante l'avvio

Usa il New-EC2Instance cmdlet con l'opzione. `-EbsOptimized`

Per abilitare l'ottimizzazione di Amazon EBS dopo l'avvio

1. Se l'istanza è in esecuzione, interromperla utilizzando il Stop-EC2Instance cmdlet.

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0
```

2. Abilita l'ottimizzazione EBS utilizzando il Edit-EC2InstanceAttribute cmdlet con l'opzione. `-EbsOptimized`

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -EbsOptimized $true
```

Opzioni della CPU per le istanze Amazon EC2

Molte istanze Amazon EC2 supportano il multithreading simultaneo (SMT), che consente l'esecuzione simultanea di più thread su un singolo core della CPU. Ciascun thread è rappresentato come una CPU virtuale (vCPU) sull'istanza. Un'istanza ha un numero predefinito di core CPU, variabile in base al tipo di istanza. Ad esempio, un tipo di istanza `m5.xlarge` ha due core CPU e due thread per core per impostazione predefinita, per un totale— di quattro vCPU.

Nella maggior parte dei casi, è presente un tipo di istanza Amazon EC2 con una combinazione di memoria e numero di vCPU adatta ai tuoi carichi di lavoro. Tuttavia, puoi specificare le seguenti opzioni della CPU sia durante che dopo l'avvio dell'istanza per ottimizzare l'istanza per carichi di lavoro specifici o determinate esigenze aziendali:

- Numero di core CPU: è possibile personalizzare il numero di core CPU per l'istanza. Questo ti offre la possibilità di ottimizzare i costi di licenza del software con un'istanza dotata di una quantità sufficiente di RAM per carichi di lavoro a memoria elevata ma di un numero minore di core CPU.
- Thread per core: puoi disabilitare l'SMT specificando un singolo thread per core della CPU. Potresti scegliere questa opzione per determinati carichi di lavoro, come quelli high performance computing (HPC).

Considerazioni

- Non è possibile modificare il numero di thread per core per le istanze Mac in silicone T2, C7a, M7a, R7a e Apple Silicon e le istanze basate sul processore Graviton. AWS
- Il numero di istanze che puoi eseguire si basa sulle vCPU predefinite per i tipi di istanza utilizzati. Il modo in cui calcoliamo le vCPU utilizzate da un'istanza non è influenzato dalla modifica delle opzioni della CPU.

Prezzi

Questa operazione non comporta costi supplementari. Per le istanze EC2 avviate da AMI Windows e SQL Server incluse nella licenza, puoi personalizzare le opzioni della CPU per sfruttare la funzionalità Ottimizzazione CPU di EC2 per pagare i costi di licenza in base al numero di vCPU configurate per l'istanza. Per altre istanze EC2, vengono addebitati gli stessi costi delle istanze avviate con le opzioni della CPU predefinite.

Indice

- Regole per specificare le opzioni della CPU per un'istanza Amazon EC2
- Opzioni della CPU supportate per i tipi di istanza Amazon EC2
- Specifica delle opzioni della CPU per un'istanza Amazon EC2
- Visualizzazione di thread e core della CPU per un'istanza Amazon EC2
- Ottimizza le CPU per le istanze License-Included

Regole per specificare le opzioni della CPU per un'istanza Amazon EC2

Per specificare le opzioni CPU per l'istanza, tieni conto delle seguenti regole:

- Non è possibile specificare le opzioni della CPU per le istanze bare metal.
- Puoi specificare le opzioni della CPU sia durante che dopo l'avvio dell'istanza.
- Per configurare le opzioni della CPU devi specificare sia il numero di core della CPU sia i thread per core. Per esempi di richieste, vedi Specifica delle opzioni della CPU per un'istanza Amazon EC2.
- Il numero di vCPU per l'istanza corrisponde al numero di core CPU moltiplicato per thread per core. Per specificare un numero di vCPU personalizzato, è necessario specificare un numero di core CPU valido e i thread per core per il tipo di istanza. Non puoi superare il numero di vCPU

predefinito per l'istanza. Per ulteriori informazioni, consulta Opzioni della CPU supportate per i tipi di istanza Amazon EC2.

- Per disabilitare il multithreading simultaneo (SMT), noto anche come hyper-threading, specifica un thread per core.
- Nella console, quando modifichi il tipo di istanza di un'istanza esistente, Amazon EC2 applica le impostazioni dell'opzione della CPU dall'istanza esistente a quella nuova, se possibile. Se il nuovo tipo di istanza non supporta tali impostazioni, le opzioni della CPU vengono ripristinate in Utilizza le opzioni della CPU predefinite. Questa opzione utilizza il numero predefinito di vCPU per il nuovo tipo di istanza.

  Per aggiornare le impostazioni per la nuova istanza, seleziona Specifica le opzioni della CPU in Dettagli avanzati nella finestra Modifica il tipo di istanza.
- Le opzioni CPU specificate restano invariate dopo l'arresto, l'avvio o il riavvio di un'istanza.
- Se utilizzi istanze riservate, è possibile che non vengano applicati sconti quando configuri Ottimizzazione CPU per istanze avviate da AMI Windows incluse nella licenza nello stesso account di pagamento. Ti consigliamo di utilizzare i piani di risparmio per ridurre i costi di licenza e offrire risparmi comparabili sui costi di elaborazione. CPU-based
- Per risparmiare sui costi di licenza per le istanze avviate da Windows e dalle AMI di SQL Server incluse nella licenza, devi configurare almeno quattro vCPU. Se configuri meno di quattro vCPU, viene applicata la fatturazione predefinita.
- L'ottimizzazione delle CPU per License-Included le istanze non è supportata sui tipi di istanze T3.
- L'ottimizzazione delle CPU per le istanze non è supportata License-Included nelle istanze dedicate.

Opzioni della CPU supportate per i tipi di istanza Amazon EC2

Nelle seguenti tabelle vengono descritti i tipi di istanze che supportano la specifica di opzioni CPU.

Indice

- Istanze per uso generale
- Istanze a calcolo ottimizzato
- Istanze con memoria ottimizzata
- Istanze con storage ottimizzato
- Istanze di calcolo accelerate
- High-performance istanze di calcolo

Istanze per uso generale

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m2.xlarge	2	2	1	1, 2	1
m2.2xlarge	4	4	1	1, 2, 3, 4	1
m2.4xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m3.large	2	1	2	1	1, 2
m3.xlarge	4	2	2	1, 2	1, 2
m3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.large	2	1	2	1	1, 2
m4.xlarge	4	2	2	1, 2	1, 2
m4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m5.large	2	1	2	1	1, 2
m5.xlarge	4	2	2	2	1, 2
m5.2xlarge	8	4	2	2, 4	1, 2
m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5a.large	2	1	2	1	1, 2
m5a.xlarge	4	2	2	2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m5a.2xlarge	8	4	2	2, 4	1, 2
m5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5ad.large	2	1	2	1	1, 2
m5ad.xlarge	4	2	2	2	1, 2
m5ad.2xlarge	8	4	2	2, 4	1, 2
m5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5d.large	2	1	2	1	1, 2
m5d.xlarge	4	2	2	2	1, 2
m5d.2xlarge	8	4	2	2, 4	1, 2
m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5dn.large	2	1	2	1	1, 2
m5dn.xlarge	4	2	2	1, 2	1, 2
m5dn.2xlarge	8	4	2	2, 4	1, 2
m5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5n.large	2	1	2	1	1, 2
m5n.xlarge	4	2	2	1, 2	1, 2
m5n.2xlarge	8	4	2	2, 4	1, 2
m5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5zn.large	2	1	2	1	1, 2
m5zn.xlarge	4	2	2	1, 2	1, 2
m5zn.2xlarge	8	4	2	2, 4	1, 2
m5zn.3xlarge	12	6	2	2, 4, 6	1, 2
m5zn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
m5zn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6a.large	2	1	2	1	1, 2
m6a.xlarge	4	2	2	1, 2	1, 2
m6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
m6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
m6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
m6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
m6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
m6g.large	2	2	1	1, 2	1
m6g.xlarge	4	4	1	1, 2, 3, 4	1
m6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6gd.large	2	2	1	1, 2	1
m6gd.xlarge	4	4	1	1, 2, 3, 4	1
m6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6i.large	2	1	2	1	1, 2
m6i.xlarge	4	2	2	1, 2	1, 2
m6i.2xlarge	8	4	2	2, 4	1, 2
m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6id.large	2	1	2	1	1, 2
m6id.xlarge	4	2	2	1, 2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6id.2xlarge	8	4	2	2, 4	1, 2
m6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6idn.large	2	1	2	1	1, 2
m6idn.xlarge	4	2	2	1, 2	1, 2
m6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6in.large	2	1	2	1	1, 2
m6in.xlarge	4	2	2	1, 2	1, 2
m6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m7a.large	2	2	1	1, 2	1
m7a.xlarge	4	4	1	1, 2, 3, 4	1
m7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
m7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
m7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m7g.large	2	2	1	1, 2	1
m7g.xlarge	4	4	1	1, 2, 3, 4	1
m7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7gd.large	2	2	1	1, 2	1
m7gd.xlarge	4	4	1	1, 2, 3, 4	1
m7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7i.large	2	1	2	1	1, 2
m7i.xlarge	4	2	2	1, 2	1, 2
m7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
m7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m7i-flex.large	2	1	2	1	1, 2
m7i-flex.xlarge	4	2	2	1, 2	1, 2
m7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8a.medium	1	1	1	1	1
m8a.large	2	2	1	1, 2	1
m8a.xlarge	4	4	1	1, 2, 3, 4	1
m8a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m8a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m8a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m8a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
m8a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m8azn.medium	1	1	1	1	1
m8azn.large	2	2	1	1, 2	1
m8azn.xlarge	4	4	1	1, 2, 3, 4	1
m8azn.3xlarge	12	12	1	1, 2, 4, 6, 8, 10, 12	1
m8azn.6xlarge	24	24	1	1, 2, 3, 4, 8, 12, 16, 20, 24	1
m8azn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48	1
m8azn.24xlarge	96	96	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96	1
m8g.large	2	2	1	1, 2	1
m8g.xlarge	4	4	1	1, 2, 3, 4	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8gb.large	2	2	1	1, 2	1
m8gb.xlarge	4	4	1	1, 2, 3, 4	1
m8gb.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8gb.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8gb.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8gb.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8gb.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8gb.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8gb.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8gd.large	2	2	1	1, 2	1
m8gd.xlarge	4	4	1	1, 2, 3, 4	1
m8gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8gn.large	2	2	1	1, 2	1
m8gn.xlarge	4	4	1	1, 2, 3, 4	1
m8gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8gn.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8gn.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8i.large	2	1	2	1	1, 2
m8i.xlarge	4	2	2	1, 2	1, 2
m8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m8i.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
m8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
m8id.large	2	1	2	1	1, 2
m8id.xlarge	4	2	2	1, 2	1, 2
m8id.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8id.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8id.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m8id.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m8id.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m8id.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8id.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m8id.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8id.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
m8i-flex.large	2	1	2	1	1, 2
m8i-flex.xlarge	4	2	2	1, 2	1, 2
m8i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m8i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m8i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m8in.large	2	1	2	1	1, 2
m8in.xlarge	4	2	2	1, 2	1, 2
m8in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m8in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m8in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m8in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m8in.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8in.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
m8idn.large	2	1	2	1	1, 2
m8idn.xlarge	4	2	2	1, 2	1, 2
m8idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m8idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m8idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m8idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m8idn.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8idn.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
m8ine.large	2	1	2	1	1, 2
m8ine.xlarge	4	2	2	1, 2	1, 2
m8ine.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m8ine.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8ine.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8ine.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m8ib.large	2	1	2	1	1, 2
m8ib.xlarge	4	2	2	1, 2	1, 2
m8ib.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m8ib.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8ib.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m8ib.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8ib.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m8ib.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m8ib.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8ib.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
m8ib.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
m8idb.large	2	1	2	1	1, 2
m8idb.xlarge	4	2	2	1, 2	1, 2
m8idb.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8idb.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8idb.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m8idb.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m8idb.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m8idb.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8idb.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m8idb.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m8idb.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
m9g.large	2	2	1	1, 2	1
m9g.xlarge	4	4	1	1, 2, 3, 4	1
m9g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m9g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m9g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m9g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m9g.16xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m9g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m9g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m9gd.large	2	2	1	1, 2	1
m9gd.xlarge	4	4	1	1, 2, 3, 4	1
m9gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m9gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m9gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m9gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1
m9gd.16xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m9gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
m9gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
t3.nano	2	1	2	1	1, 2
t3.micro	2	1	2	1	1, 2
t3.small	2	1	2	1	1, 2
t3.medium	2	1	2	1	1, 2
t3.large	2	1	2	1	1, 2
t3.xlarge	4	2	2	2	1, 2
t3.2xlarge	8	4	2	2, 4	1, 2
t3a.nano	2	1	2	1	1, 2
t3a.micro	2	1	2	1	1, 2
t3a.small	2	1	2	1	1, 2
t3a.medium	2	1	2	1	1, 2
t3a.large	2	1	2	1	1, 2
t3a.xlarge	4	2	2	2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
t3a.2xlarge	8	4	2	2, 4	1, 2
t4g.nano	2	2	1	1, 2	1
t4g.micro	2	2	1	1, 2	1
t4g.small	2	2	1	1, 2	1
t4g.medium	2	2	1	1, 2	1
t4g.large	2	2	1	1, 2	1
t4g.xlarge	4	4	1	1, 2, 3, 4	1
t4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Istanze a calcolo ottimizzato

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c3.large	2	1	2	1	1, 2
c3.xlarge	4	2	2	1, 2	1, 2
c3.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c4.large	2	1	2	1	1, 2
c4.xlarge	4	2	2	1, 2	1, 2
c4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c4.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.large	2	1	2	1	1, 2
c5.xlarge	4	2	2	2	1, 2
c5.2xlarge	8	4	2	2, 4	1, 2
c5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c5.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5a.large	2	1	2	1	1, 2
c5a.xlarge	4	2	2	1, 2	1, 2
c5a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5a.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5a.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5a.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5a.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c5a.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5ad.large	2	1	2	1	1, 2
c5ad.xlarge	4	2	2	1, 2	1, 2
c5ad.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5ad.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5ad.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5ad.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5ad.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5ad.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5d.large	2	1	2	1	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c5d.xlarge	4	2	2	2	1, 2
c5d.2xlarge	8	4	2	2, 4	1, 2
c5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5d.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5d.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5n.large	2	1	2	1	1, 2
c5n.xlarge	4	2	2	2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c5n.2xlarge	8	4	2	2, 4	1, 2
c5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5n.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5n.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c6a.large	2	1	2	1	1, 2
c6a.xlarge	4	2	2	1, 2	1, 2
c6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
c6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
c6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
c6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
c6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
c6g.large	2	2	1	1, 2	1
c6g.xlarge	4	4	1	1, 2, 3, 4	1
c6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gd.large	2	2	1	1, 2	1
c6gd.xlarge	4	4	1	1, 2, 3, 4	1
c6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gn.medium	1	1	1	1	1
c6gn.large	2	2	1	1, 2	1
c6gn.xlarge	4	4	1	1, 2, 3, 4	1
c6gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6i.large	2	1	2	1	1, 2
c6i.xlarge	4	2	2	1, 2	1, 2
c6i.2xlarge	8	4	2	2, 4	1, 2
c6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6id.large	2	1	2	1	1, 2
c6id.xlarge	4	2	2	1, 2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6id.2xlarge	8	4	2	2, 4	1, 2
c6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6in.large	2	1	2	1	1, 2
c6in.xlarge	4	2	2	1, 2	1, 2
c6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c7a.large	2	2	1	1, 2	1
c7a.xlarge	4	4	1	1, 2, 3, 4	1
c7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
c7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
c7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c7g.large	2	2	1	1, 2	1
c7g.xlarge	4	4	1	1, 2, 3, 4	1
c7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gd.large	2	2	1	1, 2	1
c7gd.xlarge	4	4	1	1, 2, 3, 4	1
c7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gn.large	2	2	1	1, 2	1
c7gn.xlarge	4	4	1	1, 2, 3, 4	1
c7gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7i.large	2	1	2	1	1, 2
c7i.xlarge	4	2	2	1, 2	1, 2
c7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
c7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c7i-flex.large	2	1	2	1	1, 2
c7i-flex.xlarge	4	2	2	1, 2	1, 2
c7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8a.medium	1	1	1	1	1
c8a.large	2	2	1	1, 2	1
c8a.xlarge	4	4	1	1, 2, 3, 4	1
c8a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c8a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c8a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c8a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
c8a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c8g.large	2	2	1	1, 2	1
c8g.xlarge	4	4	1	1, 2, 3, 4	1
c8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8gb.large	2	2	1	1, 2	1
c8gb.xlarge	4	4	1	1, 2, 3, 4	1
c8gb.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8gb.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8gb.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8gb.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8gb.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8gb.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8gb.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8gd.large	2	2	1	1, 2	1
c8gd.xlarge	4	4	1	1, 2, 3, 4	1
c8gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8gn.large	2	2	1	1, 2	1
c8gn.xlarge	4	4	1	1, 2, 3, 4	1
c8gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8gn.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8gn.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8i.large	2	1	2	1	1, 2
c8i.xlarge	4	2	2	1, 2	1, 2
c8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c8i.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
c8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
c8id.large	2	1	2	1	1, 2
c8id.xlarge	4	2	2	1, 2	1, 2
c8id.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8id.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8id.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c8id.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c8id.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c8id.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8id.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c8id.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8id.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
c8i-flex.large	2	1	2	1	1, 2
c8i-flex.xlarge	4	2	2	1, 2	1, 2
c8i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c8i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c8i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c8in.large	2	1	2	1	1, 2
c8in.xlarge	4	2	2	1, 2	1, 2
c8in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c8in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c8in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c8in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c8in.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8in.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
c8ine.large	2	1	2	1	1, 2
c8ine.xlarge	4	2	2	1, 2	1, 2
c8ine.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c8ine.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8ine.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8ine.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c8ib.large	2	1	2	1	1, 2
c8ib.xlarge	4	2	2	1, 2	1, 2
c8ib.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c8ib.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8ib.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c8ib.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8ib.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c8ib.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c8ib.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c8ib.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
c8ib.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
c9g.large	2	2	1	1, 2	1
c9g.xlarge	4	4	1	1, 2, 3, 4	1
c9g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c9g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c9g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c9g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c9g.16xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c9g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c9g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c9gd.large	2	2	1	1, 2	1
c9gd.xlarge	4	4	1	1, 2, 3, 4	1
c9gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c9gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c9gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c9gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1
c9gd.16xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c9gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
c9gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	

Istanze con memoria ottimizzata

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r3.large	2	1	2	1	1, 2
r3.xlarge	4	2	2	1, 2	1, 2
r3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r4.large	2	1	2	1	1, 2
r4.xlarge	4	2	2	1, 2	1, 2
r4.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r4.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.large	2	1	2	1	1, 2
r5.xlarge	4	2	2	2	1, 2
r5.2xlarge	8	4	2	2, 4	1, 2
r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5a.large	2	1	2	1	1, 2
r5a.xlarge	4	2	2	2	1, 2
r5a.2xlarge	8	4	2	2, 4	1, 2
r5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5ad.large	2	1	2	1	1, 2
r5ad.xlarge	4	2	2	2	1, 2
r5ad.2xlarge	8	4	2	2, 4	1, 2
r5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5b.large	2	1	2	1	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r5b.xlarge	4	2	2	1, 2	1, 2
r5b.2xlarge	8	4	2	2, 4	1, 2
r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5b.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5b.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5d.large	2	1	2	1	1, 2
r5d.xlarge	4	2	2	2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r5d.2xlarge	8	4	2	2, 4	1, 2
r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5dn.large	2	1	2	1	1, 2
r5dn.xlarge	4	2	2	1, 2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r5dn.2xlarge	8	4	2	2, 4	1, 2
r5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5n.large	2	1	2	1	1, 2
r5n.xlarge	4	2	2	1, 2	1, 2
r5n.2xlarge	8	4	2	2, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6a.large	2	1	2	1	1, 2
r6a.xlarge	4	2	2	1, 2	1, 2
r6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
r6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
r6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
r6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
r6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
r6g.large	2	2	1	1, 2	1
r6g.xlarge	4	4	1	1, 2, 3, 4	1
r6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6gd.large	2	2	1	1, 2	1
r6gd.xlarge	4	4	1	1, 2, 3, 4	1
r6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6i.large	2	1	2	1	1, 2
r6i.xlarge	4	2	2	1, 2	1, 2
r6i.2xlarge	8	4	2	2, 4	1, 2
r6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6id.large	2	1	2	1	1, 2
r6id.xlarge	4	2	2	1, 2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6id.2xlarge	8	4	2	2, 4	1, 2
r6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6idn.large	2	1	2	1	1, 2
r6idn.xlarge	4	2	2	1, 2	1, 2
r6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6in.large	2	1	2	1	1, 2
r6in.xlarge	4	2	2	1, 2	1, 2
r6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r7a.large	2	2	1	1, 2	1
r7a.xlarge	4	4	1	1, 2, 3, 4	1
r7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
r7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
r7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
r7g.large	2	2	1	1, 2	1
r7g.xlarge	4	4	1	1, 2, 3, 4	1
r7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7gd.large	2	2	1	1, 2	1
r7gd.xlarge	4	4	1	1, 2, 3, 4	1
r7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7i.large	2	1	2	1	1, 2
r7i.xlarge	4	2	2	1, 2	1, 2
r7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
r7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7iz.large	2	1	2	1	1, 2
r7iz.xlarge	4	2	2	1, 2	1, 2
r7iz.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7iz.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r7iz.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7iz.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7iz.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r7iz.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8a.medium	1	1	1	1	1
r8a.large	2	2	1	1, 2	1
r8a.xlarge	4	4	1	1, 2, 3, 4	1
r8a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r8a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r8a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
r8a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r8a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
r8g.large	2	2	1	1, 2	1
r8g.xlarge	4	4	1	1, 2, 3, 4	1
r8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8gb.large	2	2	1	1, 2	1
r8gb.xlarge	4	4	1	1, 2, 3, 4	1
r8gb.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8gb.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8gb.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8gb.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8gb.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8gb.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8gb.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8gd.large	2	2	1	1, 2	1
r8gd.xlarge	4	4	1	1, 2, 3, 4	1
r8gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8gn.large	2	2	1	1, 2	1
r8gn.xlarge	4	4	1	1, 2, 3, 4	1
r8gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8gn.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8gn.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8i.large	2	1	2	1	1, 2
r8i.xlarge	4	2	2	1, 2	1, 2
r8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r8i.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
r8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
r8id.large	2	1	2	1	1, 2
r8id.xlarge	4	2	2	1, 2	1, 2
r8id.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8id.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8id.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r8id.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r8id.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r8id.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8id.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8id.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8id.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
r8i-flex.large	2	1	2	1	1, 2
r8i-flex.xlarge	4	2	2	1, 2	1, 2
r8i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r8i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r8i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r8in.large	2	1	2	1	1, 2
r8in.xlarge	4	2	2	1, 2	1, 2
r8in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r8in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r8in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r8in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8in.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8in.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
r8idn.large	2	1	2	1	1, 2
r8idn.xlarge	4	2	2	1, 2	1, 2
r8idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r8idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r8idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r8idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8idn.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8idn.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
r8ib.large	2	1	2	1	1, 2
r8ib.xlarge	4	2	2	1, 2	1, 2
r8ib.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r8ib.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8ib.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8ib.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r8ib.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r8ib.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8ib.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8ib.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8ib.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
r8idb.large	2	1	2	1	1, 2
r8idb.xlarge	4	2	2	1, 2	1, 2
r8idb.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r8idb.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8idb.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8idb.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r8idb.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r8idb.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8idb.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8idb.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r8idb.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
r9g.large	2	2	1	1, 2	1
r9g.xlarge	4	4	1	1, 2, 3, 4	1
r9g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r9g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r9g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r9g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r9g.16xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r9g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r9g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r9gd.large	2	2	1	1, 2	1
r9gd.xlarge	4	4	1	1, 2, 3, 4	1
r9gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r9gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r9gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r9gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1
r9gd.16xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r9gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
r9gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
u-3tb1.56xlarge	224	112	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112	1, 2
u-6tb1.56xlarge	224	224	1	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u-6tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-9tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u-12tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-18tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u-24tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u7i-6tb.112xlarge	448	224	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 152, 156, 160, 164, 168, 172, 176, 180, 184, 188, 192, 196, 200, 204, 208, 212, 216, 220, 224	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u7i-8tb.112xlarge	448	224	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 152, 156, 160, 164, 168, 172, 176, 180, 184, 188, 192, 196, 200, 204, 208, 212, 216, 220, 224	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u7i-12tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u7in-16tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u7in-24tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u7in-32tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
u7inh-32tb.480xlarge	1920	960	2	32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, 256, 272, 288, 304, 320, 336, 352, 368, 384, 400, 416, 432, 448, 464, 480, 496, 512, 528, 544, 560, 576, 592, 608, 624, 640, 656, 672, 688, 704, 720, 736, 752, 768, 784, 800, 816, 832, 848, 864, 880, 896, 912, 928, 944, 960	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x1e.xlarge	4	2	2	1, 2	1, 2
x1e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x1e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x1e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x2gd.large	2	2	1	1, 2	1
x2gd.xlarge	4	4	1	1, 2, 3, 4	1
x2gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x2gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x2gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x2gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x2gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
x2idn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x2idn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2idn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iedn.xlarge	4	2	2	1, 2	1, 2
x2iedn.2xlarge	8	4	2	2, 4	1, 2
x2iedn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iedn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x2iedn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x2iedn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2iedn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iezn.2xlarge	8	4	2	2, 4	1, 2
x2iezn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iezn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x2iezn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
x2iezn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
x8g.large	2	2	1	1, 2	1
x8g.xlarge	4	4	1	1, 2, 3, 4	1
x8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
x8aedz.large	2	2	1	1, 2	1
x8aedz.xlarge	4	4	1	1, 2, 3, 4	1
x8aedz.3xlarge	12	12	1	1, 2, 4, 6, 8, 10, 12	1
x8aedz.6xlarge	24	24	1	1, 2, 3, 4, 8, 12, 16, 20, 24	1
x8aedz.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48	1
x8aedz.24xlarge	96	96	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96	1
x8i.large	2	1	2	1	1, 2
x8i.xlarge	4	2	2	1, 2	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
x8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x8i.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
x8i.64xlarge	256	128	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128	1, 2
x8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
z1d.large	2	1	2	1	1, 2
z1d.xlarge	4	2	2	1, 2	1, 2
z1d.2xlarge	8	4	2	2, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
z1d.3xlarge	12	6	2	2, 4, 6	1, 2
z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Istanze con storage ottimizzato

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
d2.xlarge	4	2	2	1, 2	1, 2
d2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
d2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
d2.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
d3.xlarge	4	2	2	1, 2	1, 2
d3.2xlarge	8	4	2	2, 4	1, 2
d3.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
d3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.xlarge	4	2	2	1, 2	1, 2
d3en.2xlarge	8	4	2	2, 4	1, 2
d3en.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
d3en.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
h1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
h1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
h1.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
h1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i2.xlarge	4	2	2	1, 2	1, 2
i2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i2.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
i3.large	2	1	2	1	1, 2
i3.xlarge	4	2	2	1, 2	1, 2
i3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i3en.large	2	1	2	1	1, 2
i3en.xlarge	4	2	2	1, 2	1, 2
i3en.2xlarge	8	4	2	2, 4	1, 2
i3en.3xlarge	12	6	2	2, 4, 6	1, 2
i3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
i3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
i3en.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
i4g.large	2	2	1	1, 2	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i4g.xlarge	4	4	1	1, 2, 3, 4	1
i4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i4g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i4g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i4g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
i4i.large	2	1	2	1	1, 2
i4i.xlarge	4	2	2	1, 2	1, 2
i4i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i4i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i4i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i4i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i4i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i4i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i4i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
i7i.large	2	1	2	1	1, 2
i7i.xlarge	4	2	2	1, 2	1, 2
i7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
i7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
i7ie.large	2	1	2	1	1, 2
i7ie.xlarge	4	2	2	1, 2	1, 2
i7ie.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i7ie.3xlarge	12	6	2	1, 2, 3, 4, 5, 6	1, 2
i7ie.6xlarge	24	12	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i7ie.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i7ie.18xlarge	72	36	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i7ie.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
i7ie.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
i8g.large	2	2	1	1, 2	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i8g.xlarge	4	4	1	1, 2, 3, 4	1
i8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
i8ge.large	2	2	1	1, 2	1
i8ge.xlarge	4	4	1	1, 2, 3, 4	1
i8ge.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i8ge.3xlarge	12	12	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	1
i8ge.6xlarge	24	24	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i8ge.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i8ge.18xlarge	72	72	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i8ge.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
i8ge.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
im4gn.large	2	2	1	1, 2	1
im4gn.xlarge	4	4	1	1, 2, 3, 4	1
im4gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
im4gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
im4gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
im4gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
is4gen.medium	1	1	1	1	1
is4gen.large	2	2	1	1, 2	1
is4gen.xlarge	4	4	1	1, 2, 3, 4	1
is4gen.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
is4gen.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
is4gen.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Istanze di calcolo accelerate

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
dl1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
dl2q.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28,	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				30, 32, 34, 36, 38, 40, 42, 44, 46, 48	
f2.6xlarge	24	12	2	1, 2, 3, 6, 9, 12	1, 2
f2.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
f2.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
g3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
g3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g4ad.xlarge	4	2	2	2	1, 2
g4ad.2xlarge	8	4	2	2, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g4ad.4xlarge	16	8	2	2, 4, 8	1, 2
g4ad.8xlarge	32	16	2	2, 4, 8, 16	1, 2
g4ad.16xlarge	64	32	2	2, 4, 8, 16, 32	1, 2
g4dn.xlarge	4	2	2	2	1, 2
g4dn.2xlarge	8	4	2	2, 4	1, 2
g4dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
g4dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
g4dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
g4dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g5g.xlarge	4	4	1	1, 2, 3, 4	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g5g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
g5g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
g5g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g5g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
g6.xlarge	4	2	2	1, 2	1, 2
g6.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g6.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
g6.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
g6e.xlarge	4	2	2	1, 2	1, 2
g6e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6e.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
g6e.12xlarge	48	24	2	3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6e.16xlarge	64	32	2	4, 8, 12, 16, 20, 24, 28, 32	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g6e.24xlarge	96	48	2	6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6e.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
g6f.large	2	1	2	1	1, 2
g6f.xlarge	4	2	2	1, 2	1, 2
g6f.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6f.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2
gr6f.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g7.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
g7.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g7.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
g7.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g7.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g7.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
g7e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g7e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g7e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
g7e.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
g7e.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
g7e.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
inf1.xlarge	4	2	2	2	1, 2
inf1.2xlarge	8	4	2	2, 4	1, 2
inf1.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
inf1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
inf2.xlarge	4	2	2	1, 2	1, 2
inf2.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
inf2.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
inf2.48xlarge	192	96	2	4, 8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
p3.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
p3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
p3dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
p4de.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p5.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
p5.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
p5e.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
p5en.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
p6-b200.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
p6-b300.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
p6e-gb200.36xlarge	144	144	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100,	1

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
				101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144	
`trn1.2xlarge`	8	4	2	2, 4	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
trn1.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
trn1n.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
trn2.3xlarge	12	6	2	1, 2, 3, 4, 5, 6	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
trn2.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
trn2u.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
vt1.3xlarge	12	6	2	6	1, 2
vt1.6xlarge	24	12	2	6, 12	1, 2
vt1.24xlarge	96	48	2	6, 12, 48	1, 2

High-performance istanze di calcolo

Tipo di istanza	vCPU predefinite	Core CPU predefiniti	Thread per core predefiniti	Core CPU validi	Thread validi per core
hpc6id.32xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1
hpc8a.96xlarge	192	192	1	24, 48, 72, 96, 120, 144, 168, 192	1

Specifica delle opzioni della CPU per un'istanza Amazon EC2

Puoi specificare le opzioni della CPU durante o dopo l'avvio dell'istanza.

Processi

- Disabilitazione del multithreading simultaneo
- Specifica di un numero personalizzato di vCPU all'avvio
- Specifica di un numero personalizzato di vCPU in un modello di avvio
- Modifica delle opzioni della CPU per l'istanza EC2

Disabilitazione del multithreading simultaneo

Per disabilitare il multithreading simultaneo (SMT), noto anche come hyper-threading, specifica 1 thread per core.

Console

Per disabilitare l'SMT durante l'avvio dell'istanza

1. Segui la procedura Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console e configura l'istanza in base alle esigenze.
2. Espandi Dettagli avanzati e seleziona la casella di controllo Specifica le opzioni della CPU.
3. Per Core count (Numero di core), selezionare il numero di core CPU richiesti. In questo esempio, per specificare il numero di core CPU predefinito per un'istanza `r5.4xlarge`, scegliere 8.
4. Per disabilitare l'SMT, per Thread per core scegli 1.
5. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

AWS CLI

Per disabilitare l'SMT durante l'avvio dell'istanza

Utilizzate il AWS CLI comando run-instances e specificate il valore 1 for `ThreadsPerCore` per il parametro. `--cpu-options` Per `CoreCount`, specificare il numero di core CPU. In

questo esempio, per specificare il numero di core CPU predefinito per un'istanza `r7i.4xlarge`, specificare un valore di 8.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7i.4xlarge \
    --cpu-options "CoreCount=8,ThreadsPerCore=1" \
    --key-name my-key-pair
```

PowerShell

Per disabilitare l'SMT durante l'avvio dell'istanza

Utilizzate il New-EC2Instance comando e specificate il valore 1 for `ThreadsPerCore` per il parametro. `-CpuOptions` Per `CoreCount`, specificare il numero di core CPU. In questo esempio, per specificare il numero di core CPU predefinito per un'istanza `r7i.4xlarge`, specificare un valore di 8.

```
New-EC2Instance `
    -ImageId 'ami-0abcdef1234567890' `
    -InstanceType 'r7i.4xlarge' `
    -CpuOptions @{CoreCount=8; ThreadsPerCore=1} `
    -KeyName 'my-key-pair'
```

> **Note**
>
> Per disabilitare l'SMT per un'istanza esistente, segui la procedura mostrata in Modifica delle opzioni della CPU per l'istanza EC2 e modifica il numero di thread eseguiti per core in 1.

Specifica di un numero personalizzato di vCPU all'avvio

Puoi personalizzare il numero di core e di thread per core della CPU quando avvii un'istanza dalla console EC2 o dalla AWS CLI. Gli esempi in questa sezione utilizzano un tipo di istanza `r5.4xlarge`, caratterizzato dalle impostazioni predefinite riportate di seguito:

- Core della CPU: 8
- Thread per core: 2

Le istanze vengono avviate con il numero massimo di vCPU disponibili per il tipo di istanza per impostazione predefinita. Per questo tipo di istanza ci sono 16 vCPU totali (8 core con 2 thread ciascuno). Per ulteriori informazioni su questo tipo di istanza, consulta Istanze con memoria ottimizzata.

Nell'esempio seguente viene avviata un'istanza `r5.4xlarge` con 4 vCPU.

Console

Per specificare un numero personalizzato di vCPU durante l'avvio dell'istanza

1. Segui la procedura Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console e configura l'istanza in base alle esigenze.
2. Espandi Dettagli avanzati e seleziona la casella di controllo Specifica le opzioni della CPU.
3. Per ottenere 4 vCPU, specifica 2 core della CPU e 2 thread per core, come riportato di seguito:
   - Per Conteggio core scegli 2.
   - In Threads per core (Thread per core), scegliere 2.
4. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

AWS CLI

Per specificare un numero personalizzato di vCPU durante l'avvio dell'istanza

Utilizzate il AWS CLI comando run-instances e specificate il numero di core della CPU e il numero di thread nel parametro. `--cpu-options` Puoi specificare 2 core della CPU e 2 thread per core per ottenere 4 vCPU.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7i.4xlarge \
    --cpu-options "CoreCount=2,ThreadsPerCore=2" \
    --key-name my-key-pair
```

In alternativa, specifica 4 core della CPU e 1 thread per core (disabilita l'SMT) per ottenere 4 vCPU:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7i.4xlarge \
    --cpu-options "CoreCount=4,ThreadsPerCore=1" \
    --key-name my-key-pair
```

PowerShell

Per specificare un numero personalizzato di vCPU durante l'avvio dell'istanza

Utilizzate il New-EC2Instance comando e specificate il numero di core della CPU e il numero di thread nel parametro. `-CpuOptions` Puoi specificare 2 core della CPU e 2 thread per core per ottenere 4 vCPU.

```
New-EC2Instance `
    -ImageId 'ami-0abcdef1234567890' `
    -InstanceType 'r7i.4xlarge' `
    -CpuOptions @{CoreCount=2; ThreadsPerCore=2} `
    -KeyName 'my-key-pair'
```

In alternativa, specifica 4 core della CPU e 1 thread per core (disabilita l'SMT) per ottenere 4 vCPU:

```
New-EC2Instance `
    -ImageId 'ami-0abcdef1234567890' `
    -InstanceType 'r7i.4xlarge' `
    -CpuOptions @{CoreCount=4; ThreadsPerCore=1} `
    -KeyName 'my-key-pair'
```

Specifica di un numero personalizzato di vCPU in un modello di avvio

Puoi personalizzare il numero di core CPU e di thread per core per l'istanza in un modello di avvio. Gli esempi in questa sezione utilizzano un tipo di istanza `r5.4xlarge`, caratterizzato dalle impostazioni predefinite riportate di seguito:

- Core della CPU: 8
- Thread per core: 2

Le istanze vengono avviate con il numero massimo di vCPU disponibili per il tipo di istanza per impostazione predefinita. Per questo tipo di istanza ci sono 16 vCPU totali (8 core con 2 thread ciascuno). Per ulteriori informazioni su questo tipo di istanza, consulta Istanze con memoria ottimizzata.

L'esempio seguente crea un modello di avvio che specifica la configurazione per un'istanza `r5.4xlarge` con 4 vCPU.

Console

Per specificare un numero personalizzato di vCPU in un modello di avvio

1. Segui la procedura Creare un modello di avvio specificando i parametri e configura il modello di avvio in base alle esigenze.
2. Espandi Dettagli avanzati e seleziona la casella di controllo Specifica le opzioni della CPU.
3. Per ottenere 4 vCPU, specifica 2 core della CPU e 2 thread per core, come riportato di seguito:
   - Per Conteggio core scegli 2.
   - In Threads per core (Thread per core), scegliere 2.
4. Nel pannello Riepilogo, verifica la configurazione dell'istanza, quindi scegli Crea modello di avvio. Per ulteriori informazioni, consulta Archivia i parametri di avvio dell'istanza nei modelli di avvio di Amazon EC2.

AWS CLI

Per specificare un numero personalizzato di vCPU in un modello di avvio

Utilizzate il AWS CLI comando create-launch-template e specificate il numero di core della CPU e il numero di thread nel parametro. `CpuOptions` Puoi specificare 2 core della CPU e 2 thread per core per ottenere 4 vCPU.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForCPUOptions \
    --version-description CPUOptionsVersion1 \
    --launch-template-data file://template-data.json
```

Di seguito è riportato un file JSON di esempio che contiene i dati del modello di avvio, che includono le opzioni della CPU, per la configurazione dell'istanza per questo esempio.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-0abcdef1234567890"
    }],
    "ImageId": "ami-0abcdef1234567890",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":2,
        "ThreadsPerCore":2
    }
}
```

In alternativa, specifica 4 core della CPU e 1 thread per core (disabilita l'SMT) per ottenere 4 vCPU:

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-0abcdef1234567890"
    }],
    "ImageId": "ami-0abcdef1234567890",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
```

```
        "ThreadsPerCore":1
    }
}
```

PowerShell

Per specificare un numero personalizzato di vCPU in un modello di avvio

Utilizzo della New-EC2LaunchTemplate.

```
New-EC2LaunchTemplate `
    -LaunchTemplateName 'TemplateForCPUOptions' `
    -VersionDescription 'CPUOptionsVersion1' `
    -LaunchTemplateData (Get-Content -Path 'template-data.json' | ConvertFrom-Json)
```

Modifica delle opzioni della CPU per l'istanza EC2

Man mano che le tue esigenze cambiano nel tempo, potresti dover modificare la configurazione delle opzioni della CPU per un'istanza esistente. Ciascun thread eseguito sull'istanza è noto come CPU virtuale (vCPU). Puoi modificare il numero di vCPU in esecuzione per un'istanza esistente nella console, nell'API o negli SDK di Amazon EC2. AWS CLI Lo stato dell'istanza deve essere `Stopped` prima di poter apportare questa modifica.

Per visualizzare i passaggi della console o della riga di comando, seleziona la scheda corrispondente al tuo ambiente. Per informazioni sulle richieste e sulle risposte alle API, consulta ModifyInstanceCpuOptions Amazon EC2 API Reference.

Console

Segui questa procedura per modificare il numero di vCPU attive per la tua istanza dalla Console di gestione AWS.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Istanze. Si apre l'elenco delle istanze definite per la Regione AWS attuale.
3. Nell'elenco Istanze seleziona l'istanza. In alternativa, puoi selezionare il link dell'istanza per aprire la pagina di dettaglio dell'istanza.
4. Se l'istanza è in esecuzione, è necessario prima arrestarla. Scegli Arresta istanza dal menu Stato istanza.

5. Per modificare la configurazione della vCPU, scegli Modifica opzioni della CPU da Impostazioni istanza nel menu Operazioni. Si apre la pagina Modifica opzioni della CPU.
6. Seleziona una delle seguenti opzioni della CPU per modificare la configurazione dell'istanza.

   Utilizza le opzioni della CPU predefinite

   Questa opzione reimposta l'istanza al numero di vCPU predefinito per il tipo di istanza. L'impostazione predefinita prevede l'esecuzione di tutti i thread per tutti i core della CPU.

   Specifica delle opzioni della CPU

   Questa opzione consente la configurazione del numero di vCPU in esecuzione sull'istanza.
7. Se scegli Specifica le opzioni della CPU, vengono visualizzati i campi vCPU attive.

   - Utilizza il primo selettore per configurare il numero di thread eseguiti per ciascun core della CPU. Per disabilitare il multithreading simultaneo, scegli 1.
   - Utilizza il secondo selettore per configurare il numero di CPU in esecuzione sull'istanza.

   I seguenti campi vengono aggiornati dinamicamente man mano che apporti modifiche ai selettori delle opzioni della CPU.

   - VCPU attive: il numero di core della CPU moltiplicato per i thread per core, in base alle selezioni effettuate. Ad esempio, se hai selezionato 2 thread e 4 core, ciò equivale a 8 vCPU.
   - VCPU totali: il numero massimo di vCPU per il tipo di istanza. Ad esempio, per un tipo di istanza `m6i.4xlarge`, sono 16 vCPU (8 core in esecuzione con 2 thread ciascuno).
8. Per applicare gli aggiornamenti, scegli Modifica.

AWS CLI

Segui questa procedura per modificare il numero di vCPU attive per la tua istanza dalla AWS CLI.

Utilizza il comando modify-instance-cpu-options e specifica il numero di core della CPU eseguiti nel parametro `--core-count` e il numero di thread eseguiti per core nel parametro `--threads-per-core`.

Gli esempi seguenti mostrano due possibili configurazioni su un'istanza di tipo `m6i.4xlarge` per eseguire 8 vCPU sull'istanza specificata. L'impostazione predefinita per questo tipo di istanza è 16 vCPU (8 core in esecuzione con 2 thread ciascuno).

Esempio 1: Esegui 4 core della CPU con 2 thread per core, per un totale di 8 vCPU.

```
aws ec2 modify-instance-cpu-options \
    --instance-id i-1234567890abcdef0 \

    --core-count=4 \
    --threads-per-core=2
```

Esempio 2: Disabilita il multithreading simultaneo modificando il numero di thread eseguiti per core in 1. La configurazione risultante esegue anche un totale di 8 vCPU (8 core della CPU con 1 thread per core).

```
aws ec2 modify-instance-cpu-options \
    --instance-id 1234567890abcdef0 \
    --core-count=8 \
    --threads-per-core=1
```

PowerShell

Per modificare il numero di vCPU attive per un'istanza

Utilizza il Edit-EC2InstanceCpuOption cmdlet e specifica il numero di core della CPU eseguiti nel `-CoreCount` parametro e il numero di thread eseguiti per core nel parametro. `ThreadsPerCore`

Esempio 1: Esegui 4 core della CPU con 2 thread per core, per un totale di 8 vCPU.

```
Edit-EC2InstanceCpuOption `
    -InstanceId 'i-1234567890abcdef0' `
    -CoreCount 4 `
    -ThreadsPerCore 2
```

Esempio 2: Disabilita il multithreading simultaneo modificando il numero di thread eseguiti per core in 1. La configurazione risultante esegue anche un totale di 8 vCPU (8 core della CPU con 1 thread per core).

```
Edit-EC2InstanceCpuOption `
    -InstanceId 'i-1234567890abcdef0' `
```

```
    -CoreCount 8 `
    -ThreadsPerCore 1
```

Visualizzazione di thread e core della CPU per un'istanza Amazon EC2

Puoi visualizzare le opzioni CPU per un'istanza esistente o descrivendo l'istanza.

Console

Per visualizzare le opzioni della CPU per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra scegliere Instances (Istanze) e selezionare l'istanza.
3. Nella scheda Details (Dettagli) in Host and placement group (Host e gruppo di collocamento), trovare Number of vCPUs (Numero di vCPU).

AWS CLI

Per visualizzare le opzioni della CPU per un'istanza

Utilizzare il comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].CpuOptions
```

Di seguito è riportato un output di esempio. Il campo `CoreCount` indica il numero di core per l'istanza. Il campo `ThreadsPerCore` indica il numero di thread per core.

```
[
    {
        "CoreCount": 24,
        "ThreadsPerCore": 2
    },
]
```

PowerShell

Per visualizzare le opzioni della CPU per un'istanza

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId 'i-1234567890abcdef0').Instances.CpuOptions
```

Di seguito è riportato un output di esempio.

```
AmdSevSnp CoreCount ThreadsPerCore
--------- --------- --------------
          24        2
```

In alternativa, per visualizzare le informazioni sulla CPU, puoi connetterti all'istanza e utilizzare uno dei seguenti strumenti di sistema:

- Windows `Task Manager` sull'istanza Windows
- Il comando lscpu sull'istanza Linux

È possibile utilizzarlo AWS Config per registrare, valutare, controllare e valutare le modifiche alla configurazione delle istanze, incluse le istanze terminate. Per ulteriori informazioni, consulta Nozioni di base su AWS Config nella AWS Config Guida per gli sviluppatori.

Ottimizza le CPU per le istanze License-Included

I carichi di lavoro come Microsoft SQL Server richiedono spesso livelli elevati di memoria e IOPS ma un basso numero di vCPU. AWS offre un'ampia gamma di tipi di istanze in grado di soddisfare la maggior parte delle esigenze di infrastruttura. Tuttavia, per ridurre i costi di CPU-based licenza per Windows e Microsoft SQL Server, puoi personalizzare il numero di vCPU in esecuzione sull'istanza EC2 mantenendo le stesse specifiche di memoria, storage e rete. Questo approccio può far risparmiare sui costi delle licenze sia per i carichi CPU-based di lavoro con licenza inclusa che per quelli (BYOL). Bring-Your-Own-License Puoi specificare le opzioni della CPU quando avvii o modifichi un'istanza utilizzando la console o l'API Amazon EC2. Per istruzioni, consulta l'argomento Specifica delle opzioni della CPU per un'istanza Amazon EC2.

Per ulteriori informazioni, consulta questo post del blog sulle best practice per ottimizzare le CPU per i carichi di lavoro di SQL Server.

Tipi di licenza supportati

Ottimizzazione CPU supporta la fatturazione in base al numero di CPU attive per i seguenti tipi di configurazioni di licenza per le istanze avviate da un'AMI inclusa nella licenza. Per ulteriori informazioni sui tipi di licenza, consulta Campi informativi di fatturazione AMI.

License-included Fatturazione delle istanze AMI

Licenze incluse	Operazione di utilizzo	Prezzo all'ora per vCPU
Windows Server	RunInstances:0002	0,046 USD
Windows Server con SQL Server Enterprise	RunInstances:0102	0,421 USD
Windows Server con SQL Server Standard	RunInstances:0006	0,166$
Windows Server con SQL Server Web	RunInstances:0202	0,063 USD

Opzioni di acquisto supportate

Ottimizzazione CPU supporta le seguenti opzioni di acquisto per le istanze con licenza inclusa:

- On-Demand
- Savings Plans

> **Warning**
>
> Se utilizzi istanze riservate, è possibile che non vengano applicati sconti quando configuri Ottimizzazione CPU per istanze con licenza inclusa nello stesso account di pagamento. Ti consigliamo di utilizzare i piani di risparmio per ridurre i costi di CPU-based licenza e offrire risparmi comparabili sui costi di elaborazione.

Gli account che utilizzavano sia Ottimizzazione CPU che le istanze riservate per Windows e SQL Server sullo stesso tipo di istanza prima del 15 ottobre 2025 sono stati aggiunti a un elenco di esclusione per mantenere la loro attuale esperienza di fatturazione. Per sfruttare i risparmi sulle licenze di Ottimizzazione CPU, contatta il centro Supporto AWS per effettuare la rimozione dall'elenco di esclusione.

Come funziona Ottimizzazione CPU per risparmiare sui costi di licenza

Gli esempi seguenti aiutano a illustrare i risparmi sui costi che sono possibili quando configuri l'utilizzo della CPU.

Esempio 1: fatturazione predefinita Questo esempio mostra un'istanza r7i.8xlarge avviata da un'AMI Windows e SQL Server Enterprise inclusa nella licenza eseguita per 100 ore con la configurazione CPU predefinita di 32 vCPU per il tipo di istanza (3.200 ore della vCPU).

La fattura mostra una voce con una tariffa combinata che include sia i costi di utilizzo che quelli di licenza.

For illustration purposes only **Amazon Web Services, Inc. charges by service** **Total services: 1** **Description**	**Usage Quantity**	**Total charges** **$1,558.88** **Amount in USD**
Elastic Compute Cloud		$1,558.88
|- US East (N. Virginia)		$1,558.88
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$1,558.88
| |- $15.5888 per On Demand Windows with SQL Server Enterprise r7i.8xlarge Instance Hour	100 Hrs	$1,558.88

Esempio 2: fatturazione di Ottimizzazione CPU Questo esempio mostra un'istanza r7i.8xlarge avviata da un'AMI Windows e SQL Server Enterprise inclusa nella licenza. Per risparmiare sui costi di licenza, il numero di CPU attive è stato ridotto a 16 vCPU. Quindi l'istanza è stata eseguita per 100 ore con la nuova configurazione.

La fattura mostra le seguenti due voci.

Descrizione della fatturazione: Elastic Compute Cloud

La prima riga mostra il costo di base dell'istanza Windows e SQL Server eseguita per 100 ore (211,68 USD).

Descrizione della fatturazione: Costi di terze parti di Ottimizzazione CPU di Amazon EC2 inclusa nella licenza

La seconda riga copre i costi di licenza in base al numero di vCPU attive durante il periodo di fatturazione (673,60 USD).

For illustration purposes only **Amazon Web Services, Inc. charges by service** **Total services: 2** **Description**	**Usage Quantity**	**Total charges** **$885.28** **Amount in USD**
Elastic Compute Cloud		$211.68
|- US East (N. Virginia)		$211.68
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$211.68
| |- $2.1168 per On Demand Windows and SQL Server Enterprise without licenses r7i.8xlarge Instance Hr	100 Hrs	$211.68
Amazon EC2 Optimize CPU License Included Third Party Fees		$673.60
|- US East (N. Virginia)		$673.60
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$673.60
| |- $0.421 per vCPU-Hour of On Demand Windows with SQL Server licenses on r7i Instance	1,600 vCPU-Hrs	$673.60

Esempio 3: fatturazione di Ottimizzazione CPU con Savings Plans Questo esempio mostra un'istanza r7i.8xlarge avviata da un'AMI Windows e SQL Server Enterprise inclusa nella licenza. Per risparmiare sui costi di licenza, il numero di CPU attive è stato ridotto a 16 vCPU. Quindi l'istanza è stata eseguita per 100 ore con la nuova configurazione.

Un piano di risparmio di un anno senza anticipazioni di calcolo con un dollaro. 60/hour L'impegno (arrotondato) offre ulteriori risparmi sui costi che riducono il costo di base dell'istanza Windows e SQL Server. L'impegno del piano di risparmio copre l'intero utilizzo per 100 ore dell'istanza r7i.8xlarge per una tariffa di Savings Plans di 1 USD. 53362/hour.

La fattura presenta le seguenti voci.

Descrizione della fatturazione: utilizzo di Savings Plans per il calcolo

La prima riga mostra l'impegno di Savings Plans per l'utilizzo completo di 100 ore (160,00 USD).

Descrizione della fatturazione: Elastic Compute Cloud

La seconda riga contiene due voci. La prima voce mostra quale sarebbe stato il costo di base dell'istanza Windows e SQL Server in esecuzione per 100 ore senza Savings Plans (211,68 USD). La seconda voce mostra che l'intero costo di base è stato coperto dal Savings Plans per il calcolo (-211,68 USD), che produce un costo netto pari a zero per questa riga.

Descrizione della fatturazione: Costi di terze parti di Ottimizzazione CPU di Amazon EC2 inclusa nella licenza

La terza riga copre i costi di licenza in base al numero di vCPU attive durante il periodo di fatturazione (673,60 USD).

For illustration purposes only
Amazon Web Services, Inc. charges by service **Total charges**
Total services: 3 **$833.60**

Description	Usage Quantity	Amount in USD
Savings Plans for Compute usage		$160.00
|- Any		$160.00
|- Compute Savings Plans		$160.00
| |- 1 year No Upfront Compute Savings Plan	100 Hrs	$160.00
Elastic Compute Cloud		$0.00
|- US East (N. Virginia)		$0.00
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$0.00
| |- $2.1168 per On Demand Windows and SQL Server Enterprise without licenses r7i.8xlarge Instance Hr	100 Hrs	$211.68
| |- r7i.8xlarge Windows with SQL Server Enterprise without licenses instance usage covered by CSP	100 Hrs	($211.68)
Amazon EC2 Optimize CPU License Included Third Party Fees		$673.60
|- US East (N. Virginia)		$673.60
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$673.60
| |- $0.421 per vCPU-Hour of On Demand Windows with SQL Server licenses on r7i Instance	1,600 vCPU-Hrs	$673.60

Istanze AMD SEV-SNP per Amazon EC2

AMD Secure Encrypted Virtualization-Secure Nested Paging (AMD SEV-SNP) è una funzionalità della CPU che fornisce le seguenti proprietà:

- Attestazione: AMD SEV-SNP consente di recuperare un rapporto di attestazione firmato che contiene una misura crittografica che può essere utilizzata per convalidare lo stato e l'identità dell'istanza e che è in esecuzione su hardware AMD originale. Per ulteriori informazioni, consulta Attesta un'istanza Amazon EC2 con AMD SEV-SNP.
- Crittografia della memoria: a partire dai processori AMD EPYC (Milano), AWS Graviton2 e Intel Xeon Scalable (Ice Lake), la memoria dell'istanza è sempre crittografata.

Puoi usare AMD SEV-SNP con host dedicati o con tenancy condivisa.

Indice

- Concetti e terminologia
- Requisiti
- Considerazioni
- Prezzi

- Trova i tipi di istanze EC2 che supportano AMD SEV-SNP
- Abilita AMD SEV-SNP per un'istanza EC2
- Attesta un'istanza Amazon EC2 con AMD SEV-SNP

Concetti e terminologia

Prima di iniziare a usare AMD SEV-SNP, assicurati di conoscere i concetti e la terminologia seguenti.

Rapporto di SEV-SNP attestazione AMD

Il rapporto di SEV-SNP attestazione AMD è un documento che un'istanza può richiedere alla CPU. Il rapporto di SEV-SNP attestazione AMD può essere utilizzato per convalidare lo stato e l'identità di un'istanza e per verificare che sia in esecuzione in un ambiente AMD sanzionato. Il rapporto include una misurazione di avvio, che è un hash crittografico dello stato di avvio iniziale di un'istanza, incluso il contenuto della memoria dell'istanza iniziale e lo stato iniziale delle vCPU. Il rapporto di SEV-SNP attestazione AMD è firmato con una firma VCEK (su host dedicati) o una firma VLEK (su tenancy condivisa) che riconduce a una radice di fiducia AMD.

VCEK

La Versioned Chip Endorsement Key (VCEK) è una chiave di firma per chip certificata da AMD e utilizzata dalla CPU AMD per firmare i report di attestazione AMD sugli host dedicati. SEV-SNP Le firme VCEK possono essere convalidate utilizzando i certificati forniti da AMD.

VLEK

La Versioned Loaded Endorsement Key (VLEK) è una chiave di firma con versione certificata da AMD e utilizzata dalla CPU AMD per firmare i report di attestazione AMD sulla tenancy condivisa. SEV-SNP Le firme VLEK possono essere convalidate utilizzando i certificati forniti da AMD.

Binario OVMF

L'Open Virtual Machine Firmware (OVMF) è il codice di avvio anticipato utilizzato per fornire un ambiente UEFI per l'istanza. Il codice di avvio anticipato viene eseguito prima dell'avvio del codice nell'AMI. L'OVMF trova ed esegue anche il boot loader fornito nell'AMI. Per ulteriori informazioni, consulta il repository OVMF.

Requisiti

I requisiti per AMD SEV-SNP dipendono dall'utilizzo di host dedicati o di una tenancy condivisa.

Requisiti per gli host dedicati

Per utilizzare AMD SEV-SNP con host dedicati, è necessario soddisfare i seguenti requisiti:

- Utilizzare uno dei seguenti tipi di istanza supportati:
  - Uso generico: `m6a.large` | `m6a.xlarge` | `m6a.2xlarge` | `m6a.4xlarge` | `m6a.8xlarge`
  - Ottimizzate per il calcolo: `c6a.large` | `c6a.xlarge` | `c6a.2xlarge` | `c6a.4xlarge` | `c6a.8xlarge` | `c6a.12xlarge` | `c6a.16xlarge`
  - Ottimizzate per la memoria: `r6a.large` | `r6a.xlarge` | `r6a.2xlarge` | `r6a.4xlarge`
- Assegna un host dedicato con AMD SEV-SNP abilitato. Per ulteriori informazioni, consulta Assegna un host dedicato con AMD SEV-SNP.
- Avvia la tua istanza in qualsiasi spot pubblicitario Regione AWS.
- Usa un'AMI con `uefi` o in modalità di `uefi-preferred` avvio e un sistema operativo che supporti AMD SEV-SNP. Perché AWS, AMD SEV-SNP è supportato su AL2023, RHEL 9.3, SLES 15 SP4 e Ubuntu 23.04 e versioni successive.

Requisiti per la locazione condivisa

Per utilizzare AMD SEV-SNP con una proprietà condivisa, è necessario soddisfare i seguenti requisiti:

- Utilizzare uno dei seguenti tipi di istanza supportati:
  - Uso generico: `m6a.large` | `m6a.xlarge` | `m6a.2xlarge` | `m6a.4xlarge` | `m6a.8xlarge`
  - Ottimizzate per il calcolo: `c6a.large` | `c6a.xlarge` | `c6a.2xlarge` | `c6a.4xlarge` | `c6a.8xlarge` | `c6a.12xlarge` | `c6a.16xlarge`
  - Ottimizzate per la memoria: `r6a.large` | `r6a.xlarge` | `r6a.2xlarge` | `r6a.4xlarge`
- Avvia la tua istanza in uno dei seguenti paesi supportati Regione AWS: Stati Uniti orientali (Ohio) o Europa (Irlanda).
- Usa un'AMI con `uefi` o in modalità di `uefi-preferred` avvio e un sistema operativo che supporti AMD SEV-SNP. Perché AWS, AMD SEV-SNP è supportato su AL2023, RHEL 9.3, SLES 15 SP4 e Ubuntu 23.04 e versioni successive.

Considerazioni

Puoi abilitare AMD SEV-SNP solo quando avvii un'istanza. Quando AMD SEV-SNP è abilitato per il lancio dell'istanza, si applicano le seguenti regole.

- Una volta abilitata, AMD non SEV-SNP può essere disattivata. Rimane abilitato per tutto il ciclo di vita dell'istanza.
- È possibile modificare il tipo di istanza solo con un altro tipo di istanza che supporti AMD SEV-SNP.
- Hibernation e Nitro Enclaves non sono supportati.

Considerazioni aggiuntive per gli host dedicati

Le seguenti considerazioni aggiuntive si applicano quando si utilizza AMD SEV-SNP con host dedicati:

- Gli aggiornamenti del firmware vengono applicati quando si assegna un host. Per ottenere il firmware più recente, rilasciate l'host esistente e assegnatene uno nuovo. Per ulteriori informazioni, consulta Aggiorna il firmware su un host dedicato AMD SEV-SNP.
- Puoi avviare istanze con o senza AMD SEV-SNP abilitato su un host dedicato con supporto AMD SEV-SNP .
- Sono supportati i gruppi di risorse degli host e le prenotazioni di host dedicati.

Considerazioni aggiuntive sulla locazione condivisa

Le seguenti considerazioni aggiuntive si applicano quando si utilizza AMD SEV-SNP con tenancy condivisa:

- Se è prevista la manutenzione dell'host sottostante dell'istanza, riceverai una notifica dell'evento programmato 14 giorni prima dell'evento. È necessario interrompere o riavviare manualmente l'istanza per spostarla su un nuovo host.

Prezzi

Host dedicati

Non sono previsti costi aggiuntivi per l'utilizzo di AMD SEV-SNP su host dedicati. Paghi solo il prezzo standard degli host dedicati. Per ulteriori informazioni, consulta i prezzi degli host dedicati.

Locazione condivisa

Quando avvii un'istanza Amazon EC2 con AMD SEV-SNP abilitata sulla tenancy condivisa, ti viene addebitata una tariffa oraria aggiuntiva di utilizzo equivalente al 10% della On-Demand tariffa oraria del tipo di istanza selezionato. Questa tariffa di SEV-SNP utilizzo AMD è una tariffa separata rispetto all'utilizzo dell'istanza Amazon EC2. Le istanze riservate, Savings Plans e l'utilizzo del sistema operativo non influiscono su questa tariffa.

Se configuri un'istanza Spot per l'avvio con AMD SEV-SNP abilitato sulla tenancy condivisa, ti verrà addebitata una tariffa oraria aggiuntiva di utilizzo equivalente al 10% della On-Demand tariffa oraria del tipo di istanza selezionato. Se la strategia di allocazione utilizza il prezzo come input, il parco istanze spot non include questa tariffa aggiuntiva; viene utilizzato solo il prezzo spot.

Trova i tipi di istanze EC2 che supportano AMD SEV-SNP

Puoi trovare tipi di istanze che supportano AMD SEV-SNP. La console Amazon EC2 non mostra questa informazione per un tipo di istanza.

AWS CLI

Per trovare i tipi di istanze che supportano AMD SEV-SNP

Utilizza il seguente comando describe-instance-types.

```
aws ec2 describe-instance-types \
    --filters Name=processor-info.supported-features,Values=amd-sev-snp \
    --query 'InstanceTypes[*].[InstanceType]' \
    --output text | sort
```

Di seguito è riportato un output di esempio.

```
c6a.12xlarge
c6a.16xlarge
c6a.2xlarge
c6a.4xlarge
c6a.8xlarge
c6a.large
c6a.xlarge
m6a.2xlarge
m6a.4xlarge
m6a.8xlarge
m6a.large
```

```
m6a.xlarge
r6a.2xlarge
r6a.4xlarge
r6a.large
r6a.xlarge
```

PowerShell

Per trovare i tipi di istanze che supportano AMD SEV-SNP

Utilizza il cmdlet Get-EC2InstanceType.

```
(Get-EC2InstanceType `
    -Filter @{Name="processor-info.supported-features"; Values="amd-sev-
snp"}).InstanceType.Value | Sort-Object
```

Di seguito è riportato un output di esempio.

```
c6a.12xlarge
c6a.16xlarge
c6a.2xlarge
c6a.4xlarge
c6a.8xlarge
c6a.large
c6a.xlarge
m6a.2xlarge
m6a.4xlarge
m6a.8xlarge
m6a.large
m6a.xlarge
r6a.2xlarge
r6a.4xlarge
r6a.large
r6a.xlarge
```

Abilita AMD SEV-SNP per un'istanza EC2

Puoi avviare un'istanza con AMD SEV-SNP abilitato. Non puoi abilitare AMD SEV-SNP dopo il lancio.

Indice

- Assegna un host dedicato con AMD SEV-SNP

- Avvia le istanze su un host SEV-SNP dedicato AMD
- Aggiorna il firmware su un host dedicato AMD SEV-SNP
- Avvia un'istanza con AMD SEV-SNP in affitto condiviso
- Controlla se un'istanza EC2 è abilitata per AMD SEV-SNP

Assegna un host dedicato con AMD SEV-SNP

Prima di poter avviare istanze con AMD SEV-SNP su un host dedicato, è necessario allocare un host dedicato con il supporto AMD SEV-SNP abilitato. Assegni un host dedicato per famiglia di istanze (ad esempio, m6a, r6a o c6a), quindi puoi eseguire qualsiasi tipo di istanza supportato di quella famiglia sull'host. Puoi allocare un host dedicato con AMD in qualsiasi spot pubblicitario. SEV-SNP Regione AWS

Console

Per allocare un host dedicato con AMD abilitato SEV-SNP

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Scegli Assegna host dedicato.
4. Per AMD SEV-SNP, scegli Abilita.
5. Configurate le restanti impostazioni dell'host secondo necessità, quindi scegliete Alloca.

AWS CLI

Per allocare un host dedicato con AMD abilitato SEV-SNP

Utilizzare il comando allocate-hosts con i parametri `--instance-type` e `--cpu-options`.

```
aws ec2 allocate-hosts \
    --instance-type "m6a.large" \
    --availability-zone "us-east-1a" \
    --auto-placement "off" \
    --cpu-options AmdSevSnp=enabled \
    --quantity 1
```

Di seguito è riportato un output di esempio.

```
{
    "HostIds": [
        "h-0123456789abcdef0"
    ]
}
```

> **Note**
>
> Quando si assegna un host dedicato con AMD SEV-SNP abilitato, l'host entra in uno `configuring` stato in cui AWS applica il firmware più recente. Questa operazione può richiedere da pochi minuti a 2 ore. L'addebito viene effettuato durante lo `configuring` stato.

Avvia le istanze su un host SEV-SNP dedicato AMD

È possibile avviare un'istanza con AMD SEV-SNP abilitato dopo aver configurato l'host dedicato.

> **Note**
>
> Puoi anche avviare istanze senza AMD SEV-SNP abilitato su un host dedicato allocato con AMD. SEV-SNP Le SEV-SNP istanze AMD SEV-SNP e non AMD possono essere eseguite fianco a fianco sullo stesso host.

AWS CLI

Per avviare un'istanza con AMD SEV-SNP su un host dedicato

Usa il run-instances comando con le `--placement` opzioni `--cpu-options` e. Sostituiscilo *`h-0123456789abcdef0`* con l'ID dell'host dedicato assegnato.

```
aws ec2 run-instances \
    --instance-type m6a.xlarge \
    --image-id ami-0123456789example \
    --cpu-options AmdSevSnp=enabled \
    --placement HostId=h-0123456789abcdef0
```

PowerShell

Per avviare un'istanza con AMD SEV-SNP su un host dedicato

Usa il New-EC2Instance cmdlet con i parametri `-CpuOption` and`-Placement_HostId`.

```
New-EC2Instance `
    -InstanceType m6a.xlarge `
    -ImageId ami-0123456789example `
    -CpuOption @{AmdSevSnp="enabled"} `
    -Placement_HostId h-0123456789abcdef0
```

Aggiorna il firmware su un host dedicato AMD SEV-SNP

Quando assegni un host dedicato con AMD SEV-SNP abilitato, AWS applica il firmware più recente disponibile all'host. Gli aggiornamenti del firmware possono includere patch di sicurezza e miglioramenti delle funzionalità di AMD.

Per applicare gli aggiornamenti del firmware, assegnate un nuovo host (che riceve il firmware più recente), spostate le istanze sul nuovo host e quindi rilasciate il vecchio host.

1. Assegna un nuovo host dedicato con AMD abilitato. SEV-SNP Il nuovo host riceve l'ultimo firmware disponibile. Per ulteriori informazioni, consulta Assegna un host dedicato con AMD SEV-SNP.
2. Arresta le istanze in esecuzione sul vecchio host dedicato.

   ```
   aws ec2 stop-instances \
       --instance-ids i-0123456789example
   ```
3. Modifica la posizione dell'istanza per indirizzare il nuovo host dedicato. Utilizza il comando modify-instance-placement.

   ```
   aws ec2 modify-instance-placement \
       --instance-id i-0123456789example \
       --host-id h-09876543210abcdef
   ```
4. Avvia le istanze sul nuovo host dedicato.

   ```
   aws ec2 start-instances \
       --instance-ids i-0123456789example
   ```
5. Rilascia il vecchio host dedicato. Utilizza il comando release-hosts.

   ```
   aws ec2 release-hosts \
   ```

```
    --host-ids h-0123456789abcdef0
```

> **Note**
>
> Ricevi le notifiche di manutenzione per i tuoi host dedicati nello stesso modo in cui le ricevi per altri eventi di manutenzione degli host dedicati. Quando ricevete una notifica, seguite i passaggi precedenti per passare a un nuovo host con firmware aggiornato.

Avvia un'istanza con AMD SEV-SNP in affitto condiviso

Puoi avviare un'istanza con AMD SEV-SNP in affitto condiviso negli Stati Uniti orientali (Ohio) ed Europa (Irlanda).

AWS CLI

Per avviare un'istanza con AMD in tenancy SEV-SNP condivisa

Utilizza il comando run-instances con l'opzione `--cpu-options`.

```
aws ec2 run-instances \
    --instance-type m6a.xlarge \
    --image-id ami-0123456789example \
    --cpu-options AmdSevSnp=enabled
```

PowerShell

Per avviare un'istanza con AMD SEV-SNP in tenancy condivisa

Usa il New-EC2Instance cmdlet con il parametro. `-CpuOption`

```
New-EC2Instance `
    -InstanceType m6a.xlarge `
    -ImageId ami-0123456789example `
    -CpuOption @{AmdSevSnp="enabled"}
```

Controlla se un'istanza EC2 è abilitata per AMD SEV-SNP

Puoi trovare istanze abilitate per AMD. SEV-SNP La console Amazon EC2 non mostra questa informazione.

AWS CLI

Per verificare se AMD SEV-SNP è abilitato per un'istanza

Utilizza il comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].CpuOptions
```

Di seguito è riportato un output di esempio. Se non `AmdSevSnp` è presente`CpuOptions`, allora AMD SEV-SNP è disabilitato.

```
[
    {
        "AmdSevSnp": "enabled",
        "CoreCount": 1,
        "ThreadsPerCore": 2
    }
]
```

PowerShell

Per verificare se AMD SEV-SNP è abilitato per un'istanza

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.CpuOptions
```

Di seguito è riportato un output di esempio. Se il valore di non `AmdSevSnp` è presente, AMD SEV-SNP è disabilitato.

```
AmdSevSnp CoreCount ThreadsPerCore
--------- --------- --------------
enabled   1         2
```

AWS CloudTrail

In AWS CloudTrail caso di richiesta di avvio dell'istanza, la seguente proprietà indica che AMD SEV-SNP è abilitato per l'istanza.

```
"cpuOptions": {"AmdSevSnp": "enabled"}
```

Attesta un'istanza Amazon EC2 con AMD SEV-SNP

L'attestazione è un processo che consente all'istanza di dimostrare il suo stato e la sua identità. Dopo aver abilitato AMD SEV-SNP per la tua istanza, puoi richiedere un rapporto di SEV-SNP attestazione AMD al processore sottostante. Il rapporto di SEV-SNP attestazione AMD contiene un hash crittografico, chiamato Launch Measurement, del contenuto iniziale della memoria guest e dello stato iniziale della vCPU. Il rapporto di attestazione è firmato con una firma VCEK (sugli host dedicati) o una firma VLEK (sulla proprietà condivisa) che riconduce a una radice di fiducia AMD. È possibile utilizzare la misurazione di avvio inclusa nel rapporto di attestazione per verificare che l'istanza sia in esecuzione in un ambiente AMD originale e per convalidare il codice di avvio iniziale utilizzato per avviare l'istanza.

Prerequisito

Avvia un'istanza abilitata per AMD. SEV-SNP Per ulteriori informazioni, consulta Abilita AMD SEV-SNP per un'istanza EC2.

Indice

- Attestazione per le istanze su host dedicati
- Attestazione per casi di locazione condivisa

Attestazione per le istanze su host dedicati

Gli host dedicati utilizzano una Versioned Chip Endorsement Key (VCEK), una chiave di firma univoca per chip, per firmare il rapporto di attestazione. È necessario convalidare la catena di fiducia dal certificato VCEK alla radice di fiducia di AMD.

> **Note**
>
> Il modello di processore attualmente supportato è. `milan`

Prerequisiti

Un'istanza in esecuzione su un host dedicato SEV-SNP abilitato per AMD con Git, Cargo e Perl installati.

Passaggio 1: crea l'utilità snpguest

In questo passaggio, si installa e si crea l'`snpguest`utilità, che viene utilizzata per generare il rapporto di attestazione, recuperare i certificati richiesti e convalidare il rapporto di attestazione.

1. Connettiti alla tua istanza.
2. Verificate che i prerequisiti siano installati.

```
$ perl --version; cargo --version; git --version
```

3. Per installare l'utilità `snpguest` da snpguest repository, esegui i seguenti comandi.

```
$ git clone https://github.com/virtee/snpguest.git
$ cd snpguest
$ cargo build -r
$ cd target/release
```

Fase 2: Generare il rapporto di attestazione

Genera una richiesta per il rapporto di attestazione. L'`snpguest`utilità richiede il rapporto di attestazione dall'AMD Secure Processor tramite l'host e lo scrive in un file binario. L'esempio seguente crea una richiesta casuale nonce e memorizza il report in. `report.bin`

```
$ ./snpguest report report.bin request-file.txt --random
```

Fase 3: Recupera e convalida la catena di certificati VCEK

Il rapporto di attestazione è firmato dal VCEK, che è unico per il chip AMD sull'host dedicato. È necessario convalidare la catena di fiducia dal VCEK alla radice della fiducia di AMD.

1. Recupera il certificato VCEK dall'AMD Key Distribution Service (KDS). Il certificato è identificato dall'ID del chip e dalla versione TCB del rapporto di attestazione.

```
$ ./snpguest fetch vcek pem ./ ./report.bin --processor-model milan
```

2. Recupera i certificati principali AMD (AMD Root Key (ARK) e AMD SEV Key (ASK)) che costituiscono la catena di fiducia.

```
$ ./snpguest fetch ca PEM ./ milan --endorser vcek
```

3. Verifica la catena di certificati.

```
$ ./snpguest verify certs ./
```

Di seguito è riportato un output di esempio.

```
The AMD ARK was self-signed!
The AMD ASK was signed by the AMD ARK!
The VCEK was signed by the AMD ASK!
```

Facoltativo: per una maggiore trasparenza, puoi verificare in modo indipendente la catena scaricando i certificati direttamente da AMD e utilizzando`openssl`.

```
$ curl --proto '=https' --tlsv1.2 -sSf https://kdsintf.amd.com/vcek/v1/Milan/cert_chain
 -o ./cert_chain.pem
$ openssl verify --CAfile ./cert_chain.pem vcek.pem
```

Di seguito è riportato un output di esempio.

```
vcek.pem: OK
```

Fase 4: Convalida della firma del rapporto di attestazione

Verifica che il rapporto di attestazione sia stato firmato dal certificato VCEK. Ciò conferma che il rapporto è stato generato su hardware AMD originale e non è stato manomesso.

```
$ ./snpguest verify attestation ./ report.bin
```

Di seguito è riportato un output di esempio.

```
Reported TCB Boot Loader from certificate matches the attestation report.
Reported TCB TEE from certificate matches the attestation report.
Reported TCB SNP from certificate matches the attestation report.
Reported TCB Microcode from certificate matches the attestation report.
VEK signed the Attestation Report!
```

I campi relativi alla versione TCB (Trusted Computing Base) confermano che le versioni del firmware nel certificato corrispondono a quelle riportate nel rapporto di attestazione. L'ultima riga conferma che il VCEK ha firmato il rapporto.

Attestazione per casi di locazione condivisa

Le istanze di tenancy condivisa utilizzano una Versioned Loaded Endorsement Key (VLEK), rilasciata da AMD per. AWSÈ necessario convalidare la catena di fiducia dal certificato VLEK alla radice di fiducia di AMD.

Passaggio 1: crea l'utilità snpguest

In questo passaggio, si installa e si crea l'`snpguest`utilità, che viene utilizzata per generare il rapporto di attestazione, recuperare i certificati richiesti e convalidare il rapporto di attestazione.

1. Connettiti alla tua istanza.
2. Per installare l'utilità `snpguest` da snpguest repository, esegui i seguenti comandi.

```
$ git clone https://github.com/virtee/snpguest.git
$ cd snpguest
$ cargo build -r
$ cd target/release
```

Fase 2: Generazione del rapporto di attestazione

Genera una richiesta per il rapporto di attestazione. L'`snpguest`utilità richiede il rapporto di attestazione dall'host e lo scrive in un file binario. L'esempio seguente crea una richiesta casuale nonce e memorizza il report in. `report.bin`

```
$ ./snpguest report report.bin request-file.txt --random
```

Richiedi i certificati dalla memoria host e archiviali come file PEM.

```
$ ./snpguest certificates PEM ./
```

Fase 3: Recupera e convalida la catena di certificati VLEK

Il rapporto di attestazione è firmato dal VLEK, rilasciato da AMD per. AWSÈ necessario convalidare la catena di fiducia dal VLEK alla radice della fiducia di AMD.

1. Scarica i certificati root of trust VLEK dall'AMD Key Distribution Service ufficiale nella directory corrente.

```
$ sudo curl --proto '=https' --tlsv1.2 -sSf https://kdsintf.amd.com/vlek/v1/Milan/
cert_chain -o ./cert_chain.pem
```

2. Utilizza `openssl` per convalidare che il certificato VLEK sia firmato dai certificati root di fiducia di AMD.

   ```
   $ sudo openssl verify --CAfile ./cert_chain.pem vlek.pem
   ```

   Di seguito è riportato un output di esempio.

   ```
   vlek.pem: OK
   ```

Fase 4: Convalida della firma del rapporto di attestazione

Verifica che il rapporto di attestazione sia stato firmato dal certificato VLEK. Ciò conferma che il rapporto è stato generato su hardware AMD originale e non è stato manomesso.

```
$ ./snpguest verify attestation ./ report.bin
```

Di seguito è riportato un output di esempio.

```
Reported TCB Boot Loader from certificate matches the attestation report.
Reported TCB TEE from certificate matches the attestation report.
Reported TCB SNP from certificate matches the attestation report.
Reported TCB Microcode from certificate matches the attestation report.
VEK signed the Attestation Report!
```

Controllo degli stati del processore delle istanze Linux Amazon EC2

C-statescontrolla i livelli di sonno che un core può raggiungere quando è inattivo. C-states sono numerati a partire da C0 (lo stato più superficiale in cui il core è completamente attivo ed esegue le istruzioni) e vanno a C6 (lo stato di inattività più profondo in cui un core è spento).

P-statescontrollano le prestazioni desiderate (in frequenza della CPU) da un core. P-states sono numerati a partire da P0 (l'impostazione delle prestazioni più elevate in cui il core può utilizzare la tecnologia Intel Turbo Boost per aumentare la frequenza, se possibile) e vanno da P1 (l'impostazione P-state che richiede la frequenza di base massima) a P15 (la frequenza più bassa possibile).

> **Note**
>
> AWS I processori Graviton sono dotati di modalità di risparmio energetico integrate e funzionano a una frequenza fissa. Pertanto, non forniscono la capacità al sistema operativo di controllare C-states e P-states.

C-states e P-states

I seguenti tipi di istanza consentono a un sistema operativo di controllare C-states e P-states:

- Uso generico: `m4.10xlarge` | `m4.16xlarge`
- Calcolo ottimizzato: `c4.8xlarge`
- Ottimizzate per la memoria: `r4.8xlarge` | `r4.16xlarge` | `x1.16xlarge` | `x1.32xlarge` | `x1e.8xlarge` | `x1e.16xlarge` | `x1e.32xlarge`
- Ottimizzate per l'archiviazione: `d2.8xlarge` | `i3.8xlarge` | `i3.16xlarge` | `h1.8xlarge` | `h1.16xlarge`
- Elaborazione accelerata: `g3.16xlarge` | `p3.16xlarge`
- Bare metal: tutte le istanze bare metal con processori Intel e AMD

C-states solo

I seguenti tipi di istanza consentono a un sistema operativo di controllare C-states:

- Uso generale: `m5.12xlarge` `m5.24xlarge` | `m5d.12xlarge` | `m5d.24xlarge` | `m5n.12xlarge` | `m5n.24xlarge` | `m5dn.12xlarge` | `m5dn.24xlarge` `m5zn.6xlarge` | `m5zn.12xlarge` | `m6a.24xlarge` | `m6a.48xlarge` | `m6i.16xlarge` | `m6i.32xlarge` | `m6id.16xlarge` `m6id.32xlarge` | `m6idn.16xlarge` | `m6in.16xlarge` | `m6in.32xlarge` | `m7a.medium` | `m7a.large` | `m7a.xlarge` | `m7a.2xlarge` `m7a.4xlarge` | `m7a.8xlarge` | `m7a.12xlarge` | `m7a.16xlarge` | `m7a.24xlarge` | `m7a.32xlarge` | `m7a.48xlarge` | `m7i.large` `m7i.xlarge` | `m7i.2xlarge` | `m7i.4xlarge` | `m7i.8xlarge` | `m7i.12xlarge` | `m7i.16xlarge` | | `m7i.24xlarge` | `m7i.48xlarge` | `m8a.medium` | `m8a.large` | `m8a.xlarge` | | `m8a.2xlarge` | `m8a.4xlarge` | `m8a.8xlarge` | `m8a.12xlarge` | `m8a.16xlarge` | | `m8a.24xlarge` | `m8a.48xlarge` | `m8azn.medium` | `m8azn.large` | `m8azn.xlarge` | | `m8azn.3xlarge` | `m8azn.6xlarge` | `m8azn.12xlarge` | `m8azn.24xlarge` | | `m8i.large` | `m8i.xlarge` | `m8i.2xlarge` | `m8i.4xlarge` | `m8i.8xlarge` | | `m8i.12xlarge` |

m8i.16xlarge | m8i.24xlarge | m8i.32xlarge | m8i.48xlarge || m8i.96xlarge | m8id.large | m8id.xlarge | m8id.2xlarge | m8id.4xlarge || m8id.8xlarge | m8id.12xlarge | m8id.16xlarge | m8id.24xlarge || m8id.32xlarge | m8id.48xlarge | m8id.96xlarge | m8in.large | m8in.xlarge || m8in.2xlarge | m8in.4xlarge | m8in.8xlarge | m8in.12xlarge | m8in.16xlarge || m8in.24xlarge | m8in.32xlarge | m8in.48xlarge | m8in.96xlarge | m8idn.large || m8idn.xlarge | m8idn.2xlarge | m8idn.4xlarge | m8idn.8xlarge || m8idn.12xlarge | m8idn.16xlarge | m8idn.24xlarge | m8idn.32xlarge | m8idn.48xlarge || m8idn.96xlarge | m8ib.large | m8ib.xlarge | m8ib.2xlarge | m8ib.4xlarge || m8ib.8xlarge | m8ib.12xlarge | m8ib.16xlarge | m8ib.24xlarge | m8ib.32xlarge || m8ib.48xlarge | m8ib.96xlarge | m8idb.large| m8idb.xlarge | m8idb.2xlarge | m8idb.4xlarge || m8idb.8xlarge | m8idb.12xlarge | m8idb.16xlarge | m8idb.24xlarge | m8idb.32xlarge | m8idb.48xlarge | m8idb.96xlarge | m8ine.large || m8ine.xlarge | m8ine.2xlarge | m8ine.4xlarge | m8ine.8xlarge | m8ine.12xlarge

- Ottimizzato per il calcolo: c5.9xlarge c5.12xlarge | c5.18xlarge | c5.24xlarge | c5a.24xlarge | c5ad.24xlarge | c5d.9xlarge | c5d.12xlarge | c5d.18xlarge | c5d.24xlarge | c5n.9xlarge | c5n.18xlarge | c6a.24xlarge | c6a.32xlarge | c6a.48xlarge || c6i.16xlarge | c6i.32xlarge | c6id.24xlarge | c6id.32xlarge | c6in.32xlarge | c7a.medium | c7a.large | c7a.xlarge | c7a.2xlarge | c7a.4xlarge | c7a.8xlarge | c7a.12xlarge | c7a.16xlarge || c7a.24xlarge | c7a.32xlarge | c7a.48xlarge | c7i.large | c7i.xlarge | c7i.2xlarge | c7i.4xlarge c7i.8xlarge| c7i.12xlarge || c7i.16xlarge | c7i.24xlarge | c7i.48xlarge | c8a.medium || c8a.large | c8a.xlarge | c8a.2xlarge || c8a.4xlarge | c8a.8xlarge | c8a.12xlarge | c8a.16xlarge || c8a.24xlarge | c8a.48xlarge | c8i.large | c8i.xlarge || c8i.2xlarge | c8i.4xlarge | c8i.8xlarge || c8i.12xlarge | c8i.16xlarge | c8i.24xlarge | c8i.32xlarge || c8i.48xlarge | c8i.96xlarge | c8id.large | c8id.xlarge || c8id.2xlarge | c8id.4xlarge | c8id.8xlarge || c8id.12xlarge | c8id.16xlarge | c8id.24xlarge | c8id.32xlarge || c8id.48xlarge | c8id.96xlarge | c8in.large c8in.xlarge| c8in.2xlarge | c8in.4xlarge || c8in.8xlarge | c8in.12xlarge | c8in.16xlarge | c8in.24xlarge | c8in.32xlarge | c8in.48xlarge || c8in.96xlarge | c8ib.large | c8ib.xlarge | c8ib.2xlarge | c8ib.4xlarge | c8ib.8xlarge || c8ib.12xlarge | c8ib.16xlarge | c8ib.24xlarge | c8ib.32xlarge | c8ib.48xlarge | c8ib.96xlarge | c8in.large || c8in.xlarge | c8in.2xlarge | c8in.4xlarge | c8in.8xlarge | c8in.12xlarge | x8i.large || x8i.xlarge | x8i.2xlarge | x8i.4xlarge | x8i.8xlarge | x8i.12xlarge | x8i.16xlarge || x8i.24xlarge | x8i.32xlarge | x8i.48xlarge | x8i.48xlarge| x8i.96xlarge

- Memoria ottimizzata: r5.12xlarge r5.24xlarge r5b.12xlarge | r5d.12xlarge | r5d.24xlarge | r5n.12xlarge r5n.24xlarge | r5dn.12xlarge | r5dn.24xlarge | r6a.24xlarge | r6a.48xlarge | r6i.16xlarge | r6i.32xlarge | r6id.16xlarge | r6id.32xlarge | r6in.16xlarge | r6in.32xlarge | r7a.medium | r7a.large | r7a.xlarge | r7a.2xlarge | r7a.4xlarge | r7a.8xlarge | r7a.12xlarge | r7a.16xlarge r7a.24xlarge | r7a.32xlarge | r7a.48xlarge | r7i.large | r7i.xlarge | r7i.2xlarge | r7i.4xlarge | r7i.8xlarge | r7i.12xlarge | r7i.16xlarge | r7i.24xlarge | r7i.48xlarge || r7iz.large | r7iz.xlarge | r7iz.2xlarge | r7iz.4xlarge | r7iz.8xlarge || r7iz.12xlarge | r7iz.16xlarge | r7iz.32xlarge | r8a.medium | r8a.large || r8a.xlarge | r8a.2xlarge | r8a.4xlarge | r8a.8xlarge | r8a.12xlarge || r8a.16xlarge | r8a.24xlarge | r8a.48xlarge | r8i.large || r8i.xlarge | r8i.2xlarge | r8i.4xlarge | r8i.8xlarge | r8i.12xlarge || r8i.16xlarge | r8i.24xlarge | r8i.32xlarge | r8i.48xlarge | r8i.96xlarge || r8id.large | r8id.xlarge | r8id.2xlarge | r8id.4xlarge | r8id.8xlarge || r8id.12xlarge | r8id.16xlarge | r8id.24xlarge | r8id.32xlarge || r8id.48xlarge | r8id.96xlarge | r8in.large | r8in.xlarge | r8in.2xlarge || r8in.4xlarge | r8in.8xlarge | r8in.12xlarge | r8in.16xlarge | r8in.24xlarge || r8in.32xlarge | r8in.48xlarge | r8in.96xlarge | r8idn.large | r8idn.xlarge || r8idn.2xlarge | r8idn.4xlarge | r8idn.8xlarge | r8idn.12xlarge || r8idn.16xlarge | r8idn.24xlarge | r8idn.32xlarge | r8idn.48xlarge | r8idn.96xlarge || r8ib.large | r8ib.xlarge | r8ib.2xlarge | r8ib.4xlarge | r8ib.8xlarge || r8ib.12xlarge | r8ib.16xlarge | r8ib.24xlarge | r8ib.32xlarge | r8ib.48xlarge || r8ib.96xlarge | r8idb.large | r8idb.xlarge| r8idb.2xlarge | r8idb.4xlarge | r8idb.8xlarge || r8idb.12xlarge | r8idb.16xlarge | r8idb.24xlarge | r8idb.32xlarge | r8idb.48xlarge | r8idb.96xlarge || u-3tb1.56xlarge | u-6tb1.56xlarge | u-6tb1.112xlarge | u-9tb1.112xlarge | u-12tb1.112xlarge | u-18tb1.112xlarge | u-24tb1.112xlarge | u7i-6tb.112xlarge || u7i-8tb.112xlarge | u7i-12tb.224xlarge | u7in-16tb.224xlarge | u7in-24tb.224xlarge | u7in-32tb.224xlarge | u7inh-32tb.480xlarge || x2idn.32xlarge | x2iedn.16xlarge | x2iedn.32xlarge | x2iezn.12xlarge | x8aedz.large | x8aedz.xlarge | x8aedz.3xlarge | x8aedz.6xlarge || x8aedz.12xlarge | x8aedz.24xlarge | z1d.6xlarge | z1d.12xlarge
- Archiviazione ottimizzata: d3en.12xlarge dl1.24xlarge i3en.12xlarge i3en.24xlarge | i4i.16xlarge | i7i.large | i7i.xlarge | i7i.2xlarge | i7i.4xlarge | i7i.8xlarge | i7i.12xlarge | i7i.16xlarge | i7i.24xlarge | i7i.48xlarge | i7ie.large |

`i7ie.xlarge` | `i7ie.2xlarge` | | `i7ie.3xlarge` | `i7ie.6xlarge` | `i7ie.12xlarge` | `i7ie.18xlarge` | `i7ie.24xlarge` | `i7ie.48xlarge` | `r5b.12xlarge` | `r5b.24xlarge`

- Calcolo accelerato: `dl1.24xlarge` `f2.6xlarge` | `f2.12xlarge` | `f2.48xlarge` | `g5.24xlarge` | `g5.48xlarge` | `g6.24xlarge` | `g6.48xlarge` | `g6e.12xlarge` | `g6e.24xlarge` | `g6e.48xlarge` | `g7e.2xlarge` | `g7e.4xlarge` | `g7e.8xlarge` | `g7e.12xlarge` | `g7e.24xlarge` | `g7e.48xlarge` | `g7.2xlarge` | `g7.4xlarge` | `g7.8xlarge` | `g7.12xlarge` | `g7.24xlarge` | `g7.48xlarge` | `inf1.24xlarge` | `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `p5.48xlarge` | `p5e.48xlarge` | `p5en.48xlarge` | `p6-b200.48xlarge` | `p6-b300.48xlarge` | `trn1.32xlarge` | `trn2.3xlarge` | `trn2.48xlarge` `trn2a.3xlarge`| `trn2a.48xlarge` | `trn2n.3xlarge` | `trn2n.48xlarge` | `trn2p.48xlarge` | `trn2u.48xlarge` `vt1.24xlarge`
- High-performance informatica: `hpc7a.12xlarge` | `hpc7a.24xlarge` | `hpc7a.48xlarge` | `hpc7a.96xlarge` | `hpc8a.96xlarge`

Potresti voler modificare P-state le impostazioni C-state o per aumentare la coerenza delle prestazioni del processore, ridurre la latenza o ottimizzare l'istanza per un carico di lavoro specifico. Le P-state impostazioni predefinite offrono C-state le massime prestazioni, ottimali per la maggior parte dei carichi di lavoro. Tuttavia, se la tua applicazione può trarre vantaggio da una latenza ridotta a scapito di frequenze single o dual-core più elevate o da prestazioni costanti a frequenze più basse rispetto alle frequenze Turbo Boost più elevate, valuta la possibilità di sperimentare con le P-state impostazioni C-state or disponibili per queste istanze.

Per informazioni sulle diverse configurazioni dei processori e su come monitorare gli effetti della configurazione per Amazon Linux, consulta Controllo dello stato del processore per le istanze EC2 Amazon Linux nella Guida per l'utente Amazon Linux 2. Queste procedure sono state scritte e applicate per Amazon Linux; tuttavia, potrebbero essere utilizzate anche per altre distribuzioni Linux kernel di Linux di 3.9 o versioni successive. Per ulteriori informazioni su altre distribuzioni Linux e sul controllo degli stati del processore, consultare la documentazione specifica del sistema.

Istanze gestite di Amazon EC2

Un'istanza gestita di Amazon EC2 è un'istanza EC2 fornita e gestita da un fornitore di servizi designato. Le istanze gestite offrono un modo semplificato per eseguire carichi di lavoro di calcolo su Amazon EC2, consentendoti di delegare il controllo operativo dell'istanza a un fornitore di servizi.

Il controllo delegato è l'unica modifica introdotta per le istanze gestite. Le specifiche tecniche e la fatturazione rimangono le stesse delle istanze EC2 non gestite. Poiché le istanze gestite

consentono di delegare il controllo al fornitore di servizi, è possibile trarre vantaggio dall'esperienza operativa e dalle best practice del fornitore di servizi. Quando un'istanza viene gestita, il provider di servizi è responsabile di attività quali il provisioning dell'istanza, la configurazione del software, il dimensionamento della capacità e la gestione degli errori, delle sostituzioni e delle terminazioni delle istanze.

Non puoi modificare direttamente le impostazioni di un'istanza gestita o terminarla. Il servizio e le operazioni specifiche sono determinati dall'accordo tra l'utente e il fornitore di servizi. Tuttavia, puoi aggiungere, modificare o rimuovere tag dalle tue istanze gestite, consentendoti di classificarle all'interno del tuo ambiente. AWS

I seguenti AWS servizi offrono istanze gestite:

- Modalità automatica EKS
- Istanze gestite da Amazon ECS
- WorkSpaces Istanze gestite principali
- Istanze gestite da Lambda
- Avvio rapido di Amazon EC2
- Istanze di runtime Bedrock AgentCore

Indice

- Fatturazione per le istanze gestite
- Identificazione di istanze gestite
- Impostazioni di visibilità delle risorse gestite
- Iniziare a utilizzare le istanze gestite

Fatturazione per le istanze gestite

Un'istanza gestita Amazon EC2 comporta lo stesso costo di base di un'istanza Amazon EC2 non gestita, più una tariffa separata per il fornitore di servizi. Questo costo aggiuntivo viene addebitato dal fornitore di servizi che gestisce l'istanza e viene fatturato separatamente. Copre il costo dei servizi forniti per il funzionamento e la manutenzione dell'istanza gestita.

Tutte le opzioni di acquisto di Amazon EC2 sono disponibili per le istanze gestite, incluse istanze, On-Demand istanze riservate, istanze Spot e piani di risparmio. Acquistando le risorse di calcolo direttamente da EC2 e poi inviandole al fornitore di servizi, puoi beneficiare di tutte le istanze

riservate o i Savings Plans esistenti applicati al tuo account, assicurandoti di utilizzare la capacità di elaborazione più conveniente disponibile.

Ad esempio, quando utilizzi la modalità automatica di Amazon EKS, paghi la tariffa standard delle istanze EC2 per le istanze sottostanti, più un costo aggiuntivo da parte di Amazon EKS per la gestione delle istanze per tuo conto. Se poi decidi di iscriverti a un Savings Plans, la tariffa delle istanze EC2 viene dedotta dal Savings Plans, mentre il costo aggiuntivo di Amazon EKS rimane invariato.

Identificazione di istanze gestite

Le istanze gestite sono identificate da un valore true nel campo Gestite. Il fornitore di servizi è identificato nel campo Operatore (nella console) o nel campo `Principal` (nella CLI).

Utilizza le procedure seguenti per identificare le istanze gestite.

Console

Per identificare un'istanza gestita

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza che vuoi controllare.
4. Nella scheda Dettagli (se hai selezionato la casella di spunta) o nell'area di riepilogo (se hai selezionato l'ID dell'istanza), trova il campo Gestite.
   - Il valore true indica un'istanza gestita.
   - Il valore false indica un'istanza non gestita.
5. Se Gestite è impostato su true, nel campo Operatore viene visualizzato un valore che identifica il fornitore di servizi responsabile della gestione dell'istanza. Ad esempio, un valore di eks.amazonaws.com identifica Amazon EKS come fornitore di servizi.

AWS CLI

Per identificare un'istanza gestita

Utilizza il comando describe-instances e specifica l'ID istanza.

```
aws ec2 describe-instances \
```

```
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].Operator
```

Di seguito è riportato un output di esempio. Se `Managed` è `true`, l'istanza è un'istanza gestita e un `Principal` è incluso. Il principale è il fornitore di servizi che gestisce l'istanza. Ad esempio, un valore di `eks.amazonaws.com` identifica Amazon EKS come fornitore di servizi.

```
[
    {
        "Managed": true,
        "Principal": "eks.amazonaws.com"
    }
]
```

Per individuare le istanze gestite

Utilizza il comando describe-instances e indica il filtro `operator.managed` con un valore di `true`. L'opzione `--query` visualizza solo gli ID delle istanze gestite.

```
aws ec2 describe-instances \
    --filters "Name=operator.managed,Values=true" \
    --query Reservations[*].Instances[].InstanceId
```

PowerShell

Per identificare un'istanza gestita

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.Operator
```

Di seguito è riportato un output di esempio.

```
Managed Principal
------- ---------
True    eks.amazonaws.com
```

Per individuare le istanze gestite

Utilizza il cmdlet Get-EC2Instance. L'esempio visualizza solo gli ID delle istanze gestite.

```
(Get-EC2Instance -Filter @{Name="operator.managed";
 Values="true"}).Instances.InstanceId
```

Impostazioni di visibilità delle risorse gestite

Puoi controllare se le risorse che AWS i servizi forniscono per tuo conto vengono visualizzate nelle visualizzazioni della console Amazon EC2 e nelle operazioni degli elenchi di API.

Cos'è la visibilità gestita delle risorse?

AWS servizi come Amazon EKS, Amazon ECS, WorkSpaces Core, AWS Lambda e Amazon Bedrock AgentCore forniscono e gestiscono le istanze Amazon EC2 direttamente all'interno del tuo account. Questi servizi si assumono la responsabilità della scalabilità, delle patch del sistema operativo, degli aggiornamenti di sicurezza e della gestione del ciclo di vita. Le istanze Amazon EC2 risultanti, i modelli di lancio di Amazon EC2, i volumi Amazon EBS, le istantanee e le interfacce di rete (ENI) vengono visualizzati insieme alle risorse gestite dai clienti nella console e nelle API di Amazon EC2. Le impostazioni di visibilità delle risorse gestite ti consentono di controllare se queste risorse gestite sono presenti nelle tue visualizzazioni delle risorse.

Tipi di risorse interessati

Tipo di risorsa	Servizi che forniscono queste risorse	Description
Istanze Amazon EC2	Nodi di lavoro Amazon EKS, istanze container Amazon ECS, ambienti di esecuzione AWS Lambda, Amazon WorkSpaces Core, Amazon Bedrock AgentCore	Tipo di risorsa principale interessato dalle impostazioni di visibilità
Modelli di avvio Amazon EC2	Amazon EKS, Amazon ECS, Amazon WorkSpaces Core, Amazon Bedrock AgentCore	Modelli di avvio creati da servizi gestiti
Volumi Amazon EBS	Amazon EKS, Amazon ECS, Amazon WorkSpaces Core, Amazon Bedrock AgentCore, Amazon EC2 Fast Launch	Volumi collegati alle istanze gestite

Tipo di risorsa	Servizi che forniscono queste risorse	Description
Amazon EBS snapshots	Avvio rapido di Amazon EC2	Istantanee gestite da Amazon EC2 Fast Launch
Interfacce di rete (ENI)	Controlli dello stato delle applicazioni Amazon EKS, Amazon ECS, AWS Lambda, Amazon WorkSpaces Core, Amazon Bedrock AgentCore, Amazon EC2	Interfacce di rete predisposte per carichi di lavoro gestiti

> **Note**
>
> Per impostazione predefinita, Amazon EC2 nasconde le risorse gestite per gli account che non disponevano di risorse gestite prima che le impostazioni di visibilità diventassero disponibili. Per gli account che disponevano già di risorse gestite, Amazon EC2 imposta l'impostazione di visibilità su Visible per preservare i flussi di lavoro esistenti. L'impostazione di visibilità si applica a tutte le risorse gestite in una regione, indipendentemente da quando sono state create. Puoi modificare le impostazioni di visibilità in qualsiasi momento.

Perché configurare le impostazioni di visibilità

La configurazione delle impostazioni di visibilità ti consente di personalizzare la visualizzazione delle risorse gestite nei tuoi strumenti operativi. Casi di utilizzo comune comprendono:

- Semplifica la governance riducendo il numero di risorse nelle dashboard di conformità alle sole risorse gestite dal cliente.
- Riduci il rumore negli strumenti di osservabilità che aggregano le metriche di Amazon EC2 su tutte le istanze di un account.
- Previeni i falsi positivi negli scanner CSPM (Cloud Security Posture Management) (ad esempio Qualys) che segnalano le risorse gestite come configurazioni errate dei clienti.
- Con le istanze gestite, AWS è responsabile della configurazione, dell'applicazione delle patch e dello stato delle istanze Amazon EC2. Controllando la visibilità, puoi articolare meglio il modello di responsabilità condivisa con gli utenti finali.

> **Note**
>
> Le impostazioni di visibilità controllano la visualizzazione delle risorse nelle visualizzazioni AWS della console e nelle operazioni degli elenchi di API. Non influiscono sulla fatturazione, sul funzionamento delle risorse o sulle autorizzazioni di accesso effettive. Le risorse nascoste rimangono completamente operative e fatturabili.

Configura la visibilità delle risorse gestite

Puoi configurare la visibilità delle risorse gestite utilizzando la console Amazon EC2 o il AWS CLI.

Console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione seleziona Pannello di controllo.
3. Nella scheda Attributi dell'account, in Impostazioni, scegli Risorse gestite.
4. Scegli Modifica.
5. In Visibilità predefinita, scegli una delle seguenti opzioni:
   - Nascosto (impostazione predefinita): nasconde tutte le risorse gestite.
   - Visibile: mostra tutte le risorse gestite.
6. Scegli Modifica visibilità.

AWS CLI

Ottieni le impostazioni di visibilità correnti

Usa il comando get-managed-resource-visibility per recuperare la configurazione di visibilità corrente:

```
aws ec2 get-managed-resource-visibility
```

Risposta di esempio:

```
{
    "visibility": {
        "defaultVisibility": "hidden"
```

```
    }
}
```

Nascondi tutte le risorse gestite

Usa il comando modify-managed-resource-visibility per nascondere tutte le risorse gestite indipendentemente dall'operatore:

```
aws ec2 modify-managed-resource-visibility \
    --default-visibility "hidden"
```

Scopri le risorse gestite nascoste

Quando disattivi la visibilità, puoi comunque accedere alle risorse gestite. I seguenti metodi li rendono disponibili su richiesta:

1. Service-specific console: accedi alla rispettiva console di AWS servizio (ad esempio, la console Amazon EKS) per visualizzare le istanze fornite per quel servizio. La console di servizio fornisce dettagli completi su tutte le risorse gestite dal servizio nel tuo account.
2. Interrogazioni API dirette: utilizza l'`describe-instances`API con un `instance-id` parametro specifico. Le query dirette con ID di istanza noti restituiscono risultati indipendentemente dalle impostazioni di visibilità. Le impostazioni di visibilità influiscono solo sulle operazioni di elenco e filtro. Puoi anche utilizzarlo `describe-instances` con il `include-managed-resources` parametro per scoprire le istanze gestite.

> **Note**
>
> Lo stesso comportamento Direct-Query-by-ID si applica a tutti i tipi di risorse interessati. È possibile utilizzare `describe-volumes` e `describe-network-interfaces` con ID di risorsa specifici per accedere a risorse gestite nascoste di questi tipi. `describe-launch-templates`

Considerazioni sulla fatturazione

Le impostazioni di visibilità delle risorse gestite non hanno alcun effetto sulla fatturazione. Le istanze gestite nascoste continuano a comparire nei dati di fatturazione perché sono risorse in

esecuzione all'interno del tuo account, assegnate per tuo conto e rimangono completamente fatturabili indipendentemente dalla configurazione della visibilità.

Le risorse nascoste rimangono visibili in:

- AWS fatture
- AWS Rapporti sui costi e sull'utilizzo

> **Important**
>
> Le istanze gestite vengono eseguite nel tuo account e consumano risorse di calcolo. Nasconderle dalle visualizzazioni della console non riduce i costi. Consulta la documentazione di fatturazione specifica del servizio (ad esempio, i prezzi di Amazon EKS, i prezzi di Amazon ECS) per i dettagli sui costi delle istanze gestite.

Limitazioni

- Le impostazioni di visibilità si applicano all'intero account e influiscono in modo uniforme su tutti i principali IAM.
- Non è possibile mostrare o nascondere selettivamente le risorse gestite in base al tipo di risorsa o al servizio che le ha create. Ad esempio, non puoi scegliere di mostrare le istanze gestite create da Amazon EKS nascondendo quelle create da Lambda, Amazon ECS o Amazon. WorkSpaces

Iniziare a utilizzare le istanze gestite

Per iniziare con le istanze gestite, consulta la documentazione del tuo fornitore di servizi preferito:

- Automatizza l'infrastruttura dei cluster con EKS Auto Mode nella Amazon EKS User Guide
- Istanze gestite da Amazon ECS nella Amazon ECS Developer Guide
- Implementa le istanze gestite nella Core Planning Guide WorkSpaces
- Istanze gestite da Lambda nella Lambda Developer Guide
- Amazon EC2 Fast Launch in questa guida
- Istanze AgentCore di runtime Bedrock nella Amazon Bedrock Developer Guide AgentCore

Usa la virtualizzazione annidata per eseguire hypervisor nelle istanze Amazon EC2

La virtualizzazione annidata consente di eseguire hypervisor come Hyper-V KVM all'interno di istanze virtuali di Amazon EC2. Le istanze EC2 virtuali sono istanze non bare metal. Questa funzionalità estende la flessibilità della virtualizzazione aggiungendo il supporto per la virtualizzazione a livello di processore alle istanze EC2 virtuali, consentendo a un hypervisor in esecuzione nell'istanza di creare e gestire macchine virtuali.

La virtualizzazione annidata può essere utile quando si utilizzano strumenti di sviluppo come Docker Desktop, Windows Subsystem for Linux 2 (WSL2), emulatori Android Studio o QEMU nel flusso di lavoro di sviluppo, poiché consente di scegliere tra un'ampia gamma di tipi di istanze virtuali Amazon EC2 standard che soddisfano i requisiti specifici di prestazioni e prezzo.

L'utilizzo della virtualizzazione annidata non comporta costi aggiuntivi.

Indice

- Come funziona
- Considerazioni
- Avvia una nuova istanza con la virtualizzazione annidata abilitata
- Configurare un'istanza esistente per utilizzare la virtualizzazione annidata
- Trova i tipi di istanza che supportano la virtualizzazione annidata

Come funziona

Le istanze EC2 virtuali vengono eseguite su un host fisico dotato dell'hypervisor Nitro. Per supportare la virtualizzazione annidata, il sistema Nitro passa le estensioni del processore, come Intel VT-x, alle istanze per facilitare l'esecuzione di macchine virtuali annidate. L'architettura di virtualizzazione annidata è composta da tre livelli: l' AWS infrastruttura fisica e l'hypervisor Nitro (L0), l'istanza EC2 che esegue un hypervisor (L1) e una o più macchine virtuali create all'interno di tale istanza (L2).

Considerazioni

Prima di iniziare a utilizzare la virtualizzazione annidata, considera quanto segue:

- Tipi di istanza supportati: la virtualizzazione annidata è attualmente supportata sui seguenti tipi di istanza:

  - Uso generale: M7i | | M8i | M8id M7i-flex | M8i-flex
  - Ottimizzato per il calcolo: C7i | | C8i | C8id | C7i-flex C8i-flex
  - Memoria ottimizzata: R7i | R7iZ | R8i | R8id | | X8i R8i-flex
  - Archiviazione ottimizzata: I7i | I7iE
- Hypervisor supportati: attualmente, KVM e sono gli hypervisor L1 supportati. Hyper-V
- Istanze Windows: quando la virtualizzazione annidata è abilitata su un'istanza Windows:
  - Credential Guard : la modalità Virtual Secure (VSM) viene disattivata automaticamente.
  - Ibernazione: l'ibernazione e la ripresa delle istanze non sono supportate.
  - Limite CPU: non supportato su istanze Windows con più di 192 CPU, ad esempio. `m8i.96xl`
- Responsabilità di sicurezza: quando si utilizza la virtualizzazione annidata su istanze EC2, AWS è responsabile della «sicurezza del cloud», della protezione dell'infrastruttura sottostante e del mantenimento dei forti confini di isolamento tra le istanze EC2 forniti dal sistema Nitro. AWS I clienti sono responsabili della «sicurezza nel cloud», che include la protezione del sistema operativo, dell'hypervisor, delle macchine virtuali annidate, dei sistemi operativi guest, delle applicazioni e dei dati all'interno delle istanze EC2.
- Prestazioni: AWS consiglia ai clienti che desiderano eseguire carichi di lavoro che richiedono l'accesso alle estensioni di virtualizzazione dell'hardware e che sono sensibili alle prestazioni o hanno requisiti di latenza rigorosi, di valutare le istanze bare metal.

Avvia una nuova istanza con la virtualizzazione annidata abilitata

Quando avvii una nuova istanza, puoi attivare la virtualizzazione annidata per eseguire hypervisor e macchine virtuali su di essa.

Console

Per abilitare la virtualizzazione annidata durante l'avvio dell'istanza

1. Segui la procedura the section called “Avvio tramite la procedura guidata di avvio dell'istanza” e configura l'istanza in base alle esigenze.
2. Assicurati che sia selezionato un tipo di istanza supportato.
3. Espandi i dettagli avanzati e, per la virtualizzazione Nested, scegli Abilita.
4. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza).

AWS CLI

Per avviare un'istanza con la virtualizzazione annidata abilitata

Utilizzare il comando run-instances.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r8i.4xlarge \
    --cpu-options "NestedVirtualization=enabled" \
    --key-name my-key-pair
```

PowerShell

Per avviare un'istanza con la virtualizzazione annidata abilitata

Utilizza il comando New-EC2Instance.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType r8i.4xlarge `
    -CpuOption @{NestedVirtualization='enabled'} `
    -KeyName my-key-pair
```

Configurare un'istanza esistente per utilizzare la virtualizzazione annidata

Puoi attivare la virtualizzazione annidata su un'istanza Amazon EC2 esistente.

Prerequisiti

- L'istanza deve trovarsi in uno stato. `stopped`
- Il tipo di istanza deve supportare la virtualizzazione annidata.

Console

Per abilitare la virtualizzazione annidata su un'istanza esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).

3. Seleziona l'istanza che desideri modificare dalla tabella delle istanze.
4. Scegliete Azioni, Impostazioni dell'istanza, Modifica le opzioni della CPU.
5. Nella pagina Modifica opzioni CPU, per la virtualizzazione Nested, scegli una delle seguenti opzioni:
   - Abilita: attiva la virtualizzazione annidata per l'istanza
   - Disabilita: disattiva la virtualizzazione annidata per l'istanza
6. Rivedi le modifiche, quindi scegli Modifica per applicare le nuove opzioni della CPU.

AWS CLI

Per abilitare la virtualizzazione annidata su un'istanza esistente

Arresta prima l'istanza, quindi usa il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-instance-cpu-options.html modify-instance-cpu-options.

```
aws ec2 modify-instance-cpu-options \
    --instance-id i-1234567890abcdef0 \
    --core-count 4 \
    --threads-per-core 2 \
    --nested-virtualization enabled
```

PowerShell

Per abilitare la virtualizzazione annidata su un'istanza esistente

Prima interrompi l'istanza, quindi usa il Edit-EC2InstanceCpuOption comando.

```
Edit-EC2InstanceCpuOption `
    -InstanceId i-1234567890abcdef0 `
    -CoreCount 4 `
    -ThreadsPerCore 2 `
    -NestedVirtualization enabled
```

Trova i tipi di istanza che supportano la virtualizzazione annidata

Puoi scoprire quali tipi di istanze Amazon EC2 supportano la virtualizzazione annidata. Puoi interrogare un intero tipo di istanza Regione AWS o controllare un tipo specifico.

AWS CLI

Per elencare tutte le famiglie di istanze che supportano la virtualizzazione annidata in una regione

Usa il comando describe-instance-types con il filtro impostato sul valore di: `processor-info.supported-features` `nested-virtualization`

```
aws ec2 describe-instance-types --region us-east-1 \
  --filters "Name=processor-info.supported-features,Values=nested-virtualization" \
  --query "InstanceTypes[].InstanceType" --output text \
  | tr '\t' '\n' | cut -d. -f1 | sort -u
```

Per verificare se un tipo di istanza specifico supporta la virtualizzazione annidata

Usa il comando describe-instance-types e interroga il campo del tipo di istanza specificato: `ProcessorInfo.SupportedFeatures`

```
aws ec2 describe-instance-types \
  --instance-types m8i.2xlarge \
  --query "InstanceTypes[].ProcessorInfo.SupportedFeatures"
```

Se il tipo di istanza supporta la virtualizzazione annidata, l'output include. `nested-virtualization` In caso contrario, il comando restituisce un array vuoto `()[]`.

PowerShell

Per elencare tutte le famiglie di istanze che supportano la virtualizzazione annidata in una regione

Usa il Get-EC2InstanceType comando con il `processor-info.supported-features` filtro impostato sul valore di: `nested-virtualization`

```
Get-EC2InstanceType -Region us-east-1 -Filter @{ Name='processor-info.supported-
features'; Values='nested-virtualization' } |
  ForEach-Object { ($_.InstanceType -split '\.')[0] } |
  Sort-Object -Unique
```

Per verificare se un tipo di istanza specifico supporta la virtualizzazione annidata

Usa il Get-EC2InstanceType comando e interroga la `ProcessorInfo.SupportedFeatures` proprietà del tipo di istanza specificato:

```
(Get-EC2InstanceType -InstanceType m8i.2xlarge).ProcessorInfo.SupportedFeatures
```

Se il tipo di istanza supporta la virtualizzazione annidata, l'output include. `nested-virtualization` In caso contrario, il comando non restituisce alcun output.

Opzioni di fatturazione e acquisto di Amazon EC2

Per ottimizzare i costi per Amazon EC2, puoi utilizzare le seguenti opzioni:

- Istanze on demand: paga al secondo per le istanze che avvii.
- Savings Plans: riduci i costi di Amazon EC2 sottoscrivendo un impegno per una quantità costante di utilizzo, in USD all'ora, per un periodo di uno o tre anni.
- Istanze riservate: puoi ridurre i costi di Amazon EC2 sottoscrivendo un impegno di utilizzo di una configurazione di istanza specifica, incluso il tipo di istanza e la Regione, per un periodo di uno o tre anni.
- Istanze spot: richiedi istanze EC2 inutilizzate con la possibilità di ridurre i costi di Amazon EC2 in modo significativo.
- Host dedicati: puoi usufruire di un host fisico a pagamento completamente dedicato all'esecuzione delle istanze, riducendo i costi relativi alle licenze software per socket, per core o per VM esistenti.
- Istanze dedicate: paga all'ora per le istanze eseguite su un hardware a tenant singolo.
- Prenotazioni di capacità - Prenota la capacità per le istanze EC2 in una determinata zona di disponibilità.

Se non puoi impegnarti per una configurazione specifica dell'istanza, ma puoi impegnarti per un importo di utilizzo, acquista Savings Plans per ridurre i costi delle istanze on demand. Se richiedi una prenotazione di capacità, puoi acquistare Istanze riservate o Prenotazioni di capacità per una zona di disponibilità specifica. I blocchi di capacità possono essere utilizzati per prenotare un cluster di istanze GPU. Le istanze spot sono una scelta conveniente se si può essere flessibili su quando vengono eseguite le applicazioni e se queste possono essere interrotte. Gli host dedicati o le istanze dedicate possono aiutarti a rispettare i requisiti di conformità e a ridurre i costi utilizzando le tue licenze software esistenti collegate al server.

Per ulteriori informazioni, consulta Prezzi di Amazon EC2 e Istanze gestite di Amazon EC2.

Acquisto di istanze On-Demand per Amazon EC2

Con Istanze on demand, sono previsti costi per la capacità di calcolo al secondo senza impegni a lungo termine. Hai il controllo completo del suo ciclo di vita: puoi decidere quando avviarla, arrestarla, ibernarla, avviarla, riavviarla o terminarla.

L'acquisto di Istanze on demand non richiede un impegno a lungo termine. Paghi solo per i secondi durante i quali le istanze on demand si trovano nello stato `running`, con un minimo di 60 secondi. Il prezzo al secondo per un'istanza on demand in esecuzione è fisso ed è indicato nella pagina dei prezzi di Amazon, EC2 prezzi on demand, pagina dei prezzi di .

Consigliamo di utilizzare Istanze on demand per le applicazioni con carichi di lavoro irregolari o a breve termine che non possono essere interrotti.

Per risparmi significativi rispetto alle istanze on demand, utilizza AWS Savings Plans, Spot Instances o Panoramica delle istanze riservate per Amazon EC2.

Indice

- Quote di istanze on demand
  - Monitoraggio delle quote e dell'utilizzo delle istanze on demand
  - Richiesta di un aumento della quota
- Eseguire una query sui prezzi delle Istanze on demand

Quote di istanze on demand

Sono previste quote per il numero di istanze On-Demand in esecuzione per regione. Account AWS Le quote delle istanze On-Demand sono gestite in termini di numero di unità di elaborazione centrale virtuali (vCPUs) utilizzate dalle istanze On-Demand in esecuzione, indipendentemente dal tipo di istanza. Ogni tipo di quota specifica il numero massimo di v CPUs per una o più famiglie di istanze.

Il tuo account include le seguenti quote per le istanze on demand. Le istanze in sospeso, terminate, interrotte e ibernate non vengono conteggiate ai fini delle quote delle istanze on demand. Le prenotazioni della capacità contano per le quote delle istanze on demand, anche se inutilizzate.

Name	Predefinita	Adattabile
Esecuzione di istanze DL on demand	0	Sì

Name	Predefinita	Adattabile
Esecuzione di istanze F on demand	0	Sì
Esecuzione di tutte le istanze G e VT on demand	0	Sì
Istanze HPC on demand in esecuzione	0	Sì
Esecuzione delle istanze a memoria elevata on demand	0	Sì
Esecuzione di istanze Inf on demand	0	Sì
Esecuzione di istanze P on demand	0	Sì
Esecuzione di istanze on demand standard (A, C, D, H, I, M, R, T, Z)	5	Sì
Istanze Trn on demand in esecuzione	0	Sì
Esecuzione di istanze X on demand	0	Sì

Per informazioni sulle diverse famiglie, generazioni e dimensioni di istanze, consulta l'Amazon EC2 Instance Types Guide.

Puoi avviare qualsiasi combinazione di tipi di istanza che soddisfi le mutevoli esigenze delle tue applicazioni, purché il numero di v CPUs non superi la quota del tuo account. Ad esempio, con una quota di istanze Standard di 256 vCPUs, è possibile avviare 32 `m5.2xlarge` istanze (32 x 8 vCPUs) o 16 `c5.4xlarge` istanze (16 x 16 vCPUs). Per ulteriori informazioni, consulta Limiti delle istanze EC2 On-Demand.

Processi

- Monitoraggio delle quote e dell'utilizzo delle istanze on demand
- Richiesta di un aumento della quota

Monitoraggio delle quote e dell'utilizzo delle istanze on demand

Puoi visualizzare e gestire le quote delle istanze on demand utilizzando i seguenti metodi.

Visualizzazione delle quote correnti utilizzando la console Service Quotas

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Nella barra di navigazione, selezionare una regione.
3. Nel campo di filtro, inserisci **`On-Demand`**.
4. La colonna Valore della quota applicata mostra il numero massimo di v CPUs per ogni tipo di quota di istanza On-Demand per il tuo account.

Per visualizzare le quote correnti utilizzando la console AWS Trusted Advisor

Apri la pagina dei limiti del servizio nella AWS Trusted Advisor console.

Per configurare gli CloudWatch allarmi

Con l'integrazione di Amazon CloudWatch Metrics, puoi monitorare EC2 l'utilizzo rispetto alle tue quote. Puoi anche configurare gli allarmi per ricevere un avviso quando stai per raggiungere le quote. Per ulteriori informazioni, consulta Service Quotas e Amazon CloudWatch alarms nella Service Quotas User Guide.

Richiesta di un aumento della quota

Anche se Amazon aumenta EC2 automaticamente le quote delle istanze On-Demand in base all'utilizzo, puoi richiedere un aumento della quota se necessario. Ad esempio, se intendi avviare più istanze di quanto consentito dalla quota corrente, puoi richiedere un aumento della quota utilizzando la console Service Quotas, descritta nella pagina Service Quotas di Amazon EC2.

Eseguire una query sui prezzi delle Istanze on demand

Puoi utilizzare l'API Price List Service o l'API AWS Price List per richiedere i prezzi delle istanze On-Demand. Per ulteriori informazioni, consulta Utilizzo dell'API AWS Price List nella Guida per l'AWS Billing utente.

Panoramica delle istanze riservate per Amazon EC2

> **Important**
>
> Consigliamo i Savings Plans rispetto alle istanze riservate. I piani di risparmio sono il modo più semplice e flessibile per risparmiare sui costi di AWS elaborazione e offrire

prezzi più bassi (fino al 72% di sconto On-Demand sui prezzi), proprio come le istanze riservate. Tuttavia, i Savings Plans sono diversi dalle istanze riservate. Con le istanze riservate, ti impegni a utilizzare una configurazione specifica dell'istanza, mentre con i piani di risparmio hai la flessibilità di utilizzare le configurazioni di istanze che meglio soddisfano le tue esigenze. Per utilizzare i Savings Plans, ti impegni per una quantità di utilizzo costante, misurata in USD per ora. Per ulteriori informazioni, consulta la Guida per l'utente dei Savings Plans di AWS.

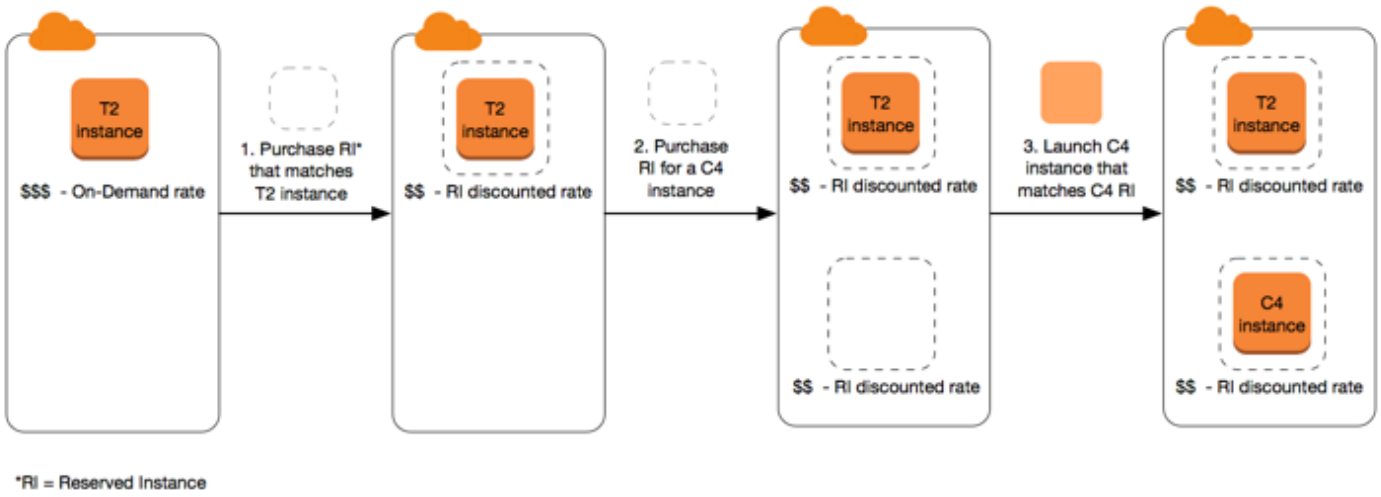
Le istanze riservate offrono risparmi significativi sui costi di Amazon EC2 rispetto ai prezzi delle istanze. On-Demand Le istanze riservate non sono istanze fisiche, ma piuttosto uno sconto di fatturazione applicato all'utilizzo delle On-Demand istanze nel tuo account. Queste On-Demand istanze devono corrispondere a determinati attributi, come il tipo di istanza e la regione, per beneficiare dello sconto sulla fatturazione.

Argomenti di istanze riservate

- Scenario di esempio delle istanze riservate
- Variabili chiave che determinano i prezzi di Istanza riservata
- Istanze riservate regionale e zonale (Ambito)
- Tipi di elementi di Istanze riservate (Classi di offerta)
- Applicazione degli sconti sulle istanze riservate
- Usa le tue Istanze riservate
- Come funziona la fatturazione con le istanze riservate
- Acquisto delle istanze riservate Amazon EC2
- Vendita di istanze riservate per Amazon EC2 nel Marketplace delle istanze riservate
- Modificare le Istanze riservate
- Scambiare le Istanze riservate modificabili
- Quote di istanze riservate

Scenario di esempio delle istanze riservate

Il diagramma seguente mostra uno scenario base dell'acquisto e dell'utilizzo di elementi delle istanze riservate.



In questo scenario, hai un' On-Demand istanza (T2) in esecuzione nel tuo account, per la quale attualmente stai pagando delle tariffe. On-Demand Acquisti un'Istanza riservata che coincide con gli attributi dell'istanza in esecuzione e il vantaggio di fatturazione viene immediatamente applicato. Successivamente, acquisti un'Istanza riservata per un'istanza C4. Non hai istanze in esecuzione nell'account corrispondenti agli attributi di questa Istanza riservata. Nella fase finale, avvii un'istanza corrispondente agli attributi dell'Istanza riservata C4 e il vantaggio di fatturazione viene immediatamente applicato.

Variabili chiave che determinano i prezzi di Istanza riservata

I prezzi di Istanza riservata sono determinati dalle seguenti variabili chiave.

Attributi istanza

Un'Istanza riservata ha quattro attributi che ne determinano il prezzo.

- Tipo di istanza: ad esempio, `m4.large`. Questo è composto dalla famiglia di istanze (ad esempio `m4`) e dalla dimensione dell'istanza (ad esempio `large`).
- Region (Regione): la regione in cui Istanza riservata è acquistata.
- Tenancy: indica se l'istanza è in esecuzione su hardware condiviso (per impostazione predefinita) o a singolo tenant (dedicato). Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2.
- Piattaforma: il sistema operativo; ad esempio, Windows o Linux/Unix. Per ulteriori informazioni, consulta Scelta di una piattaforma.

Scadenza impegno

Puoi acquistare un'Istanza riservata per un impegno di un anno o di tre anni, e l'impegno di tre anni presenta uno sconto maggiore.

- One-year: un anno è definito come 31536000 secondi (365 giorni).
- Three-year: Tre anni sono definiti come 94608000 secondi (1095 giorni).

Le istanze riservate non si rinnovano automaticamente; quando scadono, puoi continuare a utilizzare l'istanza EC2 senza interruzioni, ma ti verranno addebitate delle tariffe. On-Demand Nell'esempio precedente, quando scadono le istanze riservate che coprono le istanze T2 e C4, si torna a pagare le On-Demand tariffe fino alla chiusura delle istanze o all'acquisto di nuove istanze riservate che corrispondono agli attributi dell'istanza.

> **Important**
>
> Dopo aver acquistato un'Istanza riservata, non è possibile annullare l'operazione. Tuttavia, è possibile modificare, scambiare o vendere l'Istanza riservata qualora le tue esigenze cambiassero.

Opzioni di pagamento

Le seguenti opzioni di pagamento sono disponibili per gli elementi di Istanze riservate:

- Pagamento anticipato totale: il pagamento viene effettuato per intero all'inizio del termine, senza altri costi o tariffe orarie aggiuntive per l'intervallo restante, indipendentemente dalle ore utilizzate.
- Pagamento anticipato parziale: è richiesto il pagamento anticipato di una parte del costo, mentre le restanti ore nel termine scelto vengono fatturate in base a una tariffa oraria scontata, indipendentemente dall'utilizzo dell'Istanza riservata.
- Nessun pagamento anticipato: viene applicata una tariffa oraria scontata per ogni ora entro il termine, indipendentemente dall'utilizzo dell'Istanza riservata. Non è richiesto alcun pagamento anticipato.

> **Note**
>
> Gli elementi di Istanze riservate senza pagamento anticipato si basano su un obbligo contrattuale mensile per l'intera durata della prenotazione. Per questo motivo, è necessario

fornire una cronologia di fatturazione valida prima di poter acquistare elementi di Istanze riservate senza pagamento anticipato.

In linea generale, l'opzione più vantaggiosa consiste nello scegliere un pagamento anticipato più elevato per Istanze riservate. Puoi anche trovare istanze riservate offerte da venditori di terza parte a prezzi inferiori e per periodi più brevi sul Marketplace delle istanze riservate. Per ulteriori informazioni, consulta Vendita di istanze riservate per Amazon EC2 nel Marketplace delle istanze riservate.

Classe offerta

Se le tue esigenze di calcolo dovessero cambiare, potresti modificare o scambiare l'Istanza riservata in base alla classe di offerta.

- Standard: offre lo sconto maggiore, ma può essere solo modificata. La Istanze riservate standard non può essere scambiata.
- Modificabile: offre uno sconto rispetto alla Istanze riservate standard, ma può essere scambiata per un'altra Istanza riservata modificabile con differenti attributi di istanza. La Istanze riservate modificabile può inoltre essere modificata.

Per ulteriori informazioni, consulta Tipi di elementi di Istanze riservate (Classi di offerta).

Important

Dopo aver acquistato un'Istanza riservata, non è possibile annullare l'operazione. Tuttavia, è possibile modificare, scambiare o vendere l'Istanza riservata qualora le tue esigenze cambiassero.

Per ulteriori informazioni, consulta la pagina dei Prezzi delle istanze riservate di Amazon EC2.

Istanze riservate regionale e zonale (Ambito)

Quando acquisti una Istanza riservata, determini l'ambito della Istanza riservata. L'ambito può essere sia regionale che zonale.

- Regionale: quando acquisti una Istanza riservata per una regione, viene indicata come regionale Istanza riservata.

- Zonale: quando acquisti una Istanza riservata per una specifica zona di disponibilità viene indicata come zonale Istanza riservata.

L'ambito non influisce sul prezzo. Si paga lo stesso prezzo per una Istanza riservata regionale o zonale. Per ulteriori informazioni sui prezzi della Istanza riservata, consulta Variabili chiave che determinano i prezzi di Istanza riservata e Prezzi delle istanze riservate di Amazon EC2.

Per ulteriori informazioni sulla specifica dell'ambito di un'istanza riservata, consulta Attributi RI, specialmente il punto Zona di disponibilità.

Differenze tra Istanze riservate regionale e zonale

La tabella seguente evidenzia alcune differenze chiave tra Istanze riservate regionali e Istanze riservate zonali:

	Istanze riservate regionali	Istanze riservate zonali
Opzione di prenotazione di capacità	Un'Istanza riservata di regione non prenota la capacità.	Un'Istanza riservata di zona prenota la capacità nella zona di disponibilità specificata.
Flessibilità zona di disponibilità	Lo sconto dell'Istanza riservata si applica all'utilizzo della istanza in qualsiasi zona di disponibilità in una regione specifica.	Nessuna flessibilità della zona di disponibilità—lo sconto della Istanza riservata si applica all'utilizzo dell'istanza nella sola zona di disponibilità specificata.
Flessibilità dimensioni istanza	Lo sconto della Istanza riservata si applica all'utilizzo dell'istanza nell'ambito della stessa famiglia di istanze, indipendentemente dalla dimensione. Supportato solo su istanze Linux/Unix riservate Amazon	Nessuna flessibilità nelle dimensioni delle istanze: lo sconto sulle istanze riservate si applica solo all'utilizzo delle istanze per la famiglia di istanze e le dimensioni dell'istanza specificate.

	Istanze riservate regionali	Istanze riservate zonali
	con tenancy predefinita. Per ulteriori informazioni, consulta La flessibilità della dimensione e dell'istanza è determinata dal relativo fattore di normalizzazione..	
Mettere in coda un acquisto	Puoi mettere in coda gli acquisti per le istanze riservate regionali.	Non puoi mettere in coda gli acquisti per le istanze riservate zonali.

Per maggiori informazioni ed esempi, consulta Applicazione degli sconti sulle istanze riservate.

Tipi di elementi di Istanze riservate (Classi di offerta)

La classe di offerta di una Istanza riservata è Standard o Convertibile. Una Istanza riservata Standard offre un maggiore sconto rispetto a una Istanza riservata Convertibile, ma non è possibile scambiare una Istanza riservata Standard. È possibile scambiare una Istanze riservate Convertibile. È possibile modificare una Istanze riservate Standard e Convertibile.

La configurazione della Istanza riservata comprende un tipo di istanza singola, piattaforma, ambito e tenancy per un termine. Se le tue esigenze di elaborazione cambiano, potresti essere in grado di modificare o scambiare la tua Istanza riservata.

Differenze tra Istanze riservate Standard e Convertibile

Di seguito vengono illustrate le differenze tra Istanze riservate Standard e Convertibile.

	Istanza riservata standard	Convertible Reserved Instance
Modificare le Istanze riservate	Alcuni attributi possono essere modificati. Per ulteriori informazioni, consulta Modificare le Istanze riservate.	Alcuni attributi possono essere modificati. Per ulteriori informazioni, consulta Modificare le Istanze riservate.

	Istanza riservata standard	Convertible Reserved Instance
Cambio di istanze riservate	Non è possibile effettuare scambi.	Può essere scambiata durante il termine con un'altra Istanza riservata modificabile con nuovi attributi, tra cui famiglia di istanze, tipo di istanza, piattaforma, ambito o tenancy. Per ulteriori informazioni, consulta Scambiare le Istanze riservate modificabili.
Vendita nel Marketplace delle istanze riservate	Può essere venduta nel Marketplace delle istanze riservate.	Non può essere venduta nel Marketplace delle istanze riservate.
Acquisto nel Marketplace delle istanze riservate	Può essere acquistata nel Marketplace delle istanze riservate.	Non può essere acquistata nel Marketplace delle istanze riservate.

Applicazione degli sconti sulle istanze riservate

Le istanze riservate non sono istanze fisiche, ma piuttosto uno sconto di fatturazione applicato alle istanze in esecuzione nel tuo account. On-Demand Le On-Demand istanze devono soddisfare determinate specifiche delle istanze riservate per beneficiare dello sconto sulla fatturazione.

Se acquisti un'istanza riservata e disponi già di un' On-Demand istanza in esecuzione che corrisponde alle specifiche dell'istanza riservata, lo sconto sulla fatturazione viene applicato immediatamente e automaticamente. Non è necessario riavviare le tue istanze. Se non disponi di un' On-Demand istanza in esecuzione idonea, avvia un' On-Demand istanza con le stesse specifiche dell'istanza riservata. Per ulteriori informazioni, consulta Usa le tue Istanze riservate.

La classe di offerta (standard o convertibile) dell'istanza riservata non influisce sul modo in cui viene applicato lo sconto di fatturazione.

Argomenti

- Applicazione degli elementi di Istanze riservate zonali
- Applicazione degli elementi di Istanze riservate regionali

- Flessibilità dimensioni istanza
- Esempi di applicazione di elementi di Istanze riservate

Applicazione degli elementi di Istanze riservate zonali

Un'istanza riservata acquistata per riservare la capacità in una zona di disponibilità specifica è denominata istanza riservata zonale.

- Lo sconto dell'istanza riservata si applica all'utilizzo della istanza corrispondente in quella zona di disponibilità.
- Gli attributi (tenancy, piattaforma, zona di disponibilità, famiglia di istanze e dimensione dell'istanza) delle istanze in esecuzione devono corrispondere a quelli delle istanze riservate.

Ad esempio, se acquisti due istanze riservate Linux/Unix standard di tenancy `c4.xlarge` predefinite per la zona di disponibilità us-east-1a, fino a due istanze di tenancy `c4.xlarge` predefinite in esecuzione nella zona di disponibilità us-east-1a possono beneficiare dello Linux/Unix sconto sulle istanze riservate.

Applicazione degli elementi di Istanze riservate regionali

Un'istanza riservata acquistata per una regione è detta istanza riservata regionale e fornisce la flessibilità della zona di disponibilità.

- Lo sconto dell'Istanza riservata si applica all'utilizzo della istanza in qualsiasi zona di disponibilità della regione.
- Lo sconto dell'istanza riservata si applica all'utilizzo dell'istanza nell'ambito della stessa famiglia di istanze, indipendentemente dalla dimensione: questo è noto come flessibilità della dimensione dell'istanza.

Flessibilità dimensioni istanza

Con la flessibilità delle dimensioni delle istanze, lo sconto dell'istanza riservata si applica all'utilizzo delle istanze con la stessa famiglia. La flessibilità della dimensione dell'istanza viene applicata dall'istanza più piccola a quella più grande all'interno della famiglia di istanze sulla base del fattore di normalizzazione. Per un esempio di come viene applicato lo sconto dell'istanza riservata, consultare Scenario 2: Istanze riservate in un singolo account utilizzando il fattore di normalizzazione.

Limitazioni

- Supportata: la flessibilità delle dimensioni delle istanze è supportata solo per le istanze riservate regionali.
- Non supportata: la flessibilità delle dimensioni delle istanze non è supportata per le seguenti istanze riservate:
  - Istanze riservate acquistate pe una specifica zona di disponibilità, (Istanze riservate zonali)
  - Istanze riservate per le istanze G4ad, G4dn, G5, G5g, G6, G6e, G6f, Gr6, Gr6f, hpc7a, P5, Inf1, Inf2, u7i-6tb, and u7i-8tb
  - Istanze riservate per Windows Server, Windows Server con SQL Standard, Windows Server con SQL Server Enterprise, Windows Server con SQL Server Web, RHEL e SUSE Linux Enterprise Server
  - Istanze riservate con istanza dedicata a tenancy singola

La flessibilità della dimensione dell'istanza è determinata dal relativo fattore di normalizzazione.

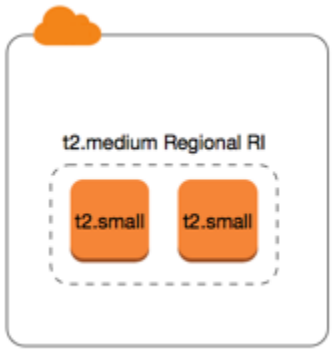
La flessibilità della dimensione dell'istanza è determinata dal relativo fattore di normalizzazione. Lo sconto si applica totalmente o parzialmente alle istanze in esecuzione della stessa famiglia di istanze, in base alla dimensione dell'istanza della prenotazione, in qualsiasi zona di disponibilità nella regione. Gli unici attributi che devono coincidere sono famiglia di istanze, tenancy e piattaforma.

La tabella seguente riporta le diverse dimensioni all'interno di una famiglia di istanze e il corrispondente fattore di normalizzazione. Questa scala viene utilizzata per applicare la tariffa scontata degli elementi di Istanze riservate all'utilizzo normalizzato della famiglia di istanze.

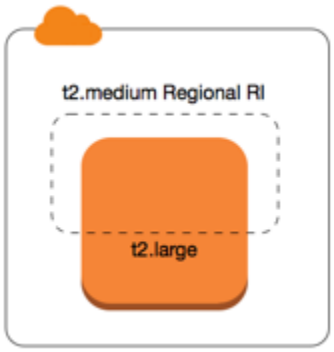
Dimensioni istanza	Fattore di normalizzazione
nano	0.25
micro	0,5
small	1
medium	2
large	4
xlarge	8

Dimensioni istanza	Fattore di normalizzazione
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
96xlarge	768
112xlarge	896

Ad esempio, il fattore di normalizzazione di un'istanza `t2.medium` è 2. Se acquisti un'istanza Linux/Unix riservata Amazon con tenancy `t2.medium` predefinita negli Stati Uniti orientali (Virginia settentrionale) e hai due `t2.small` istanze in esecuzione nel tuo account in quella regione, il vantaggio di fatturazione viene applicato integralmente a entrambe le istanze.



In alternativa, se disponi di un'istanza `t2.large` in esecuzione sul tuo account nella regione US East (N. Virginia), il vantaggio di fatturazione viene applicato al 50% dell'utilizzo dell'istanza.



Il fattore di normalizzazione viene anche applicato quando si modificano gli elementi di Istanze riservate. Per ulteriori informazioni, consulta Modificare le Istanze riservate.

Fattore di normalizzazione per le istanze bare metal

La flessibilità della dimensione dell'istanza si applica inoltre alle istanze bare metal all'interno della famiglia di istanze. Se disponi di istanze Linux/Unix riservate Amazon regionali con tenancy condivisa su istanze bare metal, puoi beneficiare dei risparmi sulle istanze riservate all'interno della stessa famiglia di istanze. È vero anche il contrario: se disponi di istanze Linux/Unix riservate Amazon regionali con tenancy condivisa su istanze della stessa famiglia di istanze bare metal, puoi beneficiare dei risparmi sulle istanze riservate sull'istanza bare metal.

Le dimensioni dell'istanza `metal` non hanno un singolo fattore di normalizzazione. Un'istanza bare metal ha lo stesso fattore di normalizzazione della dimensione dell'istanza virtualizzata equivalente all'interno della stessa famiglia di istanze. Ad esempio, un'istanza `i3.metal` ha lo stesso fattore di normalizzazione di un'istanza `i3.16xlarge`.

Dimensioni istanza	Fattore di normalizzazione
a1.metal	32
m5zn.metal | x2iezn.metal z1d.metal	96
c6g.metal | c6gd.metal | i3.metal | m6g.metal | m6gd.metal | r6g.metal | r6gd.metal | x2gd.metal	128
c5n.metal	144
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-18tb1.metal | u-24tb1.metal	448
u-6tb1.metal | u-9tb1.metal | u-12tb1.metal	896

Ad esempio, il fattore di normalizzazione di un'istanza `i3.metal` è 128. Se acquisti un'istanza Linux/Unix riservata Amazon con tenancy `i3.metal` predefinita negli Stati Uniti orientali (Virginia settentrionale), il vantaggio di fatturazione può essere applicato come segue:

- In alternativa, se disponi di una `i3.16xlarge` in esecuzione sul tuo account nella regione, il vantaggio di fatturazione è applicato integralmente all'istanza `i3.16xlarge` (`i3.16xlarge` fattore di normalizzazione = 128).
- In alternativa, se disponi di due istanze `i3.8xlarge` in esecuzione sul tuo account nella regione, il vantaggio di fatturazione è applicato integralmente alle due istanze `i3.8xlarge` (`i3.8xlarge` fattore di normalizzazione = 64).
- In alternativa, se disponi di quattro istanze `i3.4xlarge` in esecuzione sul tuo account nella regione, il vantaggio di fatturazione è applicato integralmente alle quattro istanze `i3.4xlarge` (`i3.4xlarge` fattore di normalizzazione = 32).

È vero anche il contrario. Ad esempio, se acquisti due istanze Linux/Unix riservate Amazon con tenancy `i3.8xlarge` predefinite negli Stati Uniti orientali (Virginia settentrionale) e hai un'`i3.metal`istanza in esecuzione in quella regione, il vantaggio di fatturazione viene applicato integralmente all'istanza. `i3.metal`

Esempi di applicazione di elementi di Istanze riservate

Gli scenari seguenti descrivono le modalità di applicazione degli elementi di Istanze riservate.

- Scenario 1: elementi di Istanze riservate in un singolo account
- Scenario 2: Istanze riservate in un singolo account utilizzando il fattore di normalizzazione
- Scenario 3: elementi di Istanze riservate regionali in account collegati
- Scenario 4: elementi di Istanze riservate zonali in un account collegato

Scenario 1: elementi di Istanze riservate in un singolo account

Stai eseguendo le seguenti On-Demand istanze nell'account A:

- 4 x istanze Linux `m3.large` con tenancy di default in zona di disponibilità us-east-1a
- 2 x istanze Amazon Linux `m4.xlarge` con tenancy di default in zona di disponibilità us-east-1b
- 1 x istanza Amazon Linux `c4.xlarge` con tenancy di default in zona di disponibilità us-east-1c

Acquisti gli elementi di Istanze riservate seguenti nell'account A:

- 4 x Istanze riservate Linux `m3.large` con tenancy predefinita nella zona di disponibilità us-east-1a (capacità riservata)
- 4 x Istanze riservate Amazon Linux `m4.large`con tenancy predefinita nella regione us-east-1
- 1 x Istanze riservate Amazon Linux `c4.large`con tenancy predefinita nella regione us-east-1

I vantaggi della Istanza riservata vengono applicati nel modo seguente:

- Lo sconto e la prenotazione di capacità delle quattro Istanze riservate `m3.large` di zona vengono utilizzati dalle quattro istanze `m3.large` perché i loro attributi (dimensione dell'istanza, regione, piattaforma, tenancy) coincidono.
- Le Istanze riservate `m4.large` forniscono flessibilità in termini di dimensione dell'istanza e zona di disponibilità perché sono Istanze riservate Amazon Linux regionali con tenancy predefinita.

An `m4.large` è equivalente a 4 normalizzatiunits/hour.

Hai acquistato quattro istanze riservate `m4.large` regionali e, in totale, sono pari a 16 normalizzate units/hour (4x4). L'account A ha due `m4.xlarge` istanze in esecuzione, equivalenti a 16 normalizzate (2x8). units/hour In questo caso, le quattro Istanze riservate regionali `m4.large` forniscono il vantaggio della fatturazione completa per l'uso delle due istanze `m4.xlarge`.

- L' `c4.large` regionale Istanza riservata in us-east-1 fornisce flessibilità in termini di dimensione dell'istanza e zona di disponibilità perché è un'Istanza riservata Amazon Linux regionale con tenancy predefinita che si applica all'istanza `c4.xlarge`. Un'`c4.large`istanza equivale a 4 normalizzate units/hour e a equivale a `c4.xlarge` 8 normalizzate. units/hour

  In questo caso, l'Istanza riservata `c4.large` regionale fornisce un vantaggio parziale all'utilizzo di istanze `c4.xlarge`. Questo perché l'istanza `c4.large` riservata è equivalente a 4 normalizzate units/hour di utilizzo, ma l'`c4.xlarge`istanza ne richiede 8 normalizzate. units/hour Pertanto, lo sconto di fatturazione dell'Istanza riservata `c4.large` si applica al 50% dell'uso di `c4.xlarge`. L'`c4.xlarge`utilizzo rimanente viene addebitato in base alla On-Demand tariffa.

Scenario 2: Istanze riservate in un singolo account utilizzando il fattore di normalizzazione

Stai eseguendo le seguenti On-Demand istanze nell'account A:

- 2 x istanze Amazon Linux `m3.xlarge` con tenancy predefinita in zona di disponibilità us-east-1a
- 2 x istanze Amazon Linux `m3.large` con tenancy di default in zona di disponibilità us-east-1b

Si acquistano gli elementi di Istanze riservate seguenti nell'account A:

- 1 x Istanze riservate Amazon Linux `m3.2xlarge` con tenancy predefinita nella regione us-east-1

I vantaggi della Istanza riservata vengono applicati nel modo seguente:

- L'istanza riservata regionale `m3.2xlarge` in us-east-1 fornisce flessibilità in termini di dimensione dell'istanza e zona di disponibilità perché è un'istanza riservata Amazon Linux regionale con tenancy predefinita. Si applica prima alle istanze `m3.large` e poi alle istanze `m3.xlarge`, perché si applica dalla dimensione più piccola a quella più grande all'interno della famiglia di istanze in base al fattore di normalizzazione.

  Un'`m3.large`istanza equivale a 4 normalizzateunits/hour.

Un'`m3.xlarge`istanza equivale a 8 normalizzateunits/hour.

Un'`m3.2xlarge`istanza equivale a 16 normalizzateunits/hour.

Il vantaggio viene applicato come segue:

L'istanza riservata `m3.2xlarge` regionale offre tutti i vantaggi di un `m3.large` utilizzo raddoppiato, poiché insieme queste istanze rappresentano 8 istanze normalizzate. units/hour Ciò lascia 8 normalizzati units/hour da applicare alle istanze. `m3.xlarge`

Con le restanti 8 normalizzate units/hour, l'istanza riservata `m3.2xlarge` regionale offre tutti i vantaggi di 1 `m3.xlarge` utilizzo, poiché ogni `m3.xlarge` istanza equivale a 8 normalizzate. units/hour L'`m3.xlarge`utilizzo rimanente viene addebitato in base alla On-Demand tariffa.

Scenario 3: elementi di Istanze riservate regionali in account collegati

Gli elementi di Istanze riservate vengono innanzitutto applicati all'utilizzo all'interno dell'account di acquisto e, successivamente, all'utilizzo idoneo in qualsiasi altro account nell'organizzazione. Per ulteriori informazioni, consulta Istanze riservate e fatturazione consolidata. Per gli elementi di Istanze riservate regionali che offrono flessibilità della dimensione dell'istanza viene applicata dall'istanza più piccola a quella più grande all'interno della famiglia di istanze sulla base del fattore di normalizzazione.

Stai utilizzando le seguenti On-Demand istanze nell'account A (l'account di acquisto):

- 2 x istanze Linux `m4.xlarge` con tenancy di default in zona di disponibilità us-east-1a
- 1 x istanza Linux `m4.2xlarge` con tenancy di default in zona di disponibilità us-east-1b
- 2 x istanze Linux `c4.xlarge` con tenancy di default in zona di disponibilità us-east-1a
- 1 x istanza Linux `c4.2xlarge` con tenancy di default in zona di disponibilità us-east-1b

Un altro cliente sta utilizzando le seguenti On-Demand istanze nell'account B, un account collegato:

- 2 x istanze Linux `m4.xlarge` con tenancy di default in zona di disponibilità us-east-1a

Stai acquistando i seguenti elementi di Istanze riservate regionali nell'account A:

- 4 x Istanze riservate Linux `m4.xlarge` con tenancy predefinita nella regione us-east-1

- 2 x Istanze riservate Linux `c4.xlarge` con tenancy predefinita nella regione us-east-1

I vantaggi della Istanza riservata regionale vengono applicati nel modo seguente:

- Lo sconto delle quattro Istanze riservate`m4.xlarge` è usato dalle due istanze `m4.xlarge` e dalla singola istanza `m4.2xlarge` nell'account A (account di acquisto). Tutte le tre istanze hanno i medesimi attributi (famiglia di istanze, regione, piattaforma, tenancy). Lo sconto è applicato prima alle istanze nell'account di acquisto (account A), anche se l'account B (account collegato) ha due `m4.xlarge` che anch'esse corrispondono alle Istanze riservate. Non è prevista la prenotazione di capacità perché le Istanze riservate sono Istanze riservate regionali.
- Lo sconto delle due Istanze riservate `c4.xlarge` si applica alle due istanze `c4.xlarge`, in quanto di dimensioni inferiori rispetto all'istanza`c4.2xlarge`. Non è prevista la prenotazione di capacità perché le Istanze riservate sono Istanze riservate regionali.

Scenario 4: elementi di Istanze riservate zonali in un account collegato

In generale, gli elementi di Istanze riservate di proprietà di un account vengono applicati innanzitutto all'utilizzo in quell'account. Tuttavia, in presenza di Istanze riservate idonee e non utilizzate per una zona di disponibilità specifica (Istanze riservate di zona) in altri account dell'organizzazione, queste vengono applicate all'account prima delle Istanze riservate regionali di proprietà dell'account. Questo mira a garantire il massimo utilizzo dell'Istanza riservata e una fattura ridotta. Per motivi di fatturazione, tutti gli account all'interno dell'organizzazione vengono trattati come se fossero un account unico. L'esempio seguente potrebbe aiutare a descrivere quanto illustrato in precedenza.

Stai eseguendo la seguente On-Demand istanza nell'account A (l'account di acquisto):

- 1 x istanza Linux `m4.xlarge` con tenancy di default in zona di disponibilità us-east-1a

Un cliente sta eseguendo la seguente On-Demand istanza nell'account B collegato:

- 1 x istanza Linux `m4.xlarge` con tenancy di default in zona di disponibilità us-east-1b

Stai acquistando i seguenti elementi di Istanze riservate regionali nell'account A:

- 1 x Istanza riservata Linux `m4.xlarge` con tenancy predefinita nella regione us-east-1

Un cliente acquista anche i seguenti elementi di Istanze riservate zonali nell'account collegato C:

- 1 x Istanze riservate Linux `m4.xlarge` con tenancy predefinita in zona di disponibilità us-east-1a

I vantaggi della Istanza riservata vengono applicati nel modo seguente:

- Lo sconto dell'Istanza riservata `m4.xlarge` di zona di proprietà dell'account C viene applicato all'utilizzo di `m4.xlarge` nell'account A.
- Lo sconto dell'Istanza riservata `m4.xlarge` regionale di proprietà dell'account A viene applicato all'utilizzo di `m4.xlarge` nell'account B.
- Se l'istanza riservata regionale di proprietà dell'account A è stata applicata per la prima volta all'utilizzo nell'account A, l'istanza riservata zonale di proprietà dell'account C rimane inutilizzata e l'utilizzo nell'account B viene addebitato secondo le tariffe. On-Demand

Per ulteriori informazioni, consulta Understanding your reservations in AWS Cost and Usage Report.

> **Note**
>
> Le istanze riservate zonali riservano la capacità solo all'account di proprietà e non possono essere condivise con altri Account AWS. Se hai bisogno di condividere la capacità con altri Account AWS, usa Riserva la capacità di calcolo con EC2 On-Demand Capacity Reservations.

Usa le tue Istanze riservate

Le istanze riservate vengono applicate automaticamente alle On-Demand istanze in esecuzione a condizione che le specifiche corrispondano. Se non sono presenti On-Demand istanze in esecuzione che corrispondano alle specifiche dell'istanza riservata, l'istanza riservata rimane inutilizzata finché non si avvia un'istanza con le specifiche richieste.

Se stai avviando un' On-Demand istanza per sfruttare i vantaggi in termini di fatturazione di un'istanza riservata, assicurati di specificare le seguenti informazioni quando configuri l'istanza: On-Demand

Platform (Piattaforma)

È necessario specificare una Amazon Machine Image (AMI) corrispondente alla piattaforma (descrizione del prodotto) dell'istanza riservata. Ad esempio, se si è specificato `Linux/UNIX` per l'istanza riservata, si può avviare un'istanza da un'AMI Amazon Linux o un'AMI Ubuntu.

Tipo di istanza

Se si è acquistata un'istanza riservata zonale, è necessario specificare lo stesso tipo di istanza dell'istanza riservata, ad esempio, `t3.large`. Per ulteriori informazioni, consulta Applicazione degli elementi di Istanze riservate zonali.

Se si è acquistata un'istanza riservata regionale, è necessario specificare un tipo di istanza della stessa famiglia di istanze del tipo di istanza dell'istanza riservata. Ad esempio, se si è specificato `t3.xlarge` per la propria istanza riservata, è necessario avviare l'istanza dalla famiglia T3, ma si può specificare qualsiasi dimensione, ad esempio `t3.medium`. Per ulteriori informazioni, consulta Applicazione degli elementi di Istanze riservate regionali.

Zona di disponibilità

Se si è acquistata un'Istanza riservata per una zona di disponibilità specifica, è necessario avviare l'istanza nella stessa zona di disponibilità.

Se si è acquistata un'istanza riservata regionale, è possibile avviare l'istanza in qualsiasi zona di disponibilità nella regione specificata per l'istanza riservata.

Tenancy

La tenancy (`dedicated` o `shared`) dell'istanza deve corrispondere alla tenancy dell'istanza riservata. Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2.

Per esempi di come le istanze riservate vengono applicate alle istanze in esecuzione On-Demand , consulta. Applicazione degli sconti sulle istanze riservate Per ulteriori informazioni, consulta Perché le mie istanze riservate di Amazon EC2 non si applicano alla mia AWS fatturazione nel modo previsto?

Puoi utilizzare vari metodi per avviare le On-Demand istanze che utilizzano il tuo sconto sulle istanze riservate. Per ulteriori informazioni sui diversi metodi di avvio, consultare Avviare un'istanza Amazon EC2. Per avviare un'istanza, è possibile utilizzare Amazon EC2 Auto Scaling. Per ulteriori informazioni, consulta Guida per l'utente di Amazon EC2 Auto Scaling.

Come funziona la fatturazione con le istanze riservate

Tutte le istanze riservate ti offrono uno sconto rispetto ai On-Demand prezzi. Con gli elementi di Istanze riservate, è previsto il pagamento per l'intero termine, indipendentemente dall'uso effettivo. Puoi scegliere di effettuare un pagamento anticipato, anticipato parziale o mensile per la tua Istanza riservata, in base all'opzione di pagamento specificata per l'Istanza riservata.

Quando le istanze riservate scadono, ti vengono addebitate le On-Demand tariffe per l'utilizzo delle istanze EC2. Puoi mettere in coda una Istanza riservata per l'acquisto con fino a tre anni di anticipo. Questo garantisce copertura continua. Per ulteriori informazioni, consulta Metti in coda il tuo acquisto.

Piano gratuito di AWS È disponibile per le nuove. Account AWS Se utilizzi il Piano gratuito di AWS per eseguire istanze Amazon EC2 e acquisti un'istanza riservata, ti verrà addebitato il prezzo standard. Per informazioni, consulta Piano gratuito di AWS.

Indice

- Fatturazione dell'utilizzo
- Visualizzazione di una fattura
- Istanze riservate e fatturazione consolidata
- Livelli dei prezzi di sconto della Istanza riservata

Fatturazione dell'utilizzo

Le Istanze riservate vengono fatturate ogni ora di orologio per l'intervallo di tempo selezionato, anche se non ci sono istanze in esecuzione. L'inizio dell'ora parte a zero minuti e zero secondi, in base a un orologio standard di 24 ore. Ad esempio, un'ora di orologio inizia a 1:00:00 e termina a 1:59:59. Per ulteriori informazioni sugli stati delle istanze, consulta Cambio di stato di un'istanza Amazon EC2.

Un vantaggio di fatturazione per le istanze riservate può essere applicato a un'istanza in esecuzione su base al secondo. Per-second la fatturazione è disponibile per le istanze che utilizzano una distribuzione Linux open source, come Amazon Linux e Ubuntu. Per-hour la fatturazione viene utilizzata per le distribuzioni Linux commerciali, come Red Hat Enterprise Linux e SUSE Linux Enterprise Server.

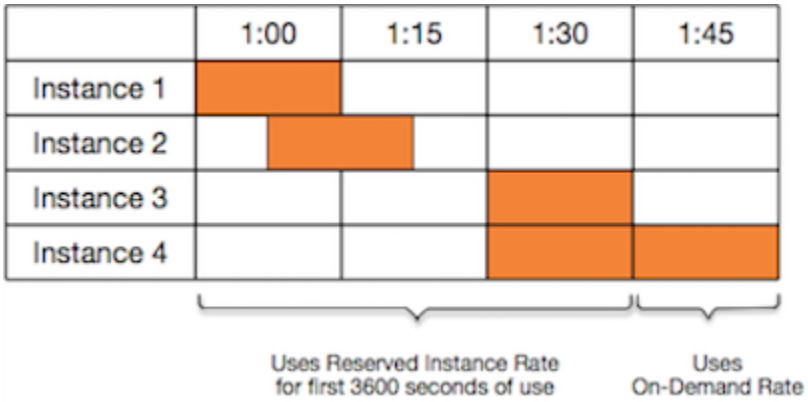
Il vantaggio di fatturazione della Istanza riservata può essere applicato a un massimo di 3600 secondi (un'ora) di utilizzo d'istanza per ora di orologio. Puoi eseguire più istanze contemporaneamente, ma puoi beneficiare dello sconto sulle istanze riservate solo per un totale di 3600 secondi all'ora; l'utilizzo dell'istanza che supera i 3600 secondi in un'ora viene fatturato alla tariffa. On-Demand

Ad esempio, se acquisti un'istanza `m4.xlarge` riservata ed esegui quattro `m4.xlarge` istanze contemporaneamente per un'ora, un'istanza viene addebitata un'ora di utilizzo dell'istanza riservata e le altre tre istanze vengono addebitate tre ore di On-Demand utilizzo.

Tuttavia, se acquisti un'istanza `m4.xlarge` riservata ed esegui quattro `m4.xlarge` istanze per 15 minuti (900 secondi) ciascuna nella stessa ora, il tempo di esecuzione totale delle istanze è di un'ora, il che si traduce in un'ora di utilizzo dell'istanza riservata e 0 ore di On-Demand utilizzo.



Se più istanze idonee sono in esecuzione contemporaneamente, il vantaggio di fatturazione delle istanze riservate viene applicato a tutte le istanze contemporaneamente fino a un massimo di 3600 secondi in un'ora; successivamente, si applicano le On-Demand tariffe.



Cost Explorer sulla console di fatturazione e gestione dei costi consente di analizzare i risparmi rispetto alle istanze in esecuzione. On-Demand Le domande frequenti sulle Istanze riservate includono un esempio di calcolo del valore di listino.

Se chiudi l' AWS account, la On-Demand fatturazione delle risorse viene interrotta. Tuttavia, se disponi di elementi di Istanze riservate nell'account, continuerai a ricevere la relativa fattura finché non scadono.

Visualizzazione di una fattura

Puoi trovare maggiori informazioni su addebiti e tariffe applicati al tuo account nella console Gestione costi e fatturazione AWS.

- Il Dashboard (Pannello di controllo) mostra un riepilogo di spesa per l'account.

- Nella pagina Bills (Fatture), sotto Details (Dettagli), espandi la sezione Elastic Compute Cloud e la regione per ottenere le informazioni di fatturazione relative alle Istanze riservate.

Puoi visualizzare gli addebiti online o scarica un file CSV.

Puoi anche monitorare l'utilizzo dell'istanza riservata utilizzando il rapporto su AWS costi e utilizzo. Per ulteriori informazioni, consulta Understanding your reservations.

Istanze riservate e fatturazione consolidata

I vantaggi in termini di prezzi degli elementi di Istanze riservate sono condivisi quando l'account di acquisto appartiene a un insieme di account fatturati in un unico account pagamento della fatturazione consolidata. L'utilizzo delle istanze in tutti gli account membri viene aggregato mensilmente nell'account pagamento. In generale, questa modalità è utile per le aziende con diversi team o gruppi funzionali. Successivamente, viene applicata la logica normale di Istanza riservata per calcolare la fattura. Per ulteriori informazioni, consulta Fatturazione consolidata per AWS Organizations.

Se chiudi l'account che ha acquistato l'istanza riservata, l'account di pagamento continuerà ad essere addebitato per l'istanza riservata fino alla scadenza dell'istanza. L'account chiuso viene eliminato definitivamente dopo 90 giorni e gli account dei membri non beneficiano più dello sconto di fatturazione Istanza riservata.

> **Note**
>
> Le istanze riservate zonali riservano la capacità solo all'account di proprietà e non possono essere condivise con altri Account AWS. Se hai bisogno di condividere la capacità con altri Account AWS, usa Riserva la capacità di calcolo con EC2 On-Demand Capacity Reservations.

Livelli dei prezzi di sconto della Istanza riservata

Se il tuo account è idoneo per un livello di prezzi di sconto, riceve automaticamente sconti su pagamento anticipato e tariffe di utilizzo delle istanze per acquisti di Istanza riservata eseguiti all'interno di tale livello a partire da quel punto. Per risultare idonei per uno sconto, il valore di listino della tua Istanze riservate nella regione deve essere pari ad almeno $500.000 USD.

Si applicano le regole seguenti:

- I livelli di prezzi e relativi sconti si applicano solo agli acquisti di Istanze riservate standard Amazon EC2.
- I livelli di prezzi non si applicano alle Istanze riservate per Windows con SQL Server Standard, SQL Server Web e SQL Server Enterprise.
- I livelli di prezzi non si applicano alle istanze riservate per Linux con SQL Server di qualsiasi tipo.
- Gli sconti sui livelli tariffari si applicano solo agli acquisti effettuati da AWS. Non si applicano agli acquisti di elementi di Istanze riservate di terze parti.
- I livelli di prezzi di sconto non sono attualmente applicabili agli acquisti di Istanza riservata modificabile.

Argomenti

- Calcolare gli sconti sui prezzi della Istanza riservata
- Acquistare con un livello di sconto
- Passaggio di livello di prezzi
- Fatturazione consolidata per i livelli di prezzi

Calcolare gli sconti sui prezzi della Istanza riservata

Puoi determinare il livello di prezzi per il tuo account calcolando il valore di listino per tutti i tuoi elementi di Istanze riservate in una regione. Moltiplica il prezzo orario ricorrente di ciascuna prenotazione per il numero totale di ore del termine e aggiungi il prezzo iniziale senza sconti (noto anche come prezzo fisso) al momento dell'acquisto. Dal momento che il valore di listino è basato su prezzi (pubblici) non scontati, non subisce variazioni qualora risultassi idoneo per uno sconto sui volumi o se il prezzo scendesse dopo l'acquisto degli elementi di Istanze riservate.

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

Ad esempio, in caso di un'Istanza riservata con pagamento anticipato parziale di un anno, `t2.small` suppone che il prezzo iniziale sia 60 USD e che la tariffa oraria sia 0,007 USD, per un valore di listino di 121,32 USD.

```
121.32 = 60.00 + (0.007 * 8760)
```

Per visualizzare i valori del prezzo fisso per le Istanze riservate tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Per visualizzare la colonna Prezzo iniziale, scegli impostazioni (
   
) nell'angolo in alto a destra, attiva Prezzo iniziale e scegli Conferma.

Per visualizzare i valori del prezzo fisso per le Istanze riservate tramite la riga di comando

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (AWS Tools for Windows PowerShell)

Acquistare con un livello di sconto

Quando si acquistano Istanze riservate, Amazon EC2 applica automaticamente qualsiasi sconto alla parte dell'acquisto che rientra in un livello di prezzi di sconto. Non è richiesto alcun intervento diverso ed è possibile acquistare Istanze riservate utilizzando qualsiasi strumento Amazon EC2. Per ulteriori informazioni, consulta Acquisto delle istanze riservate Amazon EC2.

Dopo che il valore di listino delle Istanze riservate attive in una regione passa in un livello di prezzi di sconto, qualsiasi acquisto futuro di Istanze riservate in tale regione viene addebitato a una tariffa scontata. Se un singolo acquisto di elementi di Istanze riservate in una regione ti permette di superare la soglia di un livello di sconto, la porzione dell'acquisto che va oltre tale soglia sarà addebitata alla tariffa scontata. Per ulteriori informazioni sugli ID temporanei dell'Istanza riservata creati durante il processo di acquisto, consulta Passaggio di livello di prezzi.

Se il valore di listino scende al di sotto del prezzo di vendita per tale livello di prezzi di sconto, ad esempio in caso di scadenza di — alcune Istanze riservate, gli acquisti — futuri di Istanze riservate nella regione non saranno scontati. Tuttavia, lo sconto continua a essere applicato agli elementi di Istanze riservate originariamente acquistati nel livello di prezzi di sconto.

Quando compri elementi di Istanze riservate, si verifica uno tra quattro possibili scenari:

- Nessuno sconto: l'acquisto all'interno di una regione è ancora al di sotto della soglia di sconto.
- Sconto parziale: l'acquisto all'interno di una regione supera la soglia del primo livello di sconto. Non si applica alcuno sconto a una o più prenotazioni e la tariffa scontata viene applicata alle restanti prenotazioni.

- Sconto completo: l'intero acquisto all'interno di una regione rientra in un livello di sconto e quest'ultimo viene applicato in modo corretto.
- Due tassi di sconto: l'acquisto all'interno di una regione passa da un livello di sconto inferiore a un livello di sconto superiore. Vengono applicati due tassi diversi: una o più prenotazioni alla tariffa scontata inferiore e le restanti prenotazioni alla tariffa scontata superiore.

Passaggio di livello di prezzi

Se il tuo acquisto ti permette di passare a un livello di prezzi scontati, vedrai più voci per tale acquisto: una per la parte dell'acquisto fatturata al prezzo normale e un'altra per la parte dell'acquisto addebitata alla tariffa scontata applicabile.

Il servizio dell'Istanza riservata genera vari ID dell'Istanza riservata perché l'acquisto è passato da un livello non scontato a un livello scontato o da un livello scontato a un altro. È disponibile un ID per ogni insieme di prenotazioni in un livello. Di conseguenza, l'ID restituito dal comando della CLI o dall'operazione API dell'acquisto è differente dall'ID effettivo dei nuovi elementi di Istanze riservate.

Fatturazione consolidata per i livelli di prezzi

Un account di fatturazione consolidata aggrega il valore di listino degli account membri all'interno di una regione. Quando il valore di listino di tutte le Istanze riservate attive per l'account di fatturazione consolidata raggiunge un livello di prezzi di sconto, tutte le Istanze riservate acquistate a partire da questo punto da qualsiasi membro di tale account vengono fatturate a una tariffa scontata (purché il valore di listino per tale account consolidato si mantenga al di sopra della soglia del livello dei prezzi di sconto). Per ulteriori informazioni, consulta Istanze riservate e fatturazione consolidata.

Acquisto delle istanze riservate Amazon EC2

Per acquistare un'istanza riservata per Amazon EC2, puoi utilizzare la console Amazon EC2, uno strumento a riga di comando o un SDK per cercare offerte di istanze riservate da AWS e venditori di terze parti, modificando i parametri di ricerca fino a trovare la corrispondenza esatta che stai cercando.

Durante la ricerca di elementi di Istanze riservate da acquistare, ricevi un preventivo del costo delle offerte restituite. Quando procedi con l'acquisto, imposta AWS automaticamente un prezzo limite sul prezzo di acquisto. Il costo totale dei tuoi elementi di Istanze riservate non supererà l'importo riportato nel preventivo.

Se il prezzo aumenta o varia per qualsiasi motivo, l'acquisto non viene completato. Quando acquisti un'istanza riservata da un venditore terzo dal Marketplace delle istanze riservate Amazon EC2, se ci sono offerte simili a un prezzo iniziale inferiore, AWS vende le offerte al prezzo iniziale inferiore.

Prima di confermare l'acquisto, verifica i dettagli della Istanza riservata che intendi comprare e assicurati che tutti i parametri siano accurati. Dopo aver acquistato un'Istanza riservata (da un venditore terzo nel Reserved Instance Marketplace o presso AWS), non puoi annullare l'acquisto. Puoi mettere in coda un acquisto per il futuro e annullare l'acquisto in coda prima dell'orario programmato.

Per acquistare e modificare le istanze riservate, assicurarsi che l'utente disponga delle autorizzazioni appropriate, ad esempio la possibilità di descrivere le zone di disponibilità. Per informazioni, consulta the section called "Utilizzo delle Istanze riservate" (API) o the section called "Utilizzo delle Istanze riservate" (console).

Processi

- Scelta di una piattaforma
- Metti in coda il tuo acquisto
- Acquisto di Istanze riservate Standard
- Acquista Istanze riservate modificabili.
- Acquistare dal Marketplace di Istanza riservata
- Annulla un acquisto in coda
- Rinnovare una Istanza riservata

Scelta di una piattaforma

Amazon EC2 supporta le seguenti piattaforme per le istanze riservate:

- Linux/UNIX
- Linux con SQL Server Standard
- Linux con SQL Server Web
- Linux con SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- Red Hat Enterprise Linux con HA

- Windows
- Windows con SQL Server Standard
- Windows con SQL Server Web
- Windows con SQL Server Enterprise

Considerazioni

- Se porti con te l'abbonamento esistente (BYOS) per Red Hat Enterprise Linux, SUSE Linux o Ubuntu Pro, devi scegliere un'offerta per la piattaforma. Linux/Unix
- Le istanze riservate non sono supportate sulle istanze che eseguono macOS o Ubuntu Pro (abbonamento EC2 incluso, cioè non BYOS). Per risparmiare grazie ai prezzi delle On-Demand istanze, ti consigliamo di utilizzare le istanze macOS e Ubuntu Pro (abbonamento EC2 incluso) con Savings Plans. Per ulteriori informazioni, consulta la Guida per l'utente di Savings Plans.

Per garantire che un'istanza venga eseguita in un'istanza riservata specifica, la piattaforma di quest'ultima deve corrispondere alla piattaforma dell'AMI utilizzata per avviare l'istanza. Per le AMI Linux, è importante verificare se la piattaforma AMI utilizza il valore generale Linux/UNIX o un valore più specifico come SUSE Linux.

Console

Per verificare la piattaforma AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI.
4. Nella scheda Dettagli, controlla il valore di Dettagli della piattaforma.

AWS CLI

Per verificare la piattaforma AMI

Utilizza il comando describe-images e controlla il valore di `PlatformDetails`.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
```

```
    --query Images[*].PlatformDetails
```

Di seguito è riportato un output di esempio.

```
[
    "Linux/UNIX"
]
```

PowerShell

Per verificare la piattaforma AMI

Usa il Get-EC2Image cmdlet e controlla il valore di. `PlatformDetails`

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | `
    Select PlatformDetails
```

Di seguito è riportato un output di esempio.

```
PlatformDetails
---------------
Linux/UNIX
```

Metti in coda il tuo acquisto

Per impostazione predefinita, quando si acquista una Istanza riservata, l'acquisto viene effettuato immediatamente. In alternativa, puoi accodare gli acquisti per una data e ora nel futuro. Ad esempio, puoi accodare un acquisto per l'ora approssimativa in cui un Istanza riservata esistente scade. Questo garantisce copertura continua.

Puoi accodare acquisti per Istanze riservate regionale, ma non per Istanze riservate o Istanze riservate zonale da altri venditori. Puoi mettere in coda un acquisto con fino a tre anni di anticipo. Alla data e ora pianificati, l'acquisto viene eseguito utilizzando il metodo di pagamento predefinito. Al termine del pagamento, viene applicato il vantaggio di fatturazione.

Puoi impostare una data per gli acquisti in coda nella console Amazon EC2 e questo rimarrà in coda fino alle 00:00 UTC di tale data. Per specificare un orario diverso per l'acquisto in coda, utilizza un AWS SDK o uno strumento a riga di comando.

Nella console Amazon EC2 puoi visualizzare gli acquisti messi in coda. Lo stato degli acquisti accodati è queued (in coda). Puoi annullare un acquisto messo in coda in qualsiasi momento prima dell'ora pianificata. Per informazioni dettagliate, vedi Annulla un acquisto in coda.

Acquisto di Istanze riservate Standard

Puoi acquistare elementi di Istanze riservate standard in una zona di disponibilità specifica e ottenere una prenotazione di capacità. In alternativa, puoi fare a meno della prenotazione di capacità e acquistare una Istanza riservata standard regionale.

Al termine dell'acquisto, se disponi già di un'istanza in esecuzione che coincide con le specifiche dell'Istanza riservata, il vantaggio di fatturazione viene applicato immediatamente. Non devi riavviare le istanze. Se non hai un'istanza in esecuzione idonea, avvia un'istanza e assicurati di soddisfare gli stessi criteri specificati per l'istanza riservata. Per ulteriori informazioni, consulta Usa le tue Istanze riservate.

Per esempi della modalità di applicazione delle Istanze riservate alle istanze in esecuzione, consulta Applicazione degli sconti sulle istanze riservate.

Console

Per acquistare istanze riservate standard

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate), e quindi selezionare Purchase Istanze riservate (Acquista elementi di &ris;).
3. Per Offering Class (Classe di offerta), scegliere Standard per visualizzare le Istanze riservate standard.
4. Per acquistare una prenotazione di capacità, attivare Only show offerings that reserve capacity (Mostra solo le offerte che prenotano capacità) nell'angolo in alto a destra della schermata di acquisto. Quando si attiva questa impostazione, viene visualizzato il campo Availability Zone (Zona di disponibilità).

   Per acquistare una Istanza riservata regionale, disattivare questa impostazione. Quando si disattiva questa impostazione, il campo Availability Zone (Zona di disponibilità) scompare.
5. Selezionare altre configurazioni secondo necessità e poi scegliere Search (Cerca).
6. Per ciascuna Istanza riservata che si desidera acquistare, immettere la quantità desiderata e scegliere Add to Cart (Aggiungi al carrello).

Per acquistare un'istanza riservata standard dal Marketplace delle istanze riservate, cercare 3rd Party (Terza parte) nella colonna Seller (Venditore) nei risultati della ricerca. La colonna Term (Termine) mostra termini non standard. Per ulteriori informazioni, consulta Acquistare dal Marketplace di Istanza riservata.

7. Per visualizzare un riepilogo delle Istanze riservate selezionate, scegliere View Cart (Visualizza carrello).
8. Se Order on (Ordina il) è Now (Ora), l'acquisto viene completato immediatamente dopo aver scelto Order all (Ordina tutto). Per mettere in corda un acquisto, scegli Now (Ora) e seleziona una data. Puoi selezionate una data diversa per ogni offerta idonea nel carrello. L'acquisto viene messo in coda fino alle 00:00 UTC della data selezionata.
9. Per completare l'ordine, scegliere Order all (Ordina tutto).

   Se, al momento dell'ordine, ci sono offerte simili a quelle che hai scelto ma con un prezzo inferiore, ti AWS vende le offerte al prezzo più basso.
10. Scegliere Close (Chiudi).

    Nella colonna State (Stato) viene mostrato lo stato dell'ordine. Una volta completato l'ordine, il valore State (Stato) cambia da `Payment-pending` a `Active`. Quando l'Istanza riservata è `Active`, è pronta per l'uso.

    Se lo stato è impostato su`Retired`, AWS potrebbe non aver ricevuto il pagamento.

AWS CLI

Per acquistare un'istanza riservata standard

1. Trovare le Istanze riservate istanze disponibili utilizzando il comando describe-reserved-instances-offerings. Specifica `standard` per far sì che l'opzione `--offering-class` restituisca solo istanze riservate standard. Puoi applicare criteri aggiuntivi per restringere i risultati. Ad esempio, usa il seguente comando per acquistare un'istanza riservata regionale `t2.large` con tenancy predefinita `Linux/UNIX` per un periodo di un solo anno.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
```

```
    --filters Name=duration,Values=31536000 \
              Name=scope,Values=Region
```

Per trovare istanze riservate solo sul Marketplace delle istanze riservate, utilizza il filtro `marketplace` e non specificare una durata nella richiesta, dal momento che il termine potrebbe essere inferiore a 1 o 3 anni.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=marketplace,Values=true
```

Una volta individuata un'Istanza riservata che soddisfi le proprie esigenze, prendere nota dell'ID dell'offerta. Ad esempio:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Utilizzare il comando purchase-reserved-instances-offering per acquistare l'Istanza riservata. È necessario specificare l'ID dell'offerta dell'Istanza riservata ottenuto nella fase precedente nonché il numero di istanze per la prenotazione.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

Per impostazione predefinita, l'acquisto viene completato immediatamente. In alternativa, per mettere in coda l'acquisto, aggiungi la seguente opzione alla chiamata precedente.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Utilizzare il comando describe-reserved-instances per ottenere lo stato dell'Istanza riservata.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342fec06327 \
    --query ReservedInstances[].State
```

PowerShell

Per acquistare un'istanza riservata standard

1. Trova le istanze riservate disponibili utilizzando il Get-EC2ReservedInstancesOffering cmdlet. Specificare `standard` per far sì che il parametro `-OfferingClass` restituisca solo Istanze riservate standard. Puoi applicare criteri aggiuntivi per restringere i risultati. Ad esempio, usa il seguente comando per acquistare un'istanza riservata regionale `t2.large` con tenancy predefinita `Linux/UNIX` per un periodo di un solo anno.

```
Get-EC2ReservedInstancesOffering `
    -InstanceType "t2.large" `
    -OfferingClass "standard" `
    -ProductDescription "Linux/UNIX" `
    -InstanceTenancy "default" `
    -Filters @{Name="duration"; Values="31536000"} `
             @{Name="scope"; Values="Region"
```

Per trovare istanze riservate solo sul Marketplace delle istanze riservate, utilizza il filtro `marketplace` e non specificare una durata nella richiesta, dal momento che il termine potrebbe essere inferiore a 1 o 3 anni.

```
Get-EC2ReservedInstancesOffering `
    -InstanceType t2.large `
    -OfferingClass "standard" `
    -ProductDescription "Linux/UNIX" `
    -InstanceTenancy default `
    -Filters @{Name="marketplace"; Values="true"}
```

Una volta individuata un'Istanza riservata che soddisfi le proprie esigenze, prendere nota dell'ID dell'offerta. Ad esempio:

```
bec624df-a8cc-4aad-a72f-4f8abc34caf2
```

2. Usa il New-EC2ReservedInstance cmdlet per acquistare la tua istanza riservata. È necessario specificare l'ID dell'offerta dell'Istanza riservata ottenuto nella fase precedente nonché il numero di istanze per la prenotazione.

```
New-EC2ReservedInstance `
    -ReservedInstancesOfferingId "bec624df-a8cc-4aad-a72f-4f8abc34caf2" `
```

```
    -InstanceCount 1
```

Per impostazione predefinita, l'acquisto viene completato immediatamente. In alternativa, per mettere in coda l'acquisto, aggiungere il seguente parametro alla chiamata precedente.

```
-PurchaseTime "2020-12-01T00:00:00Z"
```

3. Usa il Get-EC2ReservedInstance cmdlet per ottenere lo stato della tua istanza riservata.

```
Get-EC2ReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342fec06327 | `
    Select State
```

Acquista Istanze riservate modificabili.

Puoi acquistare elementi di Istanze riservate modificabili in una zona di disponibilità specifica e ottenere una prenotazione di capacità. In alternativa, puoi fare a meno della prenotazione di capacità e acquistare una Istanza riservata modificabile regionale.

Se disponi di un'istanza in esecuzione che coincide con le specifiche dell'Istanza riservata, il vantaggio di fatturazione viene immediatamente applicato. Non è necessario riavviare le tue istanze. Se non hai un'istanza in esecuzione idonea, avvia un'istanza e assicurati di soddisfare le stesse policy specificate per l'Istanza riservata. Per ulteriori informazioni, consulta Usa le tue Istanze riservate.

Per esempi della modalità di applicazione delle Istanze riservate alle istanze in esecuzione, consulta Applicazione degli sconti sulle istanze riservate.

Console

Per acquistare istanze riservate modificabili

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate), e quindi selezionare Purchase Istanze riservate (Acquista elementi di &ris;).
3. Per Offering Class (Classe di offerta), scegliere Convertible (Convertibile) per visualizzare le Istanze riservate modificabili.

4. Per acquistare una prenotazione di capacità, attivare Only show offerings that reserve capacity (Mostra solo le offerte che prenotano capacità) nell'angolo in alto a destra della schermata di acquisto. Quando si attiva questa impostazione, viene visualizzato il campo Availability Zone (Zona di disponibilità).

   Per acquistare una Istanza riservata regionale, disattivare questa impostazione. Quando si disattiva questa impostazione, il campo Availability Zone (Zona di disponibilità) scompare.
5. Selezionare altre configurazioni secondo necessità e scegliere Search (Cerca).
6. Per ciascuna Istanza riservata modificabile che si desidera acquistare, immettere la quantità e scegliere Add to Cart (Aggiungi al carrello).
7. Per visualizzare un riepilogo della selezione, scegliere View Cart (Visualizza carrello).
8. Se Order on (Ordina il) è Now (Ora), l'acquisto viene completato immediatamente dopo aver scelto Order all (Ordina tutto). Per mettere in corda un acquisto, scegli Now (Ora) e seleziona una data. Puoi selezionate una data diversa per ogni offerta idonea nel carrello. L'acquisto viene messo in coda fino alle 00:00 UTC della data selezionata.
9. Per completare l'ordine, scegliere Order all (Ordina tutto).

   Se, al momento dell'ordine, sono presenti offerte simili a quelle che hai scelto ma con un prezzo inferiore, ti AWS vende le offerte al prezzo inferiore.
10. Scegliere Close (Chiudi).

    Nella colonna State (Stato) viene mostrato lo stato dell'ordine. Una volta completato l'ordine, il valore State (Stato) cambia da `Payment-pending` a `Active`. Quando l'Istanza riservata è `Active`, è pronta per l'uso.

    Se lo stato è impostato su`Retired`, AWS potrebbe non aver ricevuto il pagamento.

AWS CLI

Per acquistare un'istanza riservata modificabile

1. Trovare le Istanze riservate istanze disponibili utilizzando il comando describe-reserved-instances-offerings. Specifica `convertible` per far sì che l'opzione `--offering-class` restituisca solo istanze riservate modificabili. Puoi applicare criteri aggiuntivi per restringere i risultati. Ad esempio, usa il seguente comando per acquistare un'istanza riservata regionale `t2.large` con tenancy predefinita `Linux/UNIX`.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class convertible \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=scope,Values=Region
```

Una volta individuata un'Istanza riservata che soddisfi le proprie esigenze, prendere nota dell'ID dell'offerta. Ad esempio:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Utilizzare il comando purchase-reserved-instances-offering per acquistare l'Istanza riservata. È necessario specificare l'ID dell'offerta dell'Istanza riservata ottenuto nella fase precedente nonché il numero di istanze per la prenotazione.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

Per impostazione predefinita, l'acquisto viene completato immediatamente. In alternativa, per mettere in coda l'acquisto, aggiungi la seguente opzione alla chiamata precedente.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Utilizzare il comando describe-reserved-instances per ottenere lo stato dell'Istanza riservata.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342fec06327 \
    --query ReservedInstances[].State
```

PowerShell

Per acquistare un'istanza riservata modificabile

1. Trova le istanze riservate disponibili utilizzando il Get-EC2ReservedInstancesOffering cmdlet. Specificare `convertible` per far sì che il parametro `-OfferingClass` restituisca solo Istanze riservate modificabili. Puoi applicare criteri aggiuntivi per restringere i risultati. Ad

esempio, usa il seguente comando per acquistare un'istanza riservata regionale `t2.large` con tenancy predefinita `Linux/UNIX`.

```
Get-EC2ReservedInstancesOffering `
    -InstanceType "t2.large" `
    -OfferingClass "convertible" `
    -ProductDescription "Linux/UNIX" `
    -InstanceTenancy "default" `
    -Filters @{Name="scope"; Values="Region"
```

Una volta individuata un'Istanza riservata che soddisfi le proprie esigenze, prendere nota dell'ID dell'offerta. Ad esempio:

```
bec624df-a8cc-4aad-a72f-4f8abc34caf2
```

2. Usa il New-EC2ReservedInstance cmdlet per acquistare la tua istanza riservata. Devi specificare l'ID dell'offerta dell'istanza riservata ottenuto nella fase precedente nonché il numero di istanze per la prenotazione.

```
New-EC2ReservedInstance `
    -ReservedInstancesOfferingId "bec624df-a8cc-4aad-a72f-4f8abc34caf2" `
    -InstanceCount 1
```

Per impostazione predefinita, l'acquisto viene completato immediatamente. In alternativa, per mettere in coda l'acquisto, aggiungere il seguente parametro alla chiamata precedente.

```
-PurchaseTime "2020-12-01T00:00:00Z"
```

3. Usa il Get-EC2ReservedInstance cmdlet per ottenere lo stato della tua istanza riservata.

```
Get-EC2ReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342fec06327 | `
    Select State
```

Acquistare dal Marketplace di Istanza riservata

Puoi acquistare le istanze riservate da venditori di terza parte che non ne hanno più bisogno nel Marketplace delle istanze riservate. È possibile farlo utilizzando la console Amazon EC2 o uno

strumento a riga di comando. Il processo è simile all'acquisto di istanze riservate da. AWS Per ulteriori informazioni, consulta Acquisto di Istanze riservate Standard.

Esistono alcune differenze tra le istanze riservate acquistate nel Marketplace delle istanze riservate e le istanze riservate acquistate direttamente da: AWS

- Scadenza - Le istanze riservate acquistate da venditori di terza parte hanno una validità residua inferiore a quella standard. Condizioni standard complete AWS valide per uno o tre anni.
- Prezzo iniziale: le istanze Third-party riservate possono essere vendute a diversi prezzi iniziali. Le tariffe di utilizzo o ricorrenti sono del tutto identiche a quelle stabilite al momento dell'acquisto originale delle istanze riservate da AWS.
- Tipi di istanze riservate - Dal Marketplace delle istanze riservate è possibile acquistare solo le istanze riservate Standard di Amazon EC2. Le istanze riservate convertibili, Amazon RDS e le istanze ElastiCache riservate Amazon non sono disponibili per l'acquisto sul Reserved Instance Marketplace.

Le tue informazioni di base vengono condivise con il venditore, ad esempio il codice postale e le informazioni relative al paese.

Tali informazioni consentono al venditore di calcolare tutte le imposte destinate al governo applicabili alle transazioni (come l'imposta sulle vendite o l'imposta sul valore aggiunto). Vengono comunicate come report di pagamento. In rare circostanze, AWS potrebbe essere necessario fornire al venditore il tuo indirizzo email, in modo che possa contattarti in merito a domande relative alla vendita (ad esempio, domande fiscali).

Per ragioni analoghe, AWS condivide il nome della persona giuridica del venditore sulla fattura di acquisto dell'acquirente. Se hai bisogno di informazioni aggiuntive sul venditore, per motivi fiscali o ragioni correlate, contatta Supporto.

Annulla un acquisto in coda

Puoi mettere in coda un acquisto con fino a tre anni di anticipo. Puoi annullare un acquisto messo in coda in qualsiasi momento prima dell'ora pianificata.

Console

Per annullare un acquisto in coda

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Selezionare una o più Istanze riservate.
4. Scegliere Actions (Operazioni), Delete Queued Reserved Instances (Elimina istanze riservate in coda).
5. Quando viene richiesta la conferma, scegliere Delete (Elimina) e quindi Close (Chiudi).

AWS CLI

Per annullare un acquisto in coda

Usa il comando delete-queued-reserved-instances.

```
aws ec2 delete-queued-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342fec06327
```

PowerShell

Per annullare un acquisto in coda

Utilizza il cmdlet Remove-EC2QueuedReservedInstance.

```
Remove-EC2QueuedReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342fec06327
```

Rinnovare una Istanza riservata

È possibile rinnovare una Istanza riservata prima che sia programmata per la scadenza. Rinnovando una Istanza riservata viene messo in coda l'acquisto di una Istanza riservata con la stessa configurazione fino alla scadenza della Istanza riservata corrente.

Devi rinnovare le istanze riservate utilizzando la console Amazon EC2.

Come rinnovare una Istanza riservata utilizzando un acquisto in coda

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Selezionare l'Istanza riservata da rinnovare.
4. Selezionare Actions (Operazioni), Renew Reserved Instances (Rinnova istanze riservate).

5. Per completare l'ordine, scegliere Order all (Ordina tutto), quindi Close (Chiudi).

Vendita di istanze riservate per Amazon EC2 nel Marketplace delle istanze riservate

Amazon EC2 Reserved Instance Marketplace è una piattaforma che facilita la vendita di istanze riservate standard inutilizzate da AWS clienti e venditori terzi. Queste istanze riservate possono variare in termini di durata e opzioni di prezzo. Potresti voler vendere le tue istanze riservate quando non ti servono più, ad esempio quando sposti le tue istanze su una nuova, passi a un tipo di istanza diverso Regione AWS, finisci i progetti prima della scadenza del periodo di validità delle istanze riservate, le tue esigenze aziendali cambiano o hai una capacità in eccesso.

Fino a quando le istanze riservate saranno elencate nel Marketplace delle istanze riservate, saranno disponibili per potenziali acquirenti. Tutti gli elementi di Istanze riservate sono raggruppati in base alla durata del periodo residuo e del prezzo orario.

Per soddisfare la richiesta di un acquirente di acquistare l'Istanza riservata di un venditore terzo tramite il Reserved Instance Marketplace, vende AWS innanzitutto l'Istanza riservata al prezzo iniziale più basso nel gruppo specificato. Quindi, AWS vende l'Istanza riservata al prezzo successivo più basso, fino all'evasione dell'intero ordine dell'acquirente. AWS quindi elabora le transazioni e trasferisce la proprietà delle istanze riservate all'acquirente.

Rimani proprietario della Istanza riservata finché non viene venduta. Una volta conclusa la vendita, non disporrai più della prenotazione di capacità e delle tariffe ricorrenti scontate. Se continui a utilizzare la tua istanza, ti AWS addebita il On-Demand prezzo a partire dal momento in cui l'istanza riservata è stata venduta.

Per vendere istanze riservate inutilizzate sul Marketplace delle istanze riservate, è necessario soddisfare determinati criteri di idoneità.

Per informazioni sull'acquisto di istanze riservate nel Marketplace delle istanze riservate, consulta Acquistare dal Marketplace di Istanza riservata.

Indice

- Restrizioni e limitazioni
- Registrati come venditore
- Conto bancario per il pagamento
- Informazioni fiscali
- Dare un prezzo alla Istanze riservate

- Elencare le Istanze riservate
- Stato dell'elenco d'Istanza riservata
- Ciclo di vita di un elenco
- Dopo la vendita della Istanza riservata
- Ricezione dei pagamenti
- Informazioni condivise con l'acquirente

Restrizioni e limitazioni

Prima di poter vendere le prenotazioni inutilizzate, è necessario registrarsi come venditore nel Marketplace delle istanze riservate. Per informazioni, consulta Registrati come venditore.

Le seguenti limitazioni e restrizioni si applicano alla vendita di elementi di Istanze riservate:

- Sul Marketplace delle istanze riservate è possibile vendere solo le istanze riservate regionali e zonali standard di Amazon EC2.
- Sul Marketplace delle istanze riservate non è possibile vendere le istanze riservate modificabili di Amazon EC2.
- Le istanze riservate per altri AWS servizi, come Amazon RDS e Amazon ElastiCache, non possono essere vendute nel Reserved Instance Marketplace.
- L'Istanza riservata standard deve avere almeno un mese di validità residua.
- Non è possibile vendere un'istanza riservata standard in una regione disabilitata per impostazione predefinita.
- Il prezzo minimo consentito nel Marketplace delle istanze riservate è 0 USD.
- Nel Marketplace delle istanze riservate puoi vendere istanze riservate senza pagamento anticipato, con pagamento anticipato parziale o con pagamento anticipato completo, a condizione che siano attive nel tuo account per almeno 30 giorni. Inoltre, se è previsto un pagamento anticipato su un'istanza riservata, questa può essere venduta solo dopo aver ricevuto il pagamento AWS anticipato.
- Non è possibile vendere un'istanza riservata nel Marketplace delle istanze riservate se acquistata con uno sconto di volume.
- Non è possibile modificare l'inserzione direttamente nel Marketplace delle istanze riservate. Tuttavia, puoi farlo annullandolo e successivamente creandone un altro con nuovi parametri. Per informazioni, consulta Dare un prezzo alla Istanze riservate. Puoi anche modificare gli elementi

di Istanze riservate prima di includerli nell'elenco. Per informazioni, consulta Modificare le Istanze riservate.

- AWS addebita una commissione di servizio pari al 12% del prezzo totale anticipato di ogni istanza riservata standard venduta nel Reserved Instance Marketplace. Il prezzo iniziale è il prezzo che il venditore addebita per la Istanza riservata standard.
- Quando ti registri come venditore, la banca specificata deve avere un indirizzo negli Stati Uniti. Per maggiori informazioni, consulta Requisiti aggiuntivi del venditore per i prodotti a pagamento in Guida per i venditori di Marketplace AWS .
- I clienti di Amazon Web Services India Private Limited (AWS India) non possono registrarsi come venditore su EC2 Reserved Instance Marketplace e non possono elencare o vendere istanze riservate nell'EC2 Reserved Instance Marketplace, anche se hanno un conto bancario negli Stati Uniti. Per ulteriori informazioni, consulta Quali sono le differenze tra Account AWS gli account in India? AWS
- Se cambi il tuo venditore registrato in Amazon Web Services India Private Limited (AWS India), verrai cancellato come venditore dall'EC2 Reserved Instance Marketplace e tutte le tue offerte attive esistenti sull'EC2 Reserved Instance Marketplace verranno rimosse. Per ripristinare lo stato di venditore, devi cambiare la posizione dell'account in un Paese diverso dall'India e completare nuovamente la registrazione come venditore.

Registrati come venditore

> **Note**
>
> Solo loro Utente root dell'account AWS possono registrare un account come venditore.

Per vendere nel Marketplace delle istanze riservate, devi prima registrarti come venditore. Durante la registrazione, è necessario fornire le informazioni riportate di seguito:

- Coordinate bancarie: èAWS necessario disporre delle coordinate bancarie per l'erogazione dei fondi raccolti al momento della vendita delle prenotazioni. La banca specificata deve avere un indirizzo negli Stati Uniti. Per ulteriori informazioni, consulta Conto bancario per il pagamento.
- Informazioni fiscali — Tutti i venditori devono completare un questionario fiscale per determinare gli eventuali obblighi fiscali. Per ulteriori informazioni, consulta Informazioni fiscali.

Dopo aver AWS ricevuto la registrazione come venditore completata, riceverai un'email di conferma della registrazione e ti informa che puoi iniziare a vendere nel Reserved Instance Marketplace.

Conto bancario per il pagamento

AWS devi disporre delle tue coordinate bancarie per erogare i fondi raccolti quando vendi la tua Istanza riservata. La banca specificata deve avere un indirizzo negli Stati Uniti. Per maggiori informazioni, consulta Requisiti aggiuntivi del venditore per i prodotti a pagamento in Guida per i venditori di Marketplace AWS .

Per registrare un conto bancario predefinito per pagamenti

1. Aprire la pagina per la Registrazione dei venditori nel Marketplace delle istanze riservate e accedere utilizzando le credenziali AWS .
2. Nella pagina Manage Bank Account (Gestisci conto bancario), fornire le informazioni seguenti sulla banca tramite cui ricevere il pagamento:
   - Nome del titolare del conto bancario
   - Numero di routing
   - Numero conto
   - Tipo di conto bancario

   > **Note**
   >
   > Se utilizzi un conto bancario aziendale, ti verrà richiesto di inviare le informazioni relative al conto bancario via fax (1-206-765-3424).

Dopo la registrazione, il conto bancario fornito viene impostato come predefinito, in attesa di verifica con la banca. La verifica di un nuovo conto bancario può richiedere fino a due settimane, durante le quali non è possibile ricevere alcun pagamento. In caso di conto costituito, i pagamenti richiedono in genere circa due giorni.

Per modificare il conto bancario predefinito per il pagamento

1. Nella pagina per la Registrazione dei venditori nel Marketplace delle istanze riservate, accedere con l'account utilizzato per la registrazione.

2. Nella pagina Manage Bank Account (Gestisci conto bancario), aggiungere un nuovo conto bancario o modificare il conto predefinito secondo necessità.

Informazioni fiscali

La vendita di elementi di Istanze riservate potrebbe essere soggetta a un'imposta basata sulle transazioni, come un'imposta sulle vendite o un'imposta sul valore aggiunto. È necessario consultare il reparto fiscale, legale, finanziario o contabile dell'azienda per stabilire se vi sono imposte basate sulle transazioni applicabili. Sei tenuto a riscuotere e inviare tali imposte sulle transazioni alla opportuna autorità fiscale.

Come parte del processo di registrazione dei venditori, è necessario completare un questionario fiscale nel portale di registrazione dei venditori. Il colloquio raccoglie le informazioni fiscali e compila un modulo IRS, o W-9 W-8BEN, che viene utilizzato per determinare gli eventuali obblighi di dichiarazione fiscale W-8BEN-E necessari.

Le informazioni di natura fiscale indicate come parte del questionario fiscale possono differire a seconda che operi in forma individuale o come impresa e che l'azienda sia una persona fisica o giuridica statunitense o meno. Quando si compila il questionario fiscale, è necessario tenere presente quanto segue:

- Le informazioni fornite da AWS, incluse le informazioni in questo argomento, non costituiscono consulenza fiscale, legale o di altro tipo. Per scoprire in che modo i requisiti di dichiarazione IRS possono influire sull'azienda, o in caso di altre domande, contattare il proprio consulente fiscale, legale o di altra natura professionale.
- Per soddisfare tali requisiti nella massima misura possibile, rispondere a tutte le domande e inserire tutte le informazioni richieste durante il questionario.
- Controllare le risposte. Evitare errori ortografici o di inserire numeri di identificazione fiscale errati. Ciò potrebbe comportare l'invalidazione del modulo fiscale.

In base alle risposte del questionario fiscale e alle soglie di dichiarazione dell'IRS, Amazon può presentare il modulo 1099-K, che invia per posta entro il 31 gennaio dell'anno seguente a quello in cui il tuo conto fiscale ha raggiunto i livelli di soglia. Ad esempio, se il conto raggiunge la soglia nel 2018, il modulo 1099-K viene inviato entro il 31 gennaio 2019.

Per ulteriori informazioni sui requisiti IRS e sul modulo 1099-K, consulta le domande frequenti Form 1099-K FAQs nel sito web IRS.

Dare un prezzo alla Istanze riservate

Durante la definizione del prezzo per le istanze riservate, considera quanto segue:

- Costo anticipato - Il costo anticipato è l'unica tariffa che puoi specificare per l'Istanza riservata che stai vendendo. Il costo anticipato è l'unico singolo addebito che l'acquirente paga per l'acquisto di ogni istanza riservata.

  Poiché il valore delle istanze riservate diminuisce nel tempo, per impostazione predefinita, è AWS possibile impostare una diminuzione dei prezzi con incrementi uguali mese dopo mese. Tuttavia, puoi stabilire diversi prezzi iniziali in base a quando viene venduta la prenotazione. Ad esempio se l'Istanza riservata ha una validità residua di nove mesi, puoi specificare l'importo che accetteresti se un cliente acquistasse tale Istanza riservata con una validità di nove mesi. Puoi stabilire un altro prezzo con una validità di cinque mesi e un altro ancora con un mese di validità.

  Il prezzo minimo consentito nel Marketplace delle istanze riservate è 0 USD.
- Limiti - I seguenti limiti per la vendita di istanze riservate si applicano per tutta la durata della tua Account AWS. Non si tratta di limiti annuali e non possono essere aumentati.
  - Puoi effettuare vendite fino a 50.000 USD in Istanze riservate.
  - Puoi effettuare vendite fino a 5.000 USD in Istanze riservate.
- Impossibile modificare - Non puoi modificare l'elenco direttamente. Tuttavia, puoi farlo annullandolo e successivamente creandone un altro con nuovi parametri.
- Cancellazione - Puoi annullare il tuo elenco in qualsiasi momento purché il relativo stato sia `active`. Non puoi annullare l'elenco se già oggetto di corrispondenza o in corso di elaborazione per una vendita. In caso di annullamento di un elenco contenente alcune istanze oggetto di corrispondenza, saranno rimosse da tale elenco solo le istanze non oggetto di corrispondenza.

Elencare le Istanze riservate

In qualità di venditore registrato, puoi decidere di vendere uno o più elementi di Istanze riservate. Puoi decidere di venderli tutti in un elenco o in più parti. Inoltre, puoi elencare elementi di Istanze riservate con qualsiasi configurazione di tipo di istanza, piattaforma e ambito.

La console determina un prezzo consigliato. Verifica le offerte che corrispondono alle Istanza riservata e mette in corrispondenza quella con il prezzo più basso. Altrimenti, calcola un prezzo consigliato in base al costo delle Istanza riservata per il tempo restante. Se il valore calcolato è inferiore a $1,01, il prezzo consigliato è $1,01.

Se annulli l'elenco e una parte di esso è già stato venduto, l'annullamento non viene applicato alla parte già venduta. Solo la parte invenduta dell'inserzione non è più disponibile nel Marketplace delle istanze riservate.

Console

Come pubblicare un'istanza riservata nel Marketplace delle istanze riservate

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Seleziona le Istanze riservate da elencare e scegli Actions (Operazioni), Sell Reserved Instances (Vendi le Istanze riservate).
4. Nella pagina Configure Your Istanza riservata Listing (Configura l'elenco di) impostare il numero di istanze da vendere e il prezzo iniziale per la validità residua nelle colonne corrispondenti. Per vedere in che modo cambia il valore della prenotazione nel periodo di validità residua, selezionare la freccia accanto alla colonna Months Remaining (Mesi rimanenti).
5. Gli utenti avanzati che desiderano personalizzare i prezzi, possono immettere valori diversi per i mesi successivi. Per tornare al decremento dei prezzi lineare predefinito, scegliere Reset (Reimposta).
6. Al termine della configurazione dell'elenco, scegliere Continue (Continua).
7. Confermare i dettagli dell'elenco nella pagina Confirm Your Istanza riservata Listing (Conferma l'elenco di) e, se non è necessario apportare modifiche, scegliere List Reserved Instance (Elenca istanza riservata).

Per visualizzare le inserzioni nella console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Seleziona l'Istanza riservata elencata e scegli la scheda Le My Listings (I miei elenchi) nella parte inferiore della pagina.

AWS CLI

Per gestire le istanze riservate nel Marketplace delle istanze riservate

1. Per ottenere l'elenco delle Istanze riservate, utilizzare il comando describe-reserved-instances. Annota l'ID dell'istanza riservata che desideri pubblicare.
2. Usa il comando create-reserved-instances-listing. È necessario specificare l'ID dell'Istanza riservata, il numero di istanze e il piano dei prezzi.
3. Per visualizzare l'elenco, utilizzare il comando describe-reserved-instances-listings.
4. Per annullare l'inserzione, usa il comando cancel-reserved-instances-listing.

PowerShell

Per gestire le istanze riservate nel Marketplace delle istanze riservate

1. Ottieni un elenco delle tue istanze riservate utilizzando il cmdlet. Get-EC2ReservedInstance Annota l'ID dell'istanza riservata che desideri pubblicare.
2. Utilizza il cmdlet New-EC2ReservedInstancesListing. È necessario specificare l'ID dell'Istanza riservata, il numero di istanze e il piano dei prezzi.
3. Per visualizzare l'elenco, utilizza il cmdlet. Get-EC2ReservedInstancesListing
4. Per cancellare la tua inserzione, usa il Stop-EC2ReservedInstancesListing cmdlet.

Stato dell'elenco d'Istanza riservata

L'opzione Listing State (Stato elenco) nella scheda My Listings (I miei elenchi) della pagina delle Istanze riservate mostra lo stato corrente degli elenchi:

Le informazioni visualizzate in Listing State (Stato inserzione) riguardano lo stato dell'inserzione nel Marketplace delle istanze riservate. Sono diverse dalle informazioni di stato mostrate nella colonna State (Stato) nella pagina Reserved Instances (Istanze riservate). Le informazioni in State (Stato) riguardano la prenotazione.

- active (attivo) — L'elenco è disponibile per l'acquisto.
- canceled (annullata) - L'inserzione è stata annullata e non è disponibile per l'acquisto nel Marketplace delle istanze riservate.
- closed (chiuso) — L'Istanza riservata non è inclusa nell'elenco. Un'Istanza riservata potrebbe essere `closed` perché la vendita dell'elenco è stata completata.

Ciclo di vita di un elenco

Quando tutte le istanze in elenco corrispondono e risultano vendute, la scheda My Listings (I miei elenchi) mostra una corrispondenza tra Total instance count (Conteggio totale delle istanze) e il conteggio elencato in Sold (Venduto). Inoltre, non c'è alcuna istanza Available (Disponibile) per l'elenco e il suo Status (Stato) è `closed`.

Quando viene venduta solo una parte dell'offerta, le istanze riservate AWS presenti nell'elenco vengono ritirate e viene creato un numero di istanze riservate pari alle istanze riservate rimanenti nel conteggio. Pertanto, l'ID elenco e l'elenco che rappresenta, che ora include meno prenotazioni per la vendita, è ancora attivo.

Eventuali vendite future di elementi di Istanze riservate in questo elenco sono elaborate in questo modo. Quando tutte le istanze riservate presenti nell'elenco vengono vendute, AWS contrassegna l'inserzione come. `closed`

Ad esempio, puoi creare un elenco ID di elenco di Istanze riservate 5ec28771-05ff-4b9b-aa31-9e57dexample con un conteggio pari a 5.

La scheda My Listings (I miei elenchi) nella pagina della console Reserved Instance (Istanza riservata) visualizza l'elenco in questo modo:

ID di elenco di Istanza riservata 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count (Conteggio totale delle prenotazioni) = 5
- Sold (Venduto) = 0
- Available (Disponibile) = 5
- Status (Stato) = active (attivo)

Un acquirente compra due delle prenotazioni, lasciando un conteggio di tre prenotazioni ancora disponibili per la vendita. A causa di questa vendita parziale, AWS crea una nuova prenotazione contando fino a tre per rappresentare le prenotazioni rimanenti ancora in vendita.

Questo è l'aspetto che avrebbe l'elenco nella scheda My Listings (I miei elenchi):

ID di elenco di Istanza riservata 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count (Conteggio totale delle prenotazioni) = 5

- Sold (Venduto) = 2
- Available (Disponibile) = 3
- Status (Stato) = active (attivo)

Se annulli l'elenco e una parte di esso è già stato venduto, l'annullamento non viene applicato alla parte già venduta. Solo la parte invenduta dell'inserzione non è più disponibile nel Marketplace delle istanze riservate.

Dopo la vendita della Istanza riservata

Quando la tua istanza riservata viene venduta, ti AWS invia una notifica via email. Vieni avvisato tramite notifica via e-mail di tutte le attività che si verificano in una giornata. Le attività possono includere la creazione o la vendita di un'inserzione o l' AWS invio di fondi al tuo account.

Console

Per monitorare lo stato dell'inserzione di un'istanza riservata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella pagina di navigazione scegli Reserved Instances (Istanze riservate).
3. Nella scheda I miei elenchi, trova il valore di Stato elenco. La scheda contiene anche informazioni su termine, prezzo di listino e suddivisione del numero di istanze dell'inserzione disponibili, in attesa, vendute e annullate.

AWS CLI

Per monitorare lo stato dell'inserzione di un'istanza riservata

Usa il comando describe-reserved-instances-listings con il filtro adeguato per ottenere informazioni sulle inserzioni.

```
aws ec2 describe-reserved-instances-listings
```

PowerShell

Per monitorare lo stato dell'inserzione di un'istanza riservata

Utilizza il cmdlet Get-EC2ReservedInstancesListing.

```
Get-EC2ReservedInstancesListing
```

Ricezione dei pagamenti

Non appena AWS riceve i fondi dall'acquirente, viene inviato un messaggio all'indirizzo e-mail del proprietario registrato relativo all'Istanza riservata venduta.

AWS invia un bonifico bancario Automated Clearing House (ACH) sul conto bancario specificato. In genere, questo bonifico viene effettuato in da uno a tre giorni dopo la vendita della Istanza riservata. I pagamenti vengono effettuati una volta al giorno. Riceverai un'e-mail con le informazioni di pagamento una volta erogati i fondi. Tieni presente che non puoi ricevere i pagamenti finché AWS non ricevi la verifica dalla tua banca. Ciò può richiedere fino a due settimane.

L'Istanza riservata venduta continua a comparire quando descrivi le tue Istanze riservate.

Riceverai un rimborso in contanti per le istanze riservate tramite un bonifico bancario direttamente sul tuo conto bancario. AWS addebita una commissione di servizio pari al 12% del prezzo totale anticipato di ogni Istanza riservata venduta nel Reserved Instance Marketplace.

Informazioni condivise con l'acquirente

Quando vendi nel Reserved Instance Marketplace, AWS condivide il nome legale della tua azienda sulla dichiarazione dell'acquirente in conformità con le normative statunitensi. Inoltre se l'acquirente chiama il Supporto perché ha la necessità di contattarti per una fattura o per questioni fiscali, AWS potrebbe dover fornire all'acquirente il tuo indirizzo e-mail in modo da contattarti direttamente.

Per motivi simili, il codice fiscale dell'acquirente e le informazioni sul paese vengono fornite al venditore nel report di pagamento. In qualità di venditore, potresti aver bisogno di queste informazioni a corredo di qualsiasi imposta sulle transazioni corrisposta al governo (come l'imposta sulle vendite e l'imposta sul valore aggiunto).

AWS non può offrire consulenza fiscale, ma se il tuo esperto fiscale stabilisce che hai bisogno di informazioni aggiuntive specifiche, contattaci Supporto.

Modificare le Istanze riservate

Quando le tue esigenze cambiano, puoi modificare i tuoi elementi di Istanze riservate modificabili o standard e continuare a beneficiare del vantaggio di fatturazione. Puoi modificare gli attributi quali la

zona di disponibilità, le dimensioni dell'istanza (nella stessa famiglia di istanze) e l'ambito dell'istanza riservata.

> **Note**
>
> Puoi inoltre scambiare una Istanza riservata modificabile con un'altra Istanza riservata modificabile con una configurazione diversa. Per ulteriori informazioni, consulta Scambiare le Istanze riservate modificabili.

Puoi modificare tutti gli elementi di Istanze riservate o un sottoinsieme di essi. Puoi separare le Istanze riservate originali in due o più Istanze riservate nuove. Ad esempio, se hai una prenotazione per 10 istanze in `us-east-1a` e decidi di spostarne 5 in `us-east-1b`, la richiesta di modifica determina due nuove prenotazioni: una per 5 istanze in `us-east-1a` e un'altra per 5 istanze in `us-east-1b`.

Puoi inoltre unire due o più Istanze riservate in una singola Istanza riservata. Ad esempio, se hai quattro Istanze riservate `t2.small` di un'istanza ciascuna, puoi unirli per creare un'unica Istanza riservata `t2.large`. Per ulteriori informazioni, consulta Supporto per la modifica delle dimensioni dell'istanza.

Dopo la modifica, il vantaggio degli elementi di Istanze riservate viene applicato solo alle istanze corrispondenti ai nuovi parametri. Ad esempio, se cambi la zona di disponibilità di una prenotazione, la prenotazione di capacità e i vantaggi in termini di prezzi vengono automaticamente applicati all'utilizzo dell'istanza nella nuova zona di disponibilità. Le istanze che non corrispondono più ai nuovi parametri vengono addebitate in base alla On-Demand tariffa, a meno che il tuo account non abbia altre prenotazioni applicabili.

Se la tua richiesta di modifica viene applicata

- La prenotazione modificata diventa effettiva immediatamente e il vantaggio di prezzo viene applicato alle nuove istanze a partire dall'ora della richiesta di modifica. Ad esempio, se modifichi correttamente le prenotazioni alle 21:15, il vantaggio di prezzo si trasferisce alla nuova istanza alle 21:00. Puoi ottenere la data effettiva della Istanze riservate modificata utilizzando il comando describe-reserved-instances.
- La prenotazione originale viene ritirata. La sue data di fine coincide con la data di inizio della nuova prenotazione e la data di fine della nuova prenotazione è la stessa della data di fine della Istanza riservata originale. Se modifichi una prenotazione di tre anni con una validità residua di 16 mesi,

la prenotazione modificata risultante è una prenotazione di 16 mesi con la stessa data di fine dell'originale.

- La prenotazione modificata indica un prezzo fisso di 0 USD e non quello della prenotazione originale.
- Il prezzo fisso della prenotazione modificata non influisce sui calcoli del livello di prezzi di sconto applicati al tuo account, che si basano sul prezzo fisso della prenotazione originale.

Se la richiesta di modifica genera un errore, gli elementi di Istanze riservate mantengono la configurazione originale e sono immediatamente disponibili per un'altra richiesta di modifica.

Non è previsto alcun costo per la modifica e non ricevi alcuna fattura nuova.

Puoi modificare le prenotazione alla frequenza che desideri, ma non puoi cambiare o annullare una richiesta di modifica in attesa dopo averla inviata. Dopo che la modifica è stata completata correttamente, puoi inviare un'altra richiesta di modifica per eseguire il rollback di qualsiasi modifica eseguita, se necessario.

Indice

- Requisiti e restrizioni per la modifica
- Supporto per la modifica delle dimensioni dell'istanza
- Inviare richieste di modifica
- Risoluzione dei problemi relativi alle richieste di modifica

Requisiti e restrizioni per la modifica

Puoi modificare tali attributi nel modo seguente.

Attributo modificabile	Piattaforme supportate	Considerazioni e limitazioni
Cambiare le zone di disponibilità all'interno della stessa regione	Linux e Windows	-
	Linux e Windows	Un'istanza riservata zonale viene assegnata a una zona

Attributo modificabile	Piattaforme supportate	Considerazioni e limitazioni
Cambiare l'ambito di applicazione dalla zona di disponibilità alla regione e viceversa		di disponibilità e riserva la capacità in quella zona di disponibilità. Se cambi l'ambito di applicazione da zona di disponibilità a regione (in altre parole, da zonale a regionale), perdi il vantaggio della prenotazione della capacità. Un'istanza riservata regionale viene assegnata a una regione. Lo sconto dell'Istanza riservata si applica alle istanze in esecuzione in qualsiasi zona di disponibilità di quella regione. Inoltre, lo discount dell'istanza riservata si applica all'utilizzo dell'istanza su tutte le dimensioni della stessa famiglia di istanze selezionata. Se cambi l'ambito di applicazione da regione a zona di disponibilità (in altre parole, da regionale a zonale), perdi la flessibilità della zona di disponibilità e della dimensione dell'istanza (se applicabile). Per ulteriori informazioni, consulta Applicazione degli sconti sulle istanze riservate.

Attributo modificabile	Piattaforme supportate	Considerazioni e limitazioni
Cambia la dimensione dell'istanza all'interno della stessa famiglia e generazione di istanze.	Linux/UNIX solo La flessibilità delle dimensioni delle istanze non è disponibile per Istanze riservate su altre piattaforme, tra le quali Linux con SQL Server Standard, Linux con SQL Server Web, Linux con SQL Server Enterprise, Red Hat Enterprise Linux, SUSE Linux, Windows, Windows con SQL Standard, Windows con SQL Server Enterprise e Windows con SQL Server Web.	La prenotazione deve utilizzare la tenancy predefinita. Alcune famiglie di istanze non sono supportate perché non sono disponibili altre dimensioni. Per ulteriori informazioni, consulta Supporto per la modifica delle dimensioni dell'istanza

Requisiti

Amazon EC2 elabora la richiesta di modifica se è disponibile una capacità sufficiente per la nuova configurazione (se applicabile) e se sono soddisfatte le condizioni seguenti:

- Le Istanza riservata non possono essere modificate prima o al momento del relativo acquisto
- La Istanza riservata deve essere attiva
- Non possono esserci richieste di modifica in sospeso
- L'istanza riservata non è più elencata nel Marketplace delle istanze riservate.
- Deve esserci corrispondenza tra il footprint associato alla dimensione dell'istanza della prenotazione originale e la nuova configurazione. Per ulteriori informazioni, consulta Supporto per la modifica delle dimensioni dell'istanza.
- Le Istanze riservate originali sonno tutte Istanze riservate Standard o tutte Istanze riservate modificabili, non alcune di ogni tipo
- Le Istanze riservate originali devono scadere entro lo stesso orario, se sono Istanze riservate Standard

- Per modificare la dimensione dell'istanza, l'istanza riservata deve supportare la flessibilità delle dimensioni delle istanze. Consulta Flessibilità dimensioni istanza per l'elenco delle istanze riservate che non supportano la flessibilità delle dimensioni delle istanze.

Supporto per la modifica delle dimensioni dell'istanza

È possibile modificare la dimensione dell'istanza di una Istanza riservata se sono soddisfatti i seguenti requisiti.

Requisiti

- La piattaforma è Linux/UNIX.
- Devi selezionare un'altra dimensione di istanza nella stessa famiglia di istanze (indicata da una lettera, ad esempio T) e generazione (indicata da un numero, ad esempio 2).

  Ad esempio, puoi modificare un'istanza riservata da `t2.small` a `t2.large` perché appartengono entrambe alla stessa famiglia e generazione T2. Tuttavia, non è possibile modificare un'istanza riservata da T2 a M2 o da T2 a T3, poiché in entrambi i casi, la famiglia e la generazione dell'istanza di destinazione non sono le stesse di quelle dell'istanza riservata originale.
- Puoi modificare la dimensione dell'istanza di un'istanza riservata solo se supporta la flessibilità delle dimensioni delle istanze. Consulta Flessibilità dimensioni istanza per l'elenco delle istanze riservate che non supportano la flessibilità delle dimensioni delle istanze.
- Non puoi modificare le dimensioni delle istanze riservate per le istanze `t1.micro`, poiché `t1.micro` ha una sola dimensione.
- La Istanza riservata originale e quella nuova devono avere la stessa impronta dell'istanza.

Indice

- Impronta dimensione istanza
- Fattori di normalizzazione per le istanze bare metal

Impronta dimensione istanza

Ciascuna Istanza riservata ha un'impronta associata alla dimensione dell'istanza, determinato dal fattore di normalizzazione della dimensione di istanza e dal numero di istanze nella prenotazione. Quando modifichi le dimensioni di istanza in una Istanza riservata, l'impronta della nuova

configurazione deve corrispondere a quella della configurazione originale, altrimenti la richiesta di modifica non viene elaborata.

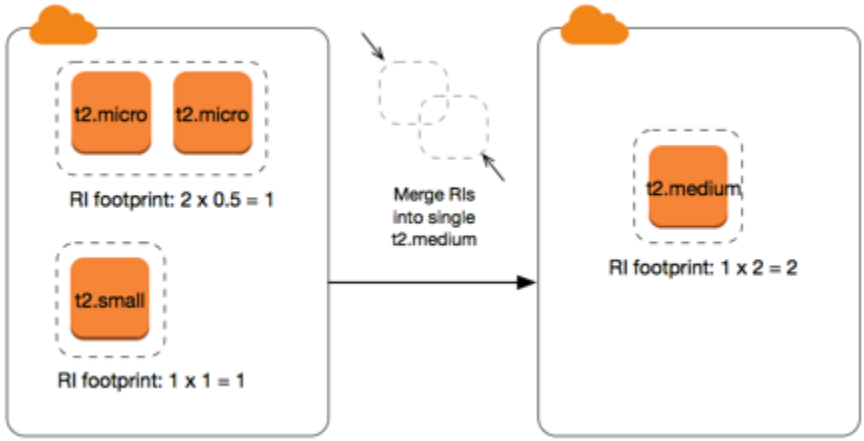
Per calcolare il footprint della dimensione dell'istanza di una Istanza riservata, moltiplica il numero di istanza per il fattore di normalizzazione. Nella console Amazon EC2, il fattore di normalizzazione si misura in unità. Nella tabella seguente viene descritto il fattore di normalizzazione per le dimensioni delle istanze in una famiglia di istanze. Ad esempio, `t2.medium` ha un fattore di normalizzazione 2, quindi una prenotazione per quattro istanze `t2.medium` ha un'impronta di 8 unità.

Dimensioni istanza	Fattore di normalizzazione
nano	0.25
micro	0,5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128

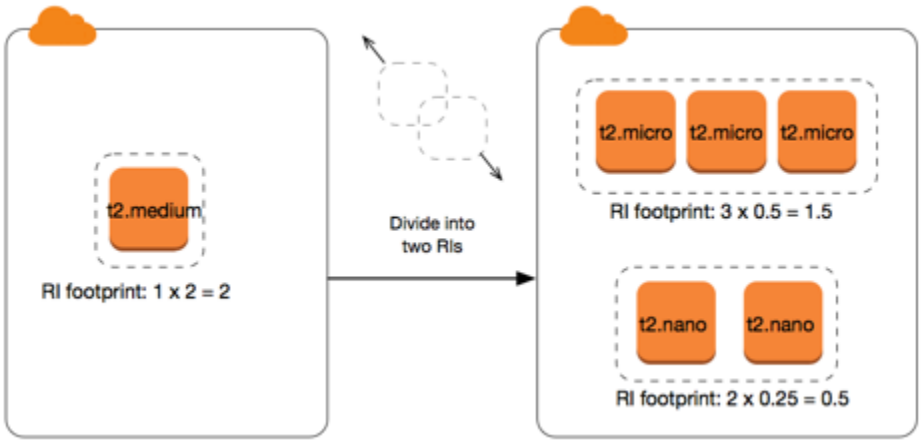
Dimensioni istanza	Fattore di normalizzazione
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
96xlarge	768
112xlarge	896

Puoi allocare le prenotazioni in diverse dimensioni di istanza nella stessa famiglia di istanze purché l'impronta della dimensione dell'istanza della prenotazione rimanga invariata. Ad esempio, è possibile dividere una prenotazione per un'istanza `t2.large` (1 @ 4 unità) in quattro istanze `t2.small` (4 @ 1 unità). Analogamente, è possibile combinare una prenotazione per quattro istanze `t2.small` in un'unica istanza `t2.large`. Tuttavia, non è possibile modificare la prenotazione per due istanze `t2.small` in un'istanza `t2.large` perché l'impronta della nuova prenotazione (4 unità) è maggiore dell'impronta della prenotazione originale (2 unità).

Nell'esempio seguente si dispone di una prenotazione con due istanze `t2.micro` (1 unità) e una prenotazione con un'istanza `t2.small` (1 unità). Se si uniscono entrambe le prenotazioni a una singola prenotazione con un'istanza `t2.medium` (2 unità), l'impronta della nuova prenotazione equivale all'impronta delle prenotazioni combinate.



Puoi inoltre modificare una prenotazione per dividerla in due o più prenotazioni. Nell'esempio seguente, hai una prenotazione con un'istanza `t2.medium` (2 unità). È possibile dividere la prenotazione in due, una con due istanze `t2.nano` (.5 unità) e l'altra con tre istanze `t2.micro` (1,5 unità).



Fattori di normalizzazione per le istanze bare metal

È possibile modificare una prenotazione con istanze `metal` che utilizzano altre dimensioni all'interno della stessa famiglia di istanze. Analogamente, puoi modificare una prenotazione con varianti diverse da quelle bare metal utilizzando le dimensioni `metal` all'interno della stessa famiglia di istanze. Generalmente, un'istanza bare metal ha la stessa dimensione della più grande dimensione disponibile all'interno della stessa famiglia di istanze. Ad esempio, un'istanza `i3.metal` ha le stesse dimensioni di un'istanza `i3.16xlarge`, quindi hanno lo stesso fattore di normalizzazione.

Nella tabella seguente viene descritto il fattore di normalizzazione per le dimensioni delle istanze bare metal nelle famiglie di istanze con istanze bare metal. Il fattore di normalizzazione per `metal` le istanze dipende dalla famiglia di istanze, a differenza delle altre dimensioni di istanza.

Dimensioni istanza	Fattore di normalizzazione
`a1.metal`	32
`m5zn.metal` | `x2iezn.metal` `z1d.metal`	96
`c6g.metal` | `c6gd.metal` | `i3.metal` | `m6g.metal` | `m6gd.metal` | `r6g.metal` | `r6gd.metal` | `x2gd.metal`	128

Dimensioni istanza	Fattore di normalizzazione
c5n.metal	144
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-18tb1.metal | u-24tb1.metal	448
u-6tb1.metal | u-9tb1.metal | u-12tb1.metal	896

Ad esempio, il fattore di normalizzazione di un'istanza `i3.metal` è 128. Se acquisti un'istanza Linux/Unix riservata Amazon con contratto di locazione `i3.metal` predefinito, puoi suddividere la prenotazione come segue:

- An `i3.16xlarge` ha le stesse dimensioni di un'`i3.metal`istanza, quindi il suo fattore di normalizzazione è 128 ()128/1. La prenotazione per una istanza `i3.metal` non può essere modificata in una istanza `i3.16xlarge`.
- An `i3.8xlarge` è la metà delle dimensioni di un'`i3.metal`istanza, quindi il suo fattore di normalizzazione è 64 ()128/2. La prenotazione per una istanza `i3.metal` non può essere divisa in due istanze `i3.8xlarge`.
- An `i3.4xlarge` è un quarto della dimensione di un'`i3.metal`istanza, quindi il suo fattore di normalizzazione è 32 ()128/4. La prenotazione per una istanza `i3.metal` non può essere divisa in quattro istanze `i3.4xlarge`.

Inviare richieste di modifica

Prima di modificare le istanze riservate, assicurati di aver letto le restrizioni applicabili. Prima di modificare la dimensione dell'istanza, calcola l'ingombro della dimensione dell'istanza totale delle prenotazioni originali che intendi modificare e assicurati che corrisponda a quello delle nuove configurazioni.

Console

Per modificare le istanze riservate

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella pagina Reserved Instances (Istanze riservate), selezionare una o più Istanze riservate da modificare e scegliere Actions (Azioni), Modify Reserved Instances (Modifica istanze riservate).

   Se le Istanze riservate non sono nello stato attivo o non possono essere modificate, l'opzione Modify Istanze riservate (Modifica Istanze riservate) è disabilitata.
3. La prima voce nella tabella di modifica indica gli attributi delle Istanze riservate selezionate e almeno una configurazione di destinazione al di sotto. La colonna Units (unità) mostra il footprint della dimensione dell'istanza totale. Selezionare Add (Aggiungi) per ciascuna nuova configurazione da aggiungere. Modificare gli attributi in base alle esigenze per ogni configurazione.

   - Scope (Ambito di applicazione): scegliere se la configurazione si applica a una zona di disponibilità o all'intera regione.
   - Availability Zone (Zona di disponibilità): scegliere la zona di disponibilità richiesta. Non applicabile agli elementi di Istanze riservate regionali.
   - Tipo di istanza: seleziona il tipo di istanza richiesto. Le configurazioni combinate devono avere un footprint delle dimensioni di istanza pari alle configurazioni originali.
   - Count (Conteggio): specificare il numero di istanze. Per dividere le Istanze riservate in più configurazioni, ridurre il conteggio, scegliere Add (Aggiungi) e specificare un conteggio per la configurazione aggiuntiva. Ad esempio, se si ha una singola configurazione con un conteggio di 10, è possibile impostare il relativo conteggio su 6 e aggiungere una configurazione con un conteggio di 4. In questo modo, l'Istanza riservata originale viene ritirata dopo l'attivazione della nuova Istanze riservate.
4. Scegliere Continue (Continua).
5. Per confermare le scelte di modifica dopo aver terminato di specificare le configurazioni di destinazione, scegliere Submit Modifications (Invia modifiche).
6. Puoi determinare lo stato della richiesta di modifica osservando la colonna State (Stato) nella schermata delle Istanze riservate. Di seguito sono riportati gli stati possibili.

   - attiva (modifica in sospeso) – Stato della transizione per la Istanze riservate di origine

- ritirata (modifica in sospeso) – Stato della transizione per la Istanze riservate di origine mentre vengono create le nuove Istanze riservate
- ritirata – Istanze riservate modificata e sostituita con successo
- attiva – Una delle seguenti opzioni:
  - Nuovi elementi di Istanze riservate creati da una richiesta di modifica corretta
  - Elementi di Istanze riservate originali dopo una richiesta di modifica errata

AWS CLI

Per modificare le istanze riservate

Usa il comando modify-reserved-instances. Puoi fornire i dettagli di configurazione in un file JSON.

```
aws ec2 modify-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342f5bd7c02 \
    --target-configurations file://configuration.json
```

Per ottenere lo stato della richiesta di modifica

Usa il comando describe-reserved-instances-modifications. Lo stato è `processing`, `fulfilled` o `failed`.

```
aws ec2 describe-reserved-instances-modifications \
    --reserved-instances-modification-ids rimod-d3ed4335-b1d3-4de6-ab31-0f13aaf46687
 \
    --query ReservedInstancesModifications[].Status
```

PowerShell

Per modificare le istanze riservate

Utilizza il cmdlet Edit-EC2ReservedInstance. Puoi fornire i dettagli di configurazione in un oggetto di tipo `Amazon.EC2.Model.ReservedInstancesConfiguration`.

```
Edit-EC2ReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342f5bd7c02 `
    -TargetConfiguration $configuration
```

Per ottenere lo stato della richiesta di modifica

Utilizza il cmdlet Get-EC2ReservedInstancesModification. Lo stato è `processing`, `fulfilled` o `failed`.

```
Get-EC2ReservedInstancesModification `
    -ReservedInstancesModificationId rimod-d3ed4335-b1d3-4de6-ab31-0f13aaf46687 | `
    Select Status
```

Risoluzione dei problemi relativi alle richieste di modifica

Se le impostazioni della configurazione di destinazione richieste erano univoche, riceverai un messaggio indicante che si sta elaborando la richiesta. In questa fase, Amazon EC2 ha solo stabilito che i parametri della richiesta di modifica siano validi. La richiesta di modifica può sempre generare un errore durante l'elaborazione se non è disponibile la capacità necessaria.

In alcune situazioni, potresti ricevere un messaggio indicante richieste di modifica incomplete o errate invece di una conferma. Utilizza le informazioni incluse in tali messaggi come punto iniziale per inviare nuovamente un'altra richiesta di modifica. Assicurati di aver letto le restrizioni applicabili prima di inviare la richiesta.

Non tutti gli elementi di Istanze riservate selezionati possono essere elaborati per la modifica

Amazon EC2 identifica ed elenca le Istanze riservate che non possono essere modificate. Se ricevi un messaggio di questo tipo, vai alla pagina Reserved Instances (Istanze riservate) nella console di Amazon EC2 e controlla le informazioni per le Istanze riservate.

Errore durante l'elaborazione della richiesta di modifica

Hai richiesto la modifica di uno o più elementi di Istanze riservate ma nessuna delle richieste può essere elaborata. In base al numero di prenotazioni modificate, puoi ottenere versioni diverse del messaggio.

Amazon EC2 mostra le ragioni per cui la richiesta non può essere elaborata. Ad esempio, potresti aver specificato la stessa configurazione di destinazione (una combinazione di zona di disponibilità e piattaforma) per uno o più sottoinsiemi delle Istanze riservate che stai modificando. Prova a inviare nuovamente le richieste di modifica, ma assicurati che i dettagli dell'istanza delle prenotazioni coincidano e che le configurazioni di destinazione per tutti i sottoinsiemi modificati siano univoci.

Scambiare le Istanze riservate modificabili

Puoi scambiare una o più Istanze riservate modificabili con un'altra Istanza riservata modificabile caratterizzata da una diversa configurazione, inclusa la famiglia di istanze, il sistema operativo e la tenancy. Non ci sono limiti al numero di scambi che puoi effettuare, purché la nuova istanza riservata modificabile abbia un valore pari o superiore alle istanze riservate modificabili che stai scambiando.

Quando scambi l'Istanza riservata modificabile, il numero di istanze per la prenotazione corrente viene scambiato con un numero di istanze che copre un valore pari o superiore alla configurazione della nuova istanza riservata modificabile. Amazon EC2 calcola il numero di istanze riservate che puoi ricevere a seguito dello scambio.

Non è possibile scambiare Istanze riservate Standard, ma è possibile modificarle. Per ulteriori informazioni, consulta Modificare le Istanze riservate.

Indice

- Requisiti per lo scambio di elementi di Istanze riservate modificabili
- Calcolare gli scambi di Istanze riservate modificabili
- Unire le Istanze riservate modificabili
- Scambiare una parte di una Istanza riservata modificabile
- Inviare richieste di scambio

Requisiti per lo scambio di elementi di Istanze riservate modificabili

Se sono soddisfatte le condizioni seguenti, Amazon EC2 elabora la tua richiesta di scambio. La Istanza riservata modificabile deve essere:

- Attivo
- Priva di una richiesta di scambio precedente
- Con tempo residuo di almeno 24 ore prima della scadenza

Si applicano le regole seguenti:

- Le istanze riservate modificabili devono essere scambiate con altre istanze riservate modificabili attualmente offerte da AWS.

- Gli elementi di Istanze riservate modificabili sono associati a una regione specifica, che resta invariata per la durata del periodo della prenotazione. Non puoi scambiare un'istanza riservata modificabile con un'altra istanza riservata modificabile in una Regione diversa.
- Per scambiare un'istanza riservata convertibile zonale, è AWS necessario disporre di una capacità sufficiente per il nuovo tipo di istanza nella regione.
- Puoi scambiare una o più Istanze riservate modificabili alla volta con una sola Istanza riservata modificabile.
- Puoi scambiare una parte di un'Istanza riservata modificabile, modificarle in due o più prenotazioni e quindi scambiare una o più prenotazioni con una nuova Istanza riservata modificabile. Per ulteriori informazioni, consulta Scambiare una parte di una Istanza riservata modificabile. Per ulteriori informazioni sulla modifica delle Istanze riservate, consulta Modificare le Istanze riservate.
- Tutte le Istanze riservate modificabili con pagamento anticipato possono essere scambiate con Istanze riservate modificabili con pagamento anticipato parziale e viceversa.

> **Note**
>
> Se il pagamento anticipato totale richiesto per lo scambio (costo effettivo) è inferiore a 0,00 USD, ti viene AWS automaticamente assegnato un numero di istanze nell'istanza riservata convertibile tale da garantire che il costo effettivo sia pari o superiore a 0,00 USD.

> **Note**
>
> Se il valore totale (prezzo anticipato + prezzo orario * numero di ore rimanenti) della nuova istanza riservata convertibile è inferiore al valore totale dell'istanza riservata convertibile scambiata, ti fornisce AWS automaticamente una quantità di istanze nell'istanza riservata convertibile che garantisce che il valore totale sia uguale o superiore a quello dell'istanza riservata convertibile scambiata.

- Per beneficiare di un prezzo migliore, puoi scambiare un'Istanza riservata modificabile senza pagamento anticipato con un'Istanza riservata modificabile con pagamento anticipato totale o parziale.
- Non puoi scambiare tutte le Istanze riservate modificabili con pagamento anticipato totale e parziale con Istanze riservate modificabili senza pagamento anticipato.

- Puoi scambiare un'Istanza riservata modificabile senza pagamento anticipato con un'altra Istanza riservata modificabile senza pagamento anticipato solo se il prezzo orario della nuova Istanza riservata modificabile è identico o superiore a quello della Istanza riservata modificabile scambiata.

  > **Note**
  >
  > Se il valore totale (tariffa oraria * numero di ore residue) della nuova istanza riservata modificabile è inferiore al valore totale dell'istanza riservata modificabile scambiata, AWS ti fornisce automaticamente una quantità di istanze nell'istanza riservata modificabile che assicura che il valore totale sia lo stesso o superiore a quello dell'istanza riservata modificabile.

- Se scambi più Istanze riservate modificabili con date di scadenza differenti, la data di scadenza della nuova Istanza riservata modificabile sarà la più lontana nel futuro.
- Se scambi una singola Istanza riservata modificabile, questa deve avere la stessa durata (1 o 3 anni) della nuova Istanza riservata modificabile. Se unisci più Istanze riservate modificabili di diversa durata, la nuova Istanza riservata modificabile ha una durata di 3 anni. Per ulteriori informazioni, consulta Unire le Istanze riservate modificabili.
- Quando Amazon EC2 scambia un'istanza riservata modificabile, ritira la prenotazione associata e trasferisce la data di fine alla nuova prenotazione. Dopo lo scambio, Amazon EC2 imposta sia la data di fine per la vecchia prenotazione sia la data di inizio per la nuova prenotazione sulla data dello scambio. Ad esempio, se sostituisci una prenotazione di 3 anni con una validità residua di 16 mesi, la nuova prenotazione sarà di 16 mesi e avrà la stessa data di fine della prenotazione dell'istanza riservata modificabile che hai scambiato.

Calcolare gli scambi di Istanze riservate modificabili

Lo scambio di elementi di Istanze riservate modificabili è gratuito. Tuttavia, potresti dover pagare un costo di allineamento, che è un costo anticipato ripartito proporzionalmente della differenza tra le Istanze riservate modificabili di cui eri in possesso e le nuove Istanze riservate modificabili ricevute nello scambio.

Ciascuna Istanza riservata modificabile ha un valore di listino. Questo valore di elenco viene confrontato con il valore di elenco delle istanze riservate convertibili che desideri determinare quante prenotazioni di istanze puoi ricevere dall'exchange.

Ad esempio, hai una Istanza riservata modificabile con un valore di listino di 35 USD che intendi scambiare per un tipo di istanza nuovo con un valore di listino di 10 USD.

```
$35/$10 = 3.5
```

Puoi scambiare la Istanza riservata modificabile con tre Istanze riservate modificabili da 10 USD. Non è possibile acquistare metà delle prenotazioni, pertanto è necessario acquistare un'ulteriore Istanza riservata modificabile che copra il resto:

```
3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved
 Instance
```

La quarta Istanza riservata modificabile ha la stessa data di fine delle altre tre. Se stai scambiando elementi di Istanze riservate modificabili con costo anticipato parziale o totale, sarà necessario pagare il costo di allineamento per la quarta prenotazione. Se il costo anticipato restante degli elementi di Istanze riservate modificabili è 500 USD, e la nuova prenotazione è di norma 600 USD su base ripartita proporzionalmente, ti verranno addebitati 100 USD.

```
$600 prorated upfront cost of new reservations - $500 remaining upfront cost of old
 reservations = $100 difference
```

Unire le Istanze riservate modificabili

Se unisci due o più Istanze riservate modificabili, il termine della nuova Istanza riservata modificabile deve essere lo stesso o più grande delle Istanze riservate modificabili originali. La data di scadenza della nuova Istanza riservata modificabile sarà la più lontana nel futuro.

Supponiamo, ad esempio, tu abbia i seguenti elementi di Istanze riservate modificabili nell'account:

ID Istanza riservata	Termine	Data di scadenza
aaaa1111	1 anno	31/12/2018
bbbb2222	1 anno	31/07/2018
cccc3333	3 anni	30/06/2018
dddd4444	3 anni	31/12/2019

- Puoi unire `aaaa1111` e `bbbb2222` e scambiarli con un'Istanza riservata modificabile di 1 anno. Non puoi scambiarli con un'Istanza riservata modificabile di 3 anni. La data di scadenza della nuova Istanza riservata modificabile è 31/12/2018.
- Puoi unire `bbbb2222` e `cccc3333` e scambiarli con un'Istanza riservata modificabile di 3 anni. Non puoi scambiarli con un'Istanza riservata modificabile di 1 anno. La data di scadenza della nuova Istanza riservata modificabile è 31/07/2018.
- Puoi unire `cccc3333` e `dddd4444` e scambiarli con un'Istanza riservata modificabile di 3 anni. Non puoi scambiarli con un'Istanza riservata modificabile di 1 anno. La data di scadenza della nuova Istanza riservata modificabile è 31/12/2019.

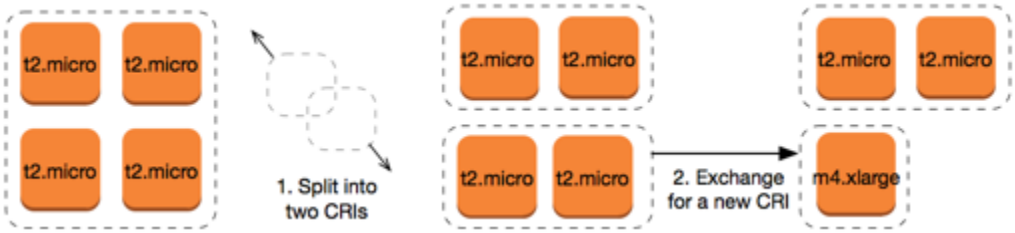
Scambiare una parte di una Istanza riservata modificabile

Puoi usare il processo di modifica per suddividere l'Istanza riservata modificabile in prenotazioni più piccole, quindi scambiare una o più delle nuove prenotazioni con una nuova Istanza riservata modificabile. Gli esempi seguenti mostrano come procedere.

Example Esempio: Istanza riservata modificabile con più istanze

In questo esempio hai un'`t2.micro` Istanza riservata modificabile con quattro istanze nella prenotazione. Per scambiare due istanze `t2.micro` con un'istanza `m4.xlarge`:

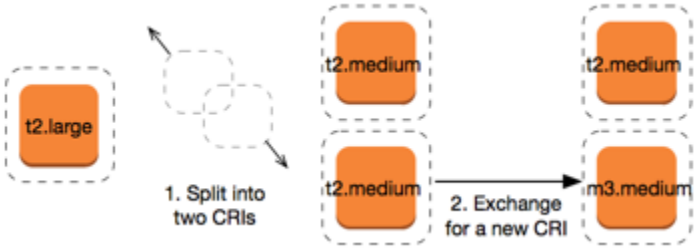
1. Modifica l'Istanza riservata modificabile `t2.micro` suddividendola in due Istanze riservate modificabili `t2.micro` con due istanze ciascuna.
2. Scambia una delle nuove Istanze riservate modificabili `t2.micro` con un'Istanza riservata modificabile `m4.xlarge`.



Example Esempio: Istanza riservata modificabile con una singola istanza

In questo esempio hai un'Istanza riservata modificabile `t2.large`. Per modificarla in una istanza `t2.medium` più piccola e un'istanza `m3.medium`:

1. Modifica l'Istanza riservata modificabile `t2.large` suddividendola in due Istanze riservate modificabili `t2.medium`. Una sola istanza `t2.large` ha lo stesso footprint della dimensione di istanza di due istanze `t2.medium`.
2. Scambia una delle nuove Istanze riservate modificabili `t2.medium` con un'Istanza riservata modificabile `m3.medium`.



Per ulteriori informazioni, consulta Supporto per la modifica delle dimensioni dell'istanza e Inviare richieste di scambio.

Inviare richieste di scambio

Puoi scambiare le istanze riservate modificabili. Le istanze riservate scambiate vengono ritirate.

Console

Per scambiare istanze riservate modificabili

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Reserved Instances (Istanze riservate), selezionare le Istanze riservate modificabili da scambiare e scegliere Actions (Azioni), Exchange Istanza riservata (Scambia Istanza riservata).
3. Selezionare gli attributi della configurazione desiderata e scegliere Find offering (Trova offerta).
4. Selezionare una nuova Istanza riservata modificabile. Nella parte inferiore dello schermo, è possibile visualizzare il numero di Istanze riservate che si riceve per lo scambio e gli eventuali costi aggiuntivi.
5. Una volta selezionata una Istanza riservata modificabile che soddisfi le proprie esigenze, scegliere Review (Verifica).
6. Scegliere Exchange (Scambia), quindi Close (Chiudi).

AWS CLI

Per scambiare un'istanza riservata modificabile

1. Trova un'istanza riservata modificabile che soddisfi le esigenze usando il comando describe-reserved-instances-offerings.
2. Ottieni un preventivo per lo scambio usando il comando get-reserved-instances-exchange-quote. Il preventivo include il numero di Istanze riservate che otterrai dallo scambio e il costo di allineamento effettivo per lo scambio:
3. Esegui lo scambio usando il comando accept-reserved-instances-exchange-quote.

PowerShell

Per scambiare un'istanza riservata modificabile

1. Trova una nuova istanza riservata convertibile che soddisfi le tue esigenze utilizzando il cmdlet. Get-EC2ReservedInstancesOffering
2. Ottieni un preventivo per lo scambio utilizzando il cmdlet. GetEC2-ReservedInstancesExchangeQuote Il preventivo include il numero di Istanze riservate che otterrai dallo scambio e il costo di allineamento effettivo per lo scambio:
3. Eseguire lo scambio utilizzando il cmdlet Approve-EC2ReservedInstancesExchangeQuote

Quote di istanze riservate

Puoi acquistare nuove istanze riservate ogni mese. Il numero di nuove istanze riservate che puoi acquistare ogni mese è determinato dalla quota mensile, come segue:

Descrizione della quota	Quota predefinita
Nuove istanze regionali riservate	20 per regione al mese
Nuove istanze riservate zonali	20 per zona di disponibilità al mese

Ad esempio, in una regione con tre zone di disponibilità, la quota predefinita è di 80 nuove istanze riservate al mese, calcolata come segue:

- 20 istanze riservate regionali per la regione

- Più 60 istanze riservate zonali (20 per ciascuna delle tre zone di disponibilità)

Le istanze nello stato `running` vengono conteggiate ai fini della quota. Le istanze negli stati `pending`, `stopping`, `stopped` e `hibernated` non vengono conteggiate ai fini della quota.

Visualizza il numero di istanze riservate acquistate

Il numero di istanze riservate acquistate è indicato dal campo Instance count (Conteggio istanze) (console) o dal parametro `InstanceCount` (AWS CLI). Quando acquisti nuove istanze riservate, la quota viene misurata rispetto al numero totale di istanze. Ad esempio, se acquisti una singola configurazione di istanza riservata con un numero di istanze pari a 10, l'acquisto viene conteggiato ai fini della tua quota come 10, e non come 1.

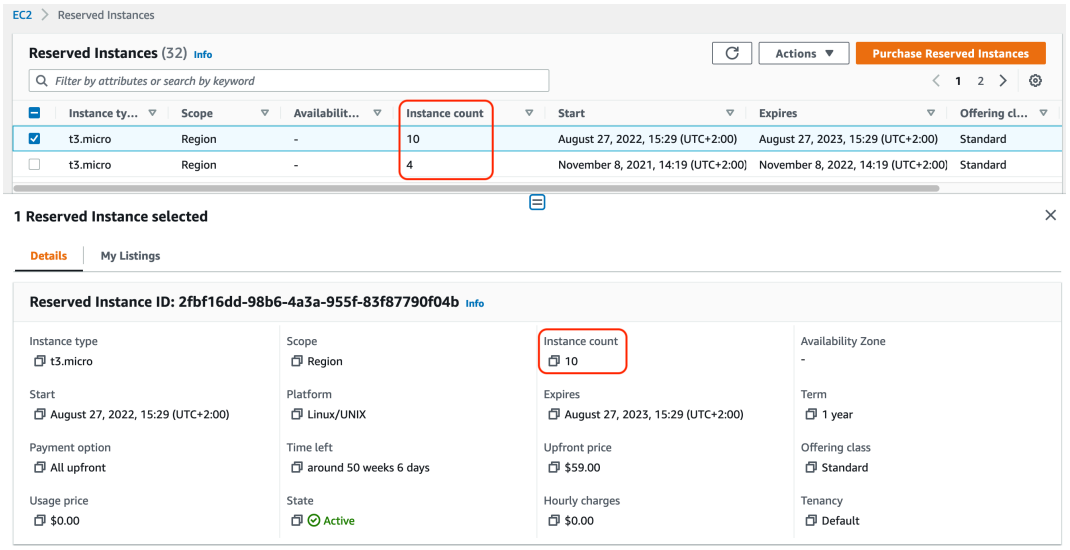
Puoi visualizzare quante istanze riservate hai acquistato utilizzando Amazon EC2 o l' AWS CLI.

Console

Per visualizzare il numero di istanze riservate acquistate

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Reserved Instances (Istanze riservate).
3. Seleziona una configurazione di istanza riservata dalla tabella e controlla il campo Instance count (Conteggio istanze).

   Nella schermata seguente, la riga selezionata rappresenta una singola configurazione dell'istanza riservata per un tipo di istanza `t3.micro`. La colonna Instance count (Conteggio istanze) nella vista della tabella e il campo Instance count (Conteggio istanze) nella vista dettagliata (evidenziata nella schermata) indicano che ci sono 10 istanze riservate per questa configurazione.



AWS CLI

Per visualizzare il numero di istanze riservate acquistate

Usa il comando describe-reserved-instances e specifica l'ID della configurazione dell'istanza riservata.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --output table
```

Di seguito è riportato un output di esempio. Il campo `InstanceCount` indica che per questa configurazione sono presenti 10 istanze riservate.

```
-------------------------------------------------------------------
|                    DescribeReservedInstances                    |
+-----------------------------------------------------------------+
||                       ReservedInstances                       ||
|+----------------------+----------------------------------------+|
||  CurrencyCode        |  USD                                   ||
||  Duration            |  31536000                              ||
||  End                 |  2023-08-27T13:29:44+00:00             ||
||  FixedPrice          |  59.0                                  ||
||  InstanceCount       |  10                                    ||
||  InstanceTenancy     |  default                               ||
||  InstanceType        |  t3.micro                              ||
||  OfferingClass       |  standard                              ||
```

```
||  OfferingType        |  All Upfront                            ||
||  ProductDescription  |  Linux/UNIX                             ||
||  ReservedInstancesId |  a1b2c3d4-5678-90ab-cdef-EXAMPLE11111   ||
||  Scope               |  Region                                 ||
||  Start               |  2022-08-27T13:29:45.938000+00:00       ||
||  State               |  active                                 ||
||  UsagePrice          |  0.0                                    ||
|+----------------------+-----------------------------------------+|
|||                     RecurringCharges                         |||
||+----------------------------------+--------------------------+||
|||  Amount                          |  0.0                     |||
|||  Frequency                       |  Hourly                  |||
||+----------------------------------+--------------------------+||
```

PowerShell

Per visualizzare il numero di istanze riservate acquistate

Utilizza il Get-EC2ReservedInstance cmdlet e specifica l'ID della configurazione dell'istanza riservata.

```
Get-EC2ReservedInstance -ReservedInstancesId a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Di seguito è riportato un output di esempio. Il campo `InstanceCount` indica che per questa configurazione sono presenti 10 istanze riservate.

```
AvailabilityZone    :
CurrencyCode        : USD
Duration            : 31536000
End                 : 1/12/2017 8:57:08 PM
FixedPrice          : 0
InstanceCount       : 10
InstanceTenancy     : default
InstanceType        : t3.medium
OfferingClass       : standard
OfferingType        : All Upfront
ProductDescription  : Windows
RecurringCharges    : {}
ReservedInstancesId : a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
Scope               : Region
Start               : 10/12/2016 4:00:00 PM
State               : active
Tags                : {}
```

```
UsagePrice          : 0
```

Considerazioni

Un'istanza riservata regionale applica uno sconto a un'istanza in esecuzione On-Demand . Il limite di On-Demand istanze predefinito è 20. Non è possibile superare il limite di On-Demand istanze in esecuzione acquistando istanze riservate regionali. Ad esempio, se hai già 20 istanze riservate in esecuzione e acquisti 20 On-Demand istanze riservate regionali, le 20 istanze riservate regionali vengono utilizzate per applicare uno sconto alle 20 istanze riservate in esecuzione. On-Demand Se acquisti più istanze riservate regionali, non potrai avviarne altre perché hai raggiunto il limite di istanze. On-Demand

Prima di acquistare istanze riservate regionali, assicurati che il limite di On-Demand istanze corrisponda o superi il numero di istanze riservate regionali che intendi possedere. Se necessario, assicurati di richiedere un aumento del limite di istanze prima di acquistare altre On-Demand istanze riservate regionali.

Istanza riservata zonale: un'Istanza riservata acquistata per una zona di disponibilità specifica, che offre la prenotazione della capacità e uno sconto. Puoi superare il limite di On-Demand istanze in esecuzione acquistando istanze riservate zonali. Ad esempio, se hai già 20 On-Demand istanze riservate in esecuzione e acquisti 20 istanze riservate zonali, puoi avviarne altre 20 che corrispondono alle specifiche delle tue On-Demand istanze riservate zonali, per un totale di 40 istanze in esecuzione.

Visualizza le quote della tua istanza riservata e richiedi un aumento della quota

La console Amazon EC2 fornisce informazioni sulle quote. Puoi anche richiedere un aumento delle quote. Per ulteriori informazioni, consulta Visualizzazione delle quote correnti e Richiesta di un aumento.

Spot Instances

Un'istanza Spot è un'istanza che utilizza capacità EC2 di riserva disponibile a un prezzo inferiore al On-Demand prezzo. Poiché Istanze spot consente di richiedere istanze EC2 inutilizzate con forti sconti, è possibile ridurre i costi di Amazon EC2 in modo significativo. La tariffa oraria per un'istanza spot è denominata prezzo Spot. Il prezzo Spot per ogni tipo di istanza in ogni zona di disponibilità viene stabilito da Amazon EC2 e regolato gradualmente in base alla fornitura sul lungo periodo e alla richiesta per Istanze spot. L'istanza spot viene eseguita ogni qualvolta è disponibile capacità.

Le Istanze spot sono una scelta conveniente se si può essere flessibili su quando vengono eseguite le applicazioni e se queste possono essere interrotte. Per esempio, le Istanze spot sono adatte all'analisi dei dati, alle attività batch, alle elaborazioni in background e alle attività opzionali. Per ulteriori informazioni, consulta Istanze spot Amazon EC2.

Per un confronto tra le diverse opzioni di acquisto per le istanze EC2, consulta Opzioni di fatturazione e acquisto di Amazon EC2.

Concetti

Prima di cominciare a utilizzare istanze spot, occorre acquisire familiarità con i concetti seguenti:

- Pool di capacità spot - Un insieme di istanze EC2 inutilizzate con lo stesso tipo di istanza (ad esempio, `m5.large`) e zona di disponibilità.
- Prezzo Spot - Il prezzo orario attuale di un'istanza spot.
- Richiesta di istanza spot - Richiede un'istanza spot. Quando la capacità è disponibile, Amazon EC2 soddisfa la richiesta. Una richiesta di istanza spot può essere una tantum o persistente. Amazon EC2 invia automaticamente una nuova richiesta di istanza spot persistente dopo che l'istanza spot associata alla richiesta viene interrotta.
- Suggerimento di ribilanciamento dell'istanza EC2: Amazon EC2 emette un segnale che suggerisce il ribilanciamento dell'istanza per segnalarti che un'istanza spot è ad alto rischio di interruzione. Questo segnale ti offre l'opportunità di ribilanciare preventivamente i carichi di lavoro tra quelli esistenti o tra nuove istanze spot senza dover attendere l'avviso di interruzione dell'istanza spot di due minuti.
- Interruzione istanza spot: Amazon EC2 termina, arresta o iberna l'istanza spot quando Amazon EC2 deve recuperare capacità. Amazon EC2 fornisce una notifica di interruzione dell'istanza spot, che dà all'istanza un preavviso di due minuti prima che venga interrotta.

Differenze tra istanze Spot e istanze On-Demand

La tabella seguente elenca le principali differenze tra le istanze Spot e le istanze. On-Demand

	Spot Instances	On-Demand Istanze
Ora di avvio		

	Spot Instances	On-Demand Istanze
	Può essere avviata immediatamente solo se è attiva la richiesta dell'istanza spot e se la capacità è disponibile.	Può essere avviata immediatamente solo se si effettua una richiesta di avvio manuale e la capacità è disponibile.
Capacità disponibile	Se la capacità non è disponibile, la richiesta dell'istanza spot continuerà a effettuare automaticamente la richiesta di avvio fino a quando la capacità non diventa disponibile.	Se la capacità non è disponibile quando si effettua una richiesta di avvio, si ottiene un errore di capacità insufficiente (ICE).
Tariffa oraria	Il prezzo orario per istanze spot varia in base alla fornitura a lungo termine e alla domanda.	Il prezzo orario per le On-Demand istanze è statico.
Raccomandazione di ribilanciamento	Il segnale che Amazon EC2 emette per un'istanza spot in esecuzione quando presenta un rischio elevato di interruzione.	Sei tu a determinare quando un' On-Demand istanza viene interrotta (interrotta, ibernata o terminata).
Interruzione istanza	Puoi interrompere e avviare un'istanza Amazon Spot. EBS-backed Amazon EC2, inoltre, può interrompere una singola istanza spot se la capacità non è più disponibile.	Sei tu a determinare quando un' On-Demand istanza viene interrotta (interrotta, ibernata o terminata).

Prezzi e risparmio

Paghi il prezzo Spot per le Istanze spot, che viene stabilito da Amazon EC2 e regolato gradualmente in base alla fornitura sul lungo periodo e alla richiesta di Istanze spot. Le istanze spot vengono eseguite fino a quando non vengono terminate, la capacità non è più disponibile o il gruppo Amazon EC2 Auto Scaling le termina durante il dimensionamento orizzontale.

Se un'istanza spot in esecuzione viene interrotta da te o da Amazon EC2, ti vengono fatturati i secondi utilizzati o l'intera ora, oppure non viene fatturato nulla, a seconda del sistema operativo

utilizzato e di chi ha interrotto l'istanza spot. Per ulteriori informazioni, consulta Fatturazione delle Istanze spot interrotte.

Le istanze spot non sono coperte dai Savings Plans. Se disponi di Savings Plans, non sono previsti risparmi aggiuntivi oltre a quelli che già ottieni utilizzando le istanze spot. Inoltre, la spesa per le istanze spot non applica gli impegni previsti dai tuoi Savings Plans per il calcolo.

Visualizza prezzi

Per visualizzare il prezzo Spot più basso attuale (aggiornato ogni cinque minuti) per Regione AWS tipo di istanza, consulta la pagina dei prezzi delle istanze Spot di Amazon EC2.

Per visualizzare la cronologia dei prezzi spot degli ultimi tre mesi, utilizza la console Amazon EC2 o il comando describe-spot-price-history. Per ulteriori informazioni, consulta Visualizzare la cronologia dei prezzi dell'istanza spot.

Associamo in modo indipendente le zone di disponibilità ai codici per ciascuna. Account AWS Pertanto, è possibile ottenere risultati diversi per lo stesso codice di zona di disponibilità (per esempio, `us-west-2a`) tra account diversi.

Visualizzare il risparmio

Puoi visualizzare i risparmi ottenuti utilizzando istanze spot per una singola serie di istanze spot o per tutte le istanze spot. È possibile visualizzare il risparmio realizzato nell'ultima ora o negli ultimi tre giorni e il costo medio orario per la vCPU e per la memoria (GiB). Gli importi risparmiati sono solo delle stime e potrebbero essere diversi da quelli effettivi, in quanto non includono gli adeguamenti della fatturazione per l'utilizzo. Per ulteriori informazioni sulla visualizzazione delle informazioni sul risparmio, consulta Risparmio sull'acquisto di Istanze spot.

Visualizzare la fattura

La fattura fornisce dettagli sull'utilizzo del servizio. Per ulteriori informazioni, consulta Visualizzazione della fattura nella Guida per l'utente di AWS Billing .

Best practice per spot di Amazon EC2

Amazon EC2 fornisce l'accesso alla capacità di calcolo EC2 di riserva nelle Cloud AWS istanze Spot con un risparmio fino al 90% rispetto ai prezzi. On-Demand L'unica differenza tra On-Demand le istanze e le istanze Spot è che le istanze Spot possono essere interrotte da Amazon EC2, con due minuti di preavviso, se Amazon EC2 ha bisogno di recuperare la capacità. Per garantire la migliore

esperienza con le istanze spot, è importante comprendere e applicare le best practice per il loro utilizzo.

Istanze spot sono consigliate per applicazioni stateless, con tolleranza ai guasti, flessibili. Ad esempio, le istanze Spot funzionano bene per big data, carichi di lavoro containerizzati, server web stateless, elaborazione ad alte prestazioni (CI/CDHPC) e carichi di lavoro di rendering.

Durante l'esecuzione, le istanze Spot sono esattamente le stesse delle istanze. On-Demand Tuttavia, Spot non garantisce la possibilità di continuare a eseguire le istanze abbastanza a lungo da completare i carichi di lavoro. Inoltre, Spot non garantisce di poter avere immediatamente a disposizione le istanze che si stanno cercando o che sia sempre possibile ottenere la capacità aggregata richiesta. Inoltre, interruzioni e capacità delle istanze spot possono cambiare nel tempo perché la disponibilità delle istanze spot varia in base all'offerta e alla domanda e le prestazioni passate non sono una garanzia di risultati futuri.

Istanze spot non sono adatte per carichi di lavoro inflessibili, stateful, senza tolleranza ai guasti o strettamente accoppiati tra nodi di istanze. Non consigliamo le istanze spot per carichi di lavoro che non tollerano periodi occasionali in cui l'intera capacità target non è completamente disponibile. Anche se seguire le best practice di Spot per essere flessibili sui tipi di istanze e sulle zone di disponibilità offre le migliori possibilità di ottenere un'elevata disponibilità, non vi è alcuna garanzia che la capacità sia disponibile, perché l'aumento della domanda di On-Demand istanze può interrompere i carichi di lavoro sulle istanze Spot.

Sconsigliamo vivamente di utilizzare le istanze Spot per questi carichi di lavoro o di tentare di eseguire il failover sulle istanze per gestire interruzioni o periodi di On-Demand indisponibilità. Il failover sulle On-Demand istanze può causare inavvertitamente interruzioni per le altre istanze Spot. Inoltre, se le istanze Spot per una combinazione di tipo di istanza e zona di disponibilità vengono interrotte, potrebbe diventare difficile ottenere istanze con la stessa combinazione. On-Demand

A prescindere che l'utente conosca già Spot o sia la prima volta che utilizza le istanze spot, se si verificano problemi di interruzioni o disponibilità delle istanze spot è consigliabile seguire queste best practice per ottenere la migliore esperienza di utilizzo del servizio Spot.

Best practice Spot

- Preparazione di singole istanze per le interruzioni
- Essere flessibili riguardo tipi di istanza e zone di disponibilità
- Utilizzo della selezione del tipo di istanza basata su attributi
- Utilizzo dei punteggi di posizionamento spot per identificare regioni e zone di disponibilità ottimali

- Utilizzo dei gruppi con dimensionamento automatico EC2 o del parco istanze EC2 per gestire la capacità aggregata
- Utilizzo della strategia di allocazione ottimizzata per prezzo e capacità
- Usa l'integrazione AWS servizi per gestire le tue istanze Spot
- Qual è il metodo di richiesta Spot migliore da utilizzare?

Preparazione di singole istanze per le interruzioni

Il modo migliore per gestire nel modo appropriato le interruzioni delle istanze spot è progettare l'applicazione affinché sia tollerante ai guasti. A tale scopo, è possibile sfruttare i suggerimenti di ribilanciamento delle istanze EC2 e gli avvisi di interruzione delle istanze spot.

Un suggerimento di ribilanciamento dell'istanza EC2 è un segnale che avvisa che un'istanza spot è a rischio elevato di interruzione. Il segnale ti dà la possibilità di gestire l'istanza spot in modo proattivo rispetto all'avviso di interruzione dell'istanza spot con preavviso di due minuti. È possibile decidere di ribilanciare il carico di lavoro su Istanze spot nuove o esistenti che non presentano un rischio elevato di interruzione. Abbiamo semplificato l'utilizzo di questo segnale utilizzando la funzionalità di ribilanciamento della capacità nei gruppi con dimensionamento automatico e nel parco istanze EC2.

Una notifica di interruzione di istanza spot è un avviso che viene emesso due minuti prima che Amazon EC2 interrompa un'istanza spot. Se il carico di lavoro è "flessibile nel tempo", puoi anche configurare le istanze spot affinché vengano arrestate o ibernate, anziché terminate, quando vengono interrotte. Amazon EC2 arresta o iberna automaticamente le istanze spot in caso di interruzione e ripristina automaticamente le istanze quando la capacità è disponibile.

Ti consigliamo di creare una regola in Amazon EventBridge che raccolga i consigli di ribilanciamento e le notifiche di interruzione, quindi attivi un checkpoint per l'avanzamento del carico di lavoro o gestisca correttamente l'interruzione. Per ulteriori informazioni, consulta Monitorare i segnali di raccomandazione di ribilanciamento. Per un esempio dettagliato che illustra come creare e utilizzare le regole degli eventi, consulta Taking Advantage of Amazon EC2 Spot Instance Interruption Notices.

Per ulteriori informazioni, consultare Raccomandazioni per il ribilanciamento delle istanze EC2 e Interruzioni dell'istanza spot.

Essere flessibili riguardo tipi di istanza e zone di disponibilità

Un pool di capacità spot è un insieme di istanze EC2 inutilizzate con lo stesso tipo di istanza (ad esempio `m5.large`) e zona di disponibilità (ad esempio, us-east-1a). È necessario essere flessibili sui tipi di istanza richiesti e sulle zone di disponibilità in cui è possibile distribuire il carico

di lavoro. Questo offre a Spot una migliore possibilità di trovare e allocare la quantità di capacità di elaborazione richiesta. Ad esempio, non richiedere solo `c5.large` se sei disposto a usare grandi quantità delle famiglie c4, m5 e m4.

A seconda delle esigenze specifiche, puoi valutare su quali tipi di istanza puoi essere flessibile per soddisfare i requisiti di calcolo. Se un carico di lavoro può essere scalato verticalmente, occorre includere tipi di istanza più grandi (più vCPU e memoria) nelle richieste. Se puoi scalare solo orizzontalmente, dovresti includere i tipi di istanza di vecchia generazione perché sono meno richiesti dai clienti. On-Demand

Una buona regola è quella di essere flessibili su almeno 10 tipi di istanza per ogni carico di lavoro. Assicurati inoltre che tutte le zone di disponibilità siano configurate per l'utilizzo nel VPC e selezionate per il carico di lavoro.

Utilizzo della selezione del tipo di istanza basata su attributi

Con la selezione del tipo di istanza basata sugli attributi, puoi specificare gli attributi dell'istanza, come vCPU, memoria e archiviazione, per il carico di lavoro che desideri eseguire. EC2 Auto Scaling o EC2 Fleet identificheranno e avvieranno automaticamente le istanze che corrispondono agli attributi specificati. Ciò elimina lo sforzo necessario per selezionare manualmente tipi di istanze specifici, il che richiede una comprensione approfondita dell'offerta di ciascun tipo di istanza.

Inoltre, la selezione del tipo di istanza basata sugli attributi consente di utilizzare automaticamente i tipi di istanza appena rilasciati non appena diventano disponibili. Ciò garantisce un accesso semplificato a una gamma sempre più ampia di capacità di istanze spot.

Attribute-based la selezione del tipo di istanza è ideale per carichi di lavoro e framework che possono essere flessibili sui tipi di istanza su cui vengono eseguiti, come l'High Performance Computing (HPC) e i carichi di lavoro di big data.

Per ulteriori informazioni, consulta Create mixed instances group using attribute-based instance type selection nella Guida per l'utente di Amazon EC2 Auto Scaling e Specifica gli attributi per la selezione del tipo di istanza per il parco del tipo per il parco istanze EC2 o il parco istanze Spot in questa guida.

Utilizzo dei punteggi di posizionamento spot per identificare regioni e zone di disponibilità ottimali

Le istanze spot sono capacità EC2 inutilizzata e tale capacità varia in base alla domanda e all'offerta di EC2. Di conseguenza, potresti non ottenere sempre la capacità spot esatta di cui hai bisogno in una posizione specifica in un determinato momento. Per mitigare questa imprevedibilità, puoi utilizzare la funzionalità del punteggio di posizionamento spot. Questa funzionalità fornisce consigli per le regioni o le zone di disponibilità che hanno maggiori probabilità di avere una capacità

sufficiente per soddisfare le esigenze di capacità spot senza che sia necessario avviare prima le istanze spot in tali posizioni.

Il punteggio di posizionamento spot viene utilizzato al meglio per carichi di lavoro che possono essere flessibili per quanto riguarda i tipi di istanze e la regione o la zona di disponibilità che possono utilizzare. Tutto ciò che devi fare è specificare la capacità spot di cui hai bisogno, i requisiti del tipo di istanza e se desideri ricevere consigli per le regioni o le zone di disponibilità. In cambio, riceverai un punteggio compreso tra 1 e 10 per ogni regione o zona di disponibilità, che indica la probabilità di fornire correttamente la capacità spot richiesta in tale posizione. Un punteggio di 10 indica che la richiesta spot ha alte probabilità di successo.

È importante notare che un punteggio di posizionamento spot è un suggerimento point-in-time, poiché la capacità può variare nel tempo. Non garantisce la capacità disponibile né prevede il rischio di interruzione.

Puoi utilizzare la funzionalità di punteggio di posizionamento Spot nella console Amazon EC2 o un SDK. AWS CLI Per ulteriori informazioni, consulta Punteggio di posizionamento spot.

Utilizzo dei gruppi con dimensionamento automatico EC2 o del parco istanze EC2 per gestire la capacità aggregata

Spot consente di pensare in termini di capacità aggregata (in unità che includono vCPU, memoria, archiviazione o throughput di rete), piuttosto che in termini di singole istanze. I gruppi con dimensionamento automatico e il parco istanze EC2 consentono di avviare e gestire una capacità di destinazione e di sostituire automaticamente le risorse interrotte o terminate manualmente. Quando configuri un gruppo con dimensionamento automatico o un parco istanze EC2, devi specificare solo i tipi di istanza e la capacità di destinazione in base alle esigenze dell'applicazione. Per ulteriori informazioni, consulta Gruppi Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling e Creazione di un parco istanze EC2 in questa guida per l'utente.

Utilizzo della strategia di allocazione ottimizzata per prezzo e capacità

Le strategie di allocazione nei gruppi Auto Scaling consentono di effettuare il provisioning della capacità target senza la necessità di cercare manualmente i pool di capacità spot con capacità inutilizzata. È consigliabile utilizzare la strategia `price-capacity-optimized` perché questa effettua automaticamente il provisioning delle istanze dai pool di capacità spot più disponibili che hanno anche il prezzo più basso possibile. Inoltre, nel parco istanze EC2 è possibile sfruttare la strategia di allocazione `price-capacity-optimized`. Poiché la capacità dell'istanza spot viene restituita da pool con capacità ottimale, ciò riduce la possibilità che le istanze spot vengano recuperate. Per ulteriori informazioni, consulta Allocation strategies for multiple instance types nella

Guida per l'utente di Amazon EC2 Auto Scaling e Quando i carichi di lavoro hanno un costo di interruzione elevato nella presente Guida per l'utente.

Usa l'integrazione AWS servizi per gestire le tue istanze Spot

Altri AWS servizi si integrano con Spot per ridurre i costi complessivi di elaborazione senza la necessità di gestire le singole istanze o flotte. Ti consigliamo di prendere in considerazione le seguenti soluzioni per i carichi di lavoro applicabili: Amazon EMR, Amazon Elastic Container Service, Amazon Elastic Kubernetes Service AWS Batch, Amazon AI e Amazon Servers. SageMaker AWS Elastic Beanstalk GameLift Per ulteriori informazioni sulle best practice Spot con questi servizi, consulta il sito Web Amazon EC2 Istanze spot Workshops.

Qual è il metodo di richiesta Spot migliore da utilizzare?

Utilizzare la tabella seguente per determinare l'API da utilizzare per richiedere istanze spot.

"Hello, World!"	Quando usarla?	Caso d'uso	Dovrei usare quest'API?
CreateAutoScalingGroup	• Sono necessari e più istanze con una configurazione singola o mista. • Vuoi automatizzare la gestione del ciclo di vita tramite un'API configurabile.	Crea un gruppo Auto Scaling che gestisce il ciclo di vita delle istanze mantenendo il numero di istanze desiderato. Supporta il dimensionamento orizzontale (aggiunta di più istanze) tra limiti minimi e massimi specificati.	Sì
CreateFleet	• Sono necessari e più istanze con una configurazione singola o mista. •	Crea una flotta di On-Demand istanze e istanze Spot in un'unica richiesta, con diverse specifiche di avvio che variano	Sì: in modalità `instant` se non occorre il dimensionamento automatico

"Hello, World!"	Quando usarla?	Caso d'uso	Dovrei usare quest'API?
	Vuoi gestire autonomamente il ciclo di vita dell'istanza. • Se non hai bisogno di scalabilità automatica, ti consigliamo di utilizzare un parco di tipo `instant`.	in base al tipo di istanza, all'AMI, alla zona di disponibilità o alla sottorete. La strategia di allocazione delle istanze spot è per impostazione predefinita `lowest-price` per unità, ma puoi modificarla in `price-capacity-optimized`, `capacity-optimized` o `diversified`.	
RunInstances	• Stai già utilizzando l' RunInstances API per avviare On-Demand le istanze e desideri semplicemente passare all'avvio delle istanze Spot modificando un singolo parametro. • Non sono necessarie più istanze con diversi tipi di istanza.	Avvia un numero di istanze specificato utilizzando un'AMI e un tipo di istanza.	No, perché RunInstances non consente l'uso di tipi misti di istanze in una singola richiesta

"Hello, World!"	Quando usarla?	Caso d'uso	Dovrei usare quest'API?
RequestSpotFleet	• Sconsigliamo vivamente di utilizzare l' RequestSpotFleet API perché è un'API legacy senza investimenti pianificati. • Se desideri gestire il ciclo di vita dell'istanza, utilizza l'API. CreateFleet • Se non desideri gestire il ciclo di vita dell'ista nza, utilizza l'API. CreateAut oScalingGroup	NON USARE. RequestSpotFleet è un'API legacy senza investimenti pianificati.	No
RequestSpotInstanc es	• Sconsigliamo vivamente di utilizzare l' RequestSp otInstances API perché è un'API legacy senza investimenti pianificati.	NON USARE. RequestSpotInstances è un'API legacy senza investimenti pianificati.	No

Come funzionano Istanze spot

Per avviare un'Istanza spot, è possibile creare una Richiesta di istanza spot oppure affidarsi ad Amazon EC2 che crea una richiesta di istanza spot per tuo conto. L'Istanza spot viene avviata quando viene soddisfatta la richiesta di istanza spot.

È possibile avviare un'istanza spot utilizzando più servizi diversi. Per ulteriori informazioni, consulta Nozioni di base sulle istanze spot Amazon EC2 Windows. In questa guida per l'utente, vengono descritti i seguenti modi per avviare un'istanza spot utilizzando EC2:

- Puoi creare una richiesta di istanza spot utilizzando la procedura guidata di avvio dell'istanza nella console Amazon EC2 o il comando run-instances. Per ulteriori informazioni, consulta Gestione delle istanze spot.
- È possibile creare un Parco istanze EC2, nel quale si specifica il numero desiderato di istanze spot. Amazon EC2 crea una richiesta di istanza spot per tuo conto per ogni istanza spot specificata nel parco istanze EC2. Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.
- È possibile creare una richiesta di istanza spot, nel quale si specifica il numero desiderato di istanze spot. Amazon EC2 crea una richiesta di istanza spot per tuo conto per ogni istanza spot specificata nella richiesta di parco istanze spot. Per ulteriori informazioni, consulta Creazione di un parco istanze Spot.

> **Note**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

L'istanza Spot viene avviata se è disponibile capacità. L'istanza spot viene eseguita fino a quando non la arresti o termini, o fino a quando Amazon EC2 non la interrompe (nota come interruzione di istanza spot). Amazon EC2 può arrestare, terminare o ibernare un'istanza spot quando la interrompe.

Quando usi le istanze spot, devi essere preparato alle interruzioni. Amazon EC2 può interrompere la tua istanza spot quando la domanda di istanze spot aumenta o la fornitura di istanze spot diminuisce. Quando Amazon EC2 interrompe un'istanza spot, invia una notifica di interruzione dell'istanza spot che fornisce all'istanza un preavviso di due minuti prima che Amazon EC2 la interrompa. Non è possibile abilitare la protezione da interruzione per Istanze spot. Per ulteriori informazioni, consulta Interruzioni dell'istanza spot.

Indice

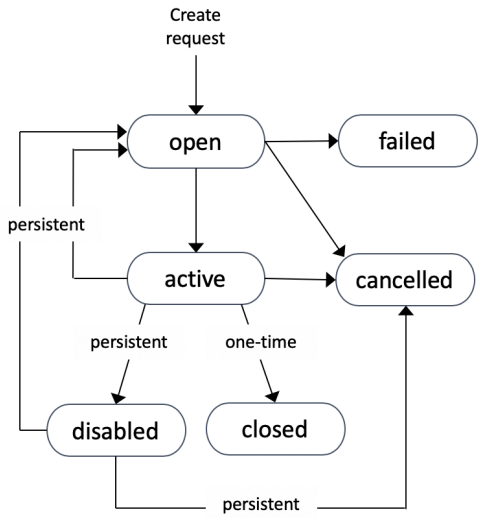
- Stati della richiesta di istanza spot
- Avviare Istanze spot in un gruppo di avvio
- Avviare le Istanze spot in un Gruppo di zona di disponibilità
- Avviare Istanze spot in un VPC
- Avvio di istanze a prestazioni espandibili
- Avvio su hardware con tenant singolo

Stati della richiesta di istanza spot

Una richiesta di istanza spot può avere uno dei seguenti stati:

- `open` - La richiesta è in attesa di essere soddisfatta.
- `active` - La richiesta è stata soddisfatta e ha un'istanza spot associata.
- `failed` - La richiesta ha uno o più parametri errati.
- `closed` - L'istanza spot è stata interrotta o terminata.
- `disabled` - L'istanza spot è stata interrotta.
- `cancelled` - La richiesta è stata annullata o è scaduta.

La figura che segue rappresenta le transizioni tra gli stati della richiesta. Le transizioni dipendono dal tipo di richiesta (una tantum o persistente).



Una richiesta di istanza spot una tantum rimane attiva fino a quando Amazon EC2 non avvia l'istanza spot, la richiesta scade oppure si annulla la richiesta. Se non è disponibile capacità, l'istanza spot viene terminata e la richiesta di istanza spot viene chiusa.

Una richiesta di istanza spot persistente rimane attiva fino a quando non scade o non viene annullata, anche se la richiesta viene soddisfatta. Se non è disponibile capacità, l'istanza spot viene interrotta. Dopo l'interruzione dell'istanza, quando diventa nuovamente disponibile capacità, l'istanza spot viene avviata, se era stata arrestata, o viene ripresa, se era stata ibernata. Puoi arrestare un'istanza spot e riavviarla se è disponibile capacità. Se l'istanza spot viene terminata (indipendentemente dal fatto che l'istanza spot sia in stato di arresto o esecuzione), la richiesta di istanza spot viene nuovamente aperta e Amazon EC2 avvia una nuova istanza spot. Per ulteriori informazioni, consultare Arrestare un'istanza spot, Avviare un'istanza spot e Terminare un'istanza spot.

È possibile monitorare lo stato delle richieste di istanza spot così come lo stato delle istanze spot avviate attraverso lo stato. Per ulteriori informazioni, consulta Ottenimento dello stato della richiesta di un'istanza spot.

Avviare Istanze spot in un gruppo di avvio

Specificare un gruppo di avvio nella richiesta di istanza spot per indicare ad Amazon EC2 di avviare un insieme di istanze spot solo se può avviarle tutte. Inoltre, se il servizio spot deve terminare una delle istanze in un gruppo di avvio, deve terminarle tutte. Tuttavia, se si terminano una o più istanze in un gruppo di avvio, Amazon EC2 non termina le altre istanze nel gruppo di avvio.

Sebbene questa opzione possa essere utile, l'aggiunta di questo vincolo può ridurre le possibilità che la richiesta di istanza spot venga soddisfatta e aumentare le possibilità che le istanze spot vengano terminate. Ad esempio, se il gruppo di avvio comprende istanze in più zone di disponibilità e la capacità in una di queste zone di disponibilità si riduce e non è più disponibile, Amazon EC2 interrompe tutte le istanze per il gruppo di avvio.

Se si crea un'altra richiesta di istanza spot valida che specifica lo stesso gruppo di avvio (esistente) di una precedente richiesta valida, le nuove istanze vengono aggiunte al gruppo di avvio. Successivamente, se un'istanza di questo gruppo di avvio viene terminata, tutte le istanze del gruppo di avvio vengono terminate, il che include le istanze avviate dalla prima e dalla seconda richiesta.

Avviare le Istanze spot in un Gruppo di zona di disponibilità

Specifica un gruppo di zone di disponibilità nella richiesta di istanza spot per indicare ad Amazon EC2 di avviare una serie di istanze spot nella stessa zona di disponibilità. Amazon EC2 non deve interrompere tutte le istanze di un gruppo di zona di disponibilità allo stesso tempo. Se Amazon

EC2 deve interrompere una delle istanze di un gruppo di zona di disponibilità, le altre restano in esecuzione.

Sebbene questa opzione possa essere utile, l'aggiunta di questo vincolo può ridurre le possibilità che la richiesta di istanza spot venga soddisfatta.

Se si specifica un gruppo di zona di disponibilità ma non una zona di disponibilità nella richiesta di istanza spot, il risultato dipende dalla rete specificata.

VPC predefinito

Amazon EC2 utilizza la zona di disponibilità per la sottorete specificata. Se non specifichi una sottorete, seleziona una zona di disponibilità e la rispettiva sottorete predefinita, ma non necessariamente quella con il prezzo più basso. Se è stata cancellata la sottorete predefinita per una zona di disponibilità, è necessario specificare una sottorete diversa.

VPC non predefinito

Amazon EC2 utilizza la zona di disponibilità per la sottorete specificata.

Avviare Istanze spot in un VPC

Specificate una sottorete per le vostre istanze Spot nello stesso modo in cui specificate una sottorete per le vostre istanze. On-Demand

- [VPC predefinito] Se si desidera che l'istanza spot venga avviata in una specifica zona di disponibilità a basso prezzo, è necessario specificare la sottorete corrispondente nella richiesta di istanza spot. Se non si specifica una sottorete, Amazon EC2 ne seleziona una e la zona di disponibilità per tale sottorete potrebbe non avere il prezzo Spot più basso.
- [VPC non predefinito] È necessario specificare la sottorete per l'istanza spot.

Avvio di istanze a prestazioni espandibili

I tipi di istanza T sono istanze con prestazioni espandibili. Se avvii le tue istanze spot utilizzando un tipo di istanza espandibile, e prevedi di utilizzare l'istanza spot espandibile immediatamente e per un breve periodo, senza alcun tempo di inattività per accumulare crediti CPU, suggeriamo di avviarla in Modalità Standard per evitare costi più elevati. Se avvii le istanze spot a prestazioni espandibili in Modalità Illimitata ed espandi la capacità di CPU immediatamente, l'espansione implicherà il dispendio dei crediti in più. Se l'istanza viene utilizzata per un periodo di tempo limitato, non riesce

ad accumulare crediti CPU per ripagare i crediti extra, che i vengono quindi addebitati al termine dell'istanza.

La modalità illimitata è adatta per la Istanze spot con prestazioni burstable solo se l'istanza viene eseguita per un periodo di tempo sufficiente ad accumulare i crediti CPU per l'espansione. In caso contrario, il pagamento di crediti in eccedenza rende le prestazioni Istanze spot espandibili più costose rispetto all'utilizzo di altre istanze. Per ulteriori informazioni, consulta Quando utilizzare la modalità illimitata rispetto alla CPU fissa.

Le istanze T2, se configurate in modalità Standard, ottengono crediti di avvio. Le istanze T2 sono le uniche istanze a prestazioni espandibili che ottengono crediti di avvio. I crediti di avvio hanno lo scopo di fornire un'esperienza di avvio iniziale produttiva per le istanze T2, fornendo risorse di calcolo sufficienti per configurare l'istanza. Non sono consentiti avvii ripetuti di istanze T2 per accedere a nuovi crediti di avvio. Se occorre una CPU duratura, è possibile guadagnare crediti (rimanendo inattivi per un certo periodo) utilizzando la Unlimited mode (Modalità Illimitata) per istanze spot T2 o un tipo di istanza con una CPU dedicata.

Avvio su hardware con tenant singolo

È possibile eseguire un'istanza spot su hardware a tenant singolo. Le istanze Spot dedicate sono fisicamente isolate dalle istanze appartenenti ad altri account. AWS Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2 e le Istanze dedicate di Amazon EC2.

Per eseguire un'istanza spot dedicata, procedere in uno dei seguenti modi:

- Specifica una tenancy di `dedicated` durante la creazione della richiesta di istanza spot. Per ulteriori informazioni, consulta Gestione delle istanze spot.
- Richiedere un'istanza spot in un VPC con una tenancy di istanza di `dedicated`. Per ulteriori informazioni, consulta Avvio di Istanze dedicate in un VPC con tenancy predefinita. Non è possibile richiedere un'istanza spot con una tenancy `default` se viene richiesta in un VPC con una tenancy di istanza `dedicated`.

Tutte le famiglie di istanze supportano Istanze spot dedicato fatta eccezione per le istanze T Per ogni famiglia di istanze supportata, solo la dimensione di istanza più grande o la dimensione del metallo supporta le Istanze spot dedicate.

Visualizzare la cronologia dei prezzi dell'istanza spot

I prezzi delle istanze spot sono stabiliti da Amazon EC2 e regolati in modo graduale in base ai trend a lungo termine di offerta e domanda di capacità delle istanze spot.

Quando la tua richiesta Spot viene soddisfatta, le tue istanze Spot vengono avviate al prezzo Spot corrente, non superiore al prezzo. On-Demand È possibile visualizzare la cronologia del prezzo Spot degli ultimi 90 giorni, filtrata per tipo di istanza, sistema operativo e zona di disponibilità.

Per i prezzi delle istanze spot correnti, consulta Prezzi delle istanze spot Amazon EC2.

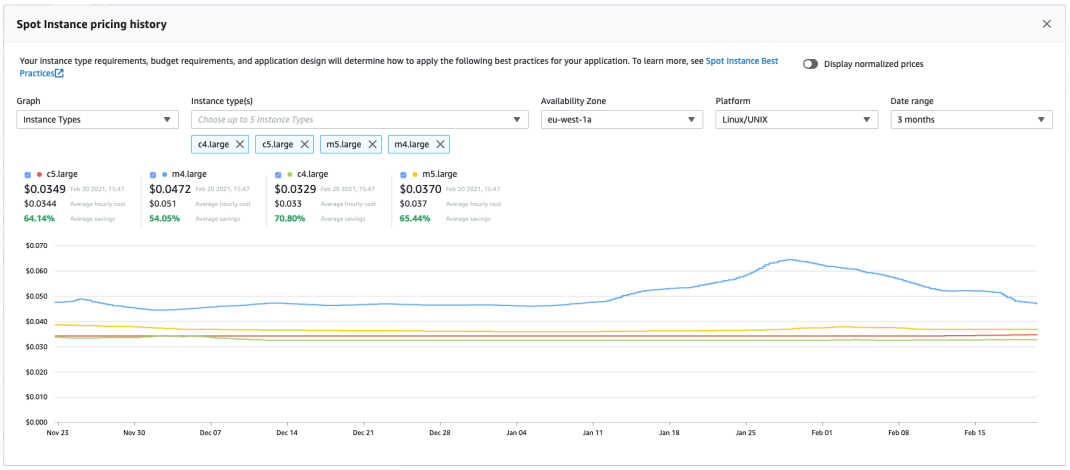
Console

Per visualizzare la cronologia del prezzo spot

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona Cronologia prezzi.
4. Per Graph (Grafico)scegliere di confrontare la cronologia dei prezzi in base alle Availability Zones (Zone di disponibilità) o ai Instance Types (Tipi di istanze).

   - Se selezioni Zone di disponibilità, scegli il Tipo di istanza, il sistema operativo (Piattaforma) e l'Intervallo di date per i quali visualizzare la cronologia dei prezzi.
   - Se selezioni Tipi di istanza, scegli fino a cinque Tipi di istanza, la Zona di disponibilità, il sistema operativo (Piattaforma) e l'Intervallo di date per i quali visualizzare la cronologia dei prezzi.

   La seguente schermata mostra un confronto dei prezzi per i diversi tipi di istanza.



5. Sposta il puntatore del mouse sul grafico per visualizzare i prezzi in momenti specifici nell'intervallo di date selezionato. I prezzi sono visualizzati nei blocchi informativi sopra il grafico. Il prezzo visualizzato nella riga superiore mostra il prezzo in una data specifica. Il prezzo visualizzato nella seconda riga mostra il prezzo medio nell'intervallo di date selezionato.
6. Per visualizzare il prezzo per vCPU, attiva o disattiva Display normalized prices (Visualizza prezzi normalizzati). Per visualizzare il prezzo per il tipo di istanza, disattiva Display normalized prices (Visualizza prezzi normalizzati).

AWS CLI

Per visualizzare la cronologia del prezzo spot

Usa il seguente comando describe-spot-price-history.

```
aws ec2 describe-spot-price-history \
    --instance-types c6i.xlarge \
    --product-descriptions "Linux/UNIX" \
    --start-time 2025-04-01T00:00:00 \
    --end-time 2025-04-02T00:00:0
```

PowerShell

Per visualizzare la cronologia del prezzo spot

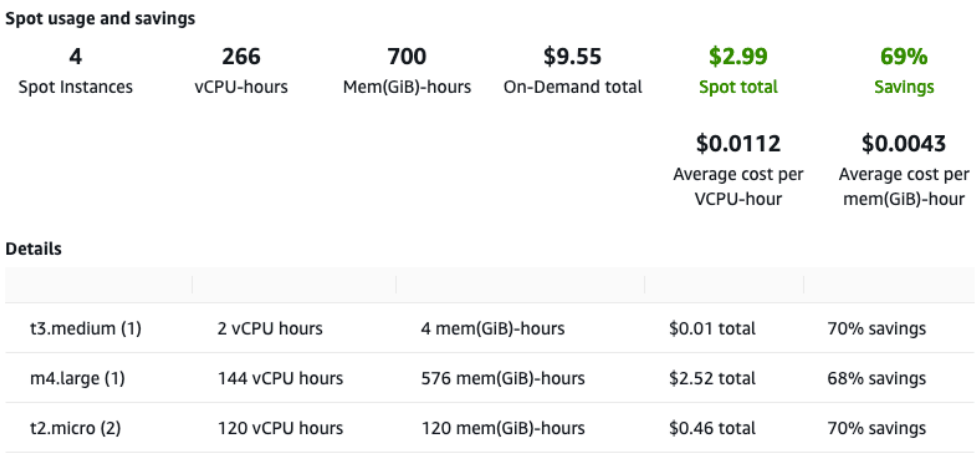
Utilizza il cmdlet Get-EC2SpotPriceHistory.

```
Get-EC2SpotPriceHistory `
    -InstanceType c6i.xlarge `
    -ProductDescription "Linux/UNIX" `
    -UtcStartTime 2025-04-01T00:00:00 `
    -UtcEndTime 2025-04-02T00:00:0
```

Risparmio sull'acquisto di Istanze spot

È possibile visualizzare informazioni sull'utilizzo e sul risparmio per le Istanze spot a livello di singolo parco istanze o per tutte le Istanze spot in esecuzione. A livello di singolo parco istanze, le informazioni su utilizzo e risparmio includono tutte le istanze avviate e terminate dal parco istanze. Puoi visualizzare queste informazioni relative all'ultima ora o agli ultimi tre giorni.

Lo screenshot seguente della sezione Risparmio mostra le informazioni relative al risparmio e all'utilizzo Spot per un parco istanze spot.



Puoi visualizzare le seguenti informazioni su utilizzo e risparmio:

- Istanze spot - Il numero di Istanze spot avviate e terminate dal Parco istanze spot. Nel riepilogo del risparmio il numero rappresenta tutte le Istanze spot in esecuzione.
- v CPU-hours — Il numero di ore di vCPU utilizzate in tutte le istanze Spot per il periodo di tempo selezionato.
- Mem(GiB)-hours (Mem(GiB)/ora) – Il numero di ore di utilizzo dei GiB di memoria in tutte le Istanze spot per l'intervallo di tempo selezionato.
- On-Demand totale: l'importo totale che avresti pagato per il periodo di tempo selezionato se avessi avviato queste istanze come istanze. On-Demand
- Spot total (Totale Spot) – L'importo totale da pagare per l'intervallo di tempo selezionato.
- Risparmi: la percentuale che stai risparmiando non pagando il On-Demand prezzo.
- Costo medio per v CPU-hour: il costo orario medio dell'utilizzo delle vCPU in tutte le istanze Spot per l'intervallo di tempo selezionato, calcolato come segue: Costo medio per v CPU-hour = totale Spot/v. CPU-hours
- Costo medio per mem (GiB) -ora: il costo orario medio dell'utilizzo di GiBs tutte le istanze Spot per il periodo di tempo selezionato, calcolato come segue: Costo medio per mem (GiB) -ora = Spot total/Mem (GiB) -ore.
- Tabella Details (Dettagli) - I diversi tipi di istanza (il numero di istanze per tipo è indicato tra parentesi) che costituiscono il Parco istanze spot. Nel riepilogo del risparmio sono incluse tutte le Istanze spot in esecuzione.

Le informazioni relative al risparmio possono essere visualizzate solo utilizzando la console di Amazon EC2.

> **Note**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Per visualizzare le informazioni sui risparmi per un parco istanze spot

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona l'ID di una richiesta della serie di istanze spot e scorri fino alla sezione Risparmio.

   In alternativa, seleziona la casella di controllo accanto all'ID richiesta del parco istanze spot e scegli la casella di controllo Risparmi.
4. Per impostazione predefinita, nella pagina sono visualizzate le informazioni relative a utilizzo e risparmio relative agli ultimi tre giorni. È possibile scegliere last hour (ultima ora) o last three days (ultimi tre giorni). Per i Parchi istanze spot lanciati meno di un'ora prima, la pagina mostra il risparmio stimato per l'ora.

Per visualizzare le informazioni sui risparmi per tutte le istanze spot in esecuzione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona Riepilogo risparmio.

Creare una richiesta di istanza spot

Per utilizzare istanze spot, viene creata una richiesta di istanza spot che include il numero desiderato di istanze, il tipo di istanza e la zona di disponibilità. Quando è disponibile capacità, Amazon EC2 soddisfa la richiesta immediatamente. Altrimenti, Amazon EC2 attende finché la richiesta non può essere soddisfatta o finché la richiesta non viene annullata.

Puoi utilizzare la procedura guidata di avvio dell'istanza nella console Amazon EC2 o il comando run-instances per richiedere un'istanza Spot nello stesso modo in cui puoi avviare un'istanza. On-Demand Questo metodo è consigliato solo per i seguenti motivi:

- Stai già utilizzando la procedura guidata di avvio dell'istanza o il comando run-instances per avviare le istanze e vuoi semplicemente passare all'avvio On-Demand delle istanze Spot modificando un singolo parametro.
- Non sono necessarie più istanze con diversi tipi di istanza.

Questo metodo non è generalmente consigliato per avviare le istanze Spot perché non puoi specificare più tipi di istanze e non puoi avviare le istanze Spot e le istanze nella stessa richiesta. On-Demand Per i metodi preferiti per il lancio di istanze Spot, che includono il lancio di un parco che include istanze Spot e istanze con più tipi di istanze, consulta On-Demand Qual è il metodo di richiesta Spot migliore da utilizzare?

Se si richiedono più istanze spot alla volta, Amazon EC2 crea richieste di istanza spot separate, così da consentire di monitorare lo stato di ogni richiesta separatamente. Per ulteriori informazioni sul monitoraggio delle richieste di istanza spot, consulta Ottenimento dello stato della richiesta di un'istanza spot.

Console

Per creare una richiesta di istanza spot

I passaggi da 1 a 9 sono gli stessi da utilizzare per avviare un'istanza. On-Demand Al passaggio 10, configuri la richiesta di istanza spot.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore della schermata seleziona la regione.
3. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).
4. (Facoltativo) In)Name and tags (Nome e tag), puoi assegnare un nome all'istanza e aggiungere un tag alla richiesta di istanza spot, all'istanza, ai volumi e alla grafica elastica. Per ulteriori informazioni sui tag, consulta Tagging delle risorse Amazon EC2..
    a. Per Name (Nome), inserisci un nome descrittivo per l'istanza.

Il nome dell'istanza è un tag, dove la chiave è Name (Nome) e il valore è il nome specificato. Se non si specifica un nome, l'istanza può essere identificata dal relativo ID, che viene generato automaticamente all'avvio dell'istanza.

b. Per aggiungere tag alla richiesta di istanza spot, all'istanza, ai volumi e alla grafica elastica, scegli Add additional tags (Aggiungi altri tag). Scegliere Add tag (Aggiungi tag), quindi immettere una chiave e un valore e selezionare il tipo di risorsa da taggare. Scegliere Add tag (Aggiungi tag) per ogni tag aggiuntivo.

5. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), scegli il sistema operativo (SO) per la tua istanza, quindi seleziona un'AMI. Per ulteriori informazioni, consulta Immagini di applicazioni e sistema operativo (Amazon Machine Image).
6. In Instance type (Tipo di istanza), seleziona il tipo di istanza che soddisfa i requisiti per la configurazione hardware e le dimensioni dell'istanza. Per ulteriori informazioni, consulta Tipo di istanza.
7. In Key pair (login) (Coppia di chiavi [login]), scegli una coppia di chiavi esistente oppure scegli Create new key pair (Crea nuova coppia di chiavi) per creane una nuova. Per ulteriori informazioni, consulta Coppie di chiavi Amazon EC2 e istanze Amazon EC2.

> **Important**
>
> Se si sceglie l'opzione Proceed without key pair (Not recommended) (Procedi senza una coppia di chiavi [non consigliato]), non sarà possibile connetterti all'istanza a meno che non si scelga un'AMI configurata per offrire agli utenti un metodo di accesso alternativo.

8. In Network settings (Impostazioni di rete), utilizza le impostazioni predefinite o scegli Edit (Modifica) per configurare le impostazioni di rete come necessario.

   I gruppi di sicurezza fanno parte delle impostazioni di rete e definiscono le regole del firewall per l'istanza. Tali regole specificano quale traffico di rete in entrata deve viene distribuito sulla tua istanza.

   Per ulteriori informazioni, consulta Impostazioni di rete.
9. L'AMI selezionata include uno o più volumi di storage, compreso il volume dispositivo root. In Configure storage (Configura archiviazione), è possibile specificare altri volumi da collegare

all'istanza scegliendo Add New Volume (Aggiungi nuovo volume). Per ulteriori informazioni, consulta Per configurare l'archiviazione.

10. In Advanced details (Dettagli avanzati), configura la richiesta di istanza spot nel modo seguente:

    a. In Opzione di acquisto, seleziona la casella di controllo Richiedi istanze spot.

    b. È possibile mantenere la configurazione predefinita per la richiesta dell'istanza spot o scegliere Customize (Personalizza) (a destra) per specificare impostazioni personalizzate per la richiesta di istanza spot.

    Quando scegli Customize (Personalizza) vengono visualizzati i seguenti campi.

    i. Prezzo massimo: puoi richiedere le istanze Spot al prezzo Spot, con un limite massimo, oppure puoi specificare l'importo massimo che sei disposto a On-Demand pagare.

> **Warning**
>
> Se specifichi un prezzo massimo, le tue istanze verranno interrotte con maggiore frequenza rispetto a quando scegli Nessun prezzo massimo. Se specifichi un prezzo massimo, deve essere superiore a 0,001 USD. Specificando un valore inferiore a 0,001 USD, l'avvio non andrà a buon fine.

- No maximum price (Nessun prezzo massimo): l'istanza spot verrà avviata al prezzo Spot corrente. Il prezzo non supererà mai il On-Demand prezzo. (Consigliato)
- Imposta il prezzo massimo (per instance/hour): puoi specificare l'importo massimo che sei disposto a pagare.
  - Se specifichi un prezzo massimo inferiore al prezzo Spot corrente, l'istanza spot non viene avviata.
  - Se specifichi un prezzo massimo superiore al prezzo Spot corrente, la tua istanza spot viene avviata e viene addebitato il prezzo Spot corrente. Dopo l'esecuzione dell'istanza spot, se il prezzo Spot sale al di sopra del prezzo massimo, Amazon EC2 interrompe l'istanza spot.
  - Indipendentemente dal prezzo massimo specificato, ti verrà sempre addebitato il prezzo spot corrente.

Per esaminare le tendenze del prezzo Spot, consultare Visualizzare la cronologia dei prezzi dell'istanza spot.

ii. Request type (Tipo richiesta): il tipo di richiesta di istanza spot scelto determina cosa succede se l'istanza spot viene interrotta.

- One-time: Amazon EC2 invia una richiesta una tantum per la tua istanza Spot. Se l'istanza spot viene interrotta, la richiesta non viene inviata di nuovo.
- Persistent request (Richiesta persistente): Amazon EC2 invia una richiesta persistente per la tua istanza spot. Se l'istanza spot viene interrotta, la richiesta viene nuovamente inviata per ricostituire l'istanza spot interrotta.

Se non specifichi un valore, il valore predefinito è una richiesta una tantum.

iii. Valid to (Valido per): la data di scadenza di una richiesta di istanza spot persistente.

Questo campo non è supportato per le richieste una tantum. Una richiesta una tantum rimane attiva fino a quando tutte le istanze nella richiesta non vengono avviate o non si annulla la richiesta.

- No request expiry date (Nessuna data di scadenza della richiesta): la richiesta rimane attiva fino a quando non viene annullata.
- Set your request expiry date (Imposta la data di scadenza della richiesta): la richiesta persistente rimane attiva fino alla data specificata o fino alla cancellazione.

iv. Interruption behavior (Comportamento di interruzione): il comportamento scelto determina cosa succede quando un'istanza spot viene interrotta.

- Per le richieste persistenti, i valori validi sono Stop (Arresta) e Hibernate (Iberna). Quando un'istanza viene interrotta, si applicano gli addebiti per l'archiviazione del volume EBS.

> **Note**
>
> Le istanze Spot ora utilizzano la stessa funzionalità di ibernazione delle istanze. On-Demand Per abilitare l'ibernazione, puoi scegliere Iberna qui oppure puoi scegliere Abilita dal campo Comportamento di interruzione/ibernazione che appare più in basso nella procedura guidata

di avvio dell'istanza. Per i prerequisiti di ibernazione, consulta la pagina Prerequisiti per l'ibernazione dell'istanza EC2.

- Per richieste una tantum, è valido solo il valore Terminate (Termina).

Se non specifichi un valore, il valore predefinito è Terminate (Termina), che non è valido per una richiesta di istanza spot persistente. Se mantieni il valore predefinito e provi a lanciare una richiesta di istanza spot persistente, riceverai un errore.

Per ulteriori informazioni, consulta Comportamento delle interruzioni dell'istanza spot.

11. Nel pannello Summary (Riepilogo), per Number of instances (Numero di istanze), inserisci il numero di istanze da avviare.

> **Note**
>
> Amazon EC2 crea una richiesta separata per ciascuna istanza spot.

12. Nel pannello Summary (Riepilogo), rivedi i dettagli della tua istanza e apporta tutte le modifiche necessarie. Dopo aver inviato la richiesta di istanza spot, non è più possibile modificare i parametri della richiesta. È possibile passare direttamente a una sezione nella procedura guidata di avvio delle istanze scegliendo il relativo collegamento nel pannello Summary (Riepilogo). Per ulteriori informazioni, consulta Riepilogo.
13. Quando si è pronti per avviare l'istanza, scegliere Launch instance (Avvia istanza).

    Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio dell'istanza Amazon EC2.

AWS CLI

Per creare una richiesta di istanza spot utilizzando run-instances

Usa il comando run-instances e specifica le opzioni dell'istanza spot nel parametro `--instance-market-options` come indicato di seguito.

```
--instance-market-options file://spot-options.json
```

Di seguito è riportata la struttura dei dati da specificare nel file JSON. Puoi inoltre specificare `ValidUntil` e `InstanceInterruptionBehavior`. Se non specifichi un campo nella struttura dati viene utilizzato il valore predefinito.

Nell'esempio seguente viene creata una richiesta `persistent`.

```
{
  "MarketType": "spot",
  "SpotOptions": {
    "SpotInstanceType": "persistent"
  }
}
```

Per creare una richiesta di istanza Spot utilizzando request-spot-instances

> **Note**
>
> Sconsigliamo caldamente l'uso del comando request-spot-instances per richiedere un'istanza spot perché è un'API legacy senza investimenti pianificati. Per ulteriori informazioni, consulta Qual è il metodo di richiesta Spot migliore da utilizzare?

Utilizzare il comando request-spot-instances per creare una richiesta una tantum.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json
```

Utilizzare il comando request-spot-instances per creare una richiesta persistente.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "persistent" \
    --launch-specification file://specification.json
```

Per i file di esempio delle specifiche di lancio da utilizzare con questi comandi, consultare Esempio delle specifiche di avvio di una richiesta di istanza spot. Se invece si scarica un file delle specifiche di avvio dalla console Richieste Spot, è necessario utilizzare il comando request-spot-

fleet (la console Richieste Spot specifica una richiesta di istanza spot tramite una serie di istanze spot).

PowerShell

Per creare una richiesta di istanza spot

Utilizza il New-EC2Instance cmdlet e specifica le opzioni dell'istanza Spot utilizzando il parametro. `-InstanceMarketOption`

```
-InstanceMarketOptions $marketOptions
```

Crea la struttura dei dati per le opzioni dell'istanza spot come indicato di seguito.

```
$spotOptions = New-Object Amazon.EC2.Model.SpotMarketOptions
$spotOptions.SpotInstanceType="persistent"
$marketOptions = New-Object Amazon.EC2.Model.InstanceMarketOptionsRequest
$marketOptions.MarketType = "spot"
$marketOptions.SpotOptions = $spotOptions
```

Esempio delle specifiche di avvio di una richiesta di istanza spot

Gli esempi seguenti illustrano configurazioni di avvio che è possibile utilizzare con il comando request-spot-instances per creare una richiesta di istanza spot. Per ulteriori informazioni, consulta Gestione delle istanze spot.

> **Important**
>
> Sconsigliamo caldamente l'uso del comando request-spot-instances per richiedere un'istanza spot perché è un'API legacy senza investimenti pianificati. Per ulteriori informazioni, consulta Qual è il metodo di richiesta Spot migliore da utilizzare?.

Esempi

- Esempio 1: Avvio di Istanze spot
- Esempio 2: Avviare le Istanze spot nella zona di disponibilità specificata
- Esempio 3: Avvio di Istanze spot nella sottorete specificata
- Esempio 4: Avvio di un'istanza spot dedicata

Esempio 1: Avvio di Istanze spot

L'esempio seguente non include una zona di disponibilità o una sottorete. Amazon EC2 seleziona automaticamente una zona di disponibilità. Amazon EC2 avvia le istanze nella sottorete predefinita della zona di disponibilità selezionata.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Esempio 2: Avviare le Istanze spot nella zona di disponibilità specificata

L'esempio seguente include una zona di disponibilità. Amazon EC2 avvia le istanze nella sottorete predefinita della zona di disponibilità specificata.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "Placement": {
    "AvailabilityZone": "us-west-2a"
  },
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Esempio 3: Avvio di Istanze spot nella sottorete specificata

L'esempio seguente include una sottorete. Amazon EC2 avvia le istanze nella sottorete specificata. Se il VPC non è predefinito, l'istanza non riceve un indirizzo IPv4 pubblico per impostazione predefinita.

```
{
```

```
  "ImageId": "ami-0abcdef1234567890",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "SubnetId": "subnet-1a2b3c4d",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Per assegnare un indirizzo IPv4 pubblico a un'istanza in un VPC non predefinito, specificare il campo `AssociatePublicIpAddress` come mostrato negli esempi seguenti. Quando specifichi un'interfaccia di rete, devi includere l'ID sottorete e l'ID gruppo di sicurezza tramite l'interfaccia di rete anziché tramite i campi `SubnetId` e `SecurityGroupIds` visualizzati nel blocco di codice precedente.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "InstanceType": "m5.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
      "Groups": [ "sg-1a2b3c4d5e6f7g8h9" ],
      "AssociatePublicIpAddress": true
    }
  ],
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Esempio 4: Avvio di un'istanza spot dedicata

L'esempio seguente richiede un'istanza spot con una tenancy di `dedicated`. Un'istanza spot dedicata deve essere avviata in un VPC.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "c5.8xlarge",
```

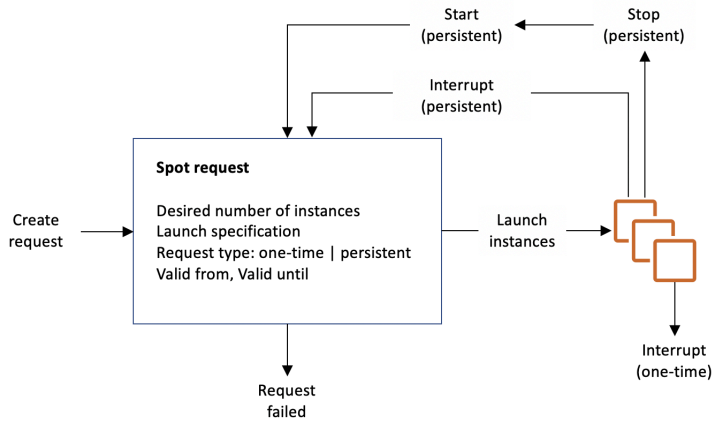
```
  "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
  "Placement": {
    "Tenancy": "dedicated"
  }
}
```

Ottenimento dello stato della richiesta di un'istanza spot

Per aiutarti a monitorare le richieste di istanza spot e a pianificare l'utilizzo delle istanze spot, usa lo stato della richiesta fornito da Amazon EC2. Per esempio, lo stato della richiesta può fornire il motivo per cui la propria richiesta Spot non è ancora stata soddisfatta, oppure elencare i vincoli che impediscono il soddisfacimento della richiesta Spot.

A ogni fase del processo, detto anche ciclo di vita della richiesta Spot, eventi specifici determinano gli stati successivi della richiesta.

La figura seguente mostra come funzionano le richieste delle istanze spot. Il tipo di richiesta (una tantum o persistente) determina se la richiesta viene aperta nuovamente quando Amazon EC2 interrompe un'istanza spot o se un'istanza spot viene arrestata. Se la richiesta è persistente, viene riaperta dopo che l'istanza spot viene interrotta. Se la richiesta è persistente e si arresta l'istanza spot, la richiesta si apre solo dopo aver avviato l'istanza spot.



Indice

- Ottenere informazioni sullo stato della richiesta
- Codici di stato della richiesta Spot
- Evento di approvazione della richiesta di istanza spot EC2
- Modifiche dello stato per una richiesta spot

Ottenere informazioni sullo stato della richiesta

Puoi ottenere informazioni sullo stato della richiesta di istanza spot.

Console

Per ottenere informazioni sullo stato della richiesta

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Spot Requests (Richieste Spot) e selezionare la richiesta Spot.
3. Per verificare lo stato, nella scheda Descrizione selezionare il campo Stato.

AWS CLI

Per ottenere informazioni sullo stato della richiesta

Usa il seguente comando describe-spot-instance-requests.

```
aws ec2 describe-spot-instance-requests --spot-instance-request-
ids sir-0e54a519c9EXAMPLE
```

PowerShell

Per ottenere informazioni sullo stato della richiesta

Utilizza il cmdlet Get-EC2SpotInstanceRequest.

```
Get-EC2SpotInstanceRequest -SpotInstanceRequestId sir-0e54a519c9EXAMPLE
```

Codici di stato della richiesta Spot

Le informazioni sullo stato della richiesta Spot sono composte da un codice di stato, dall'ora di aggiornamento e da un messaggio di stato. Nel loro insieme, queste consentono di determinare la disposizione della richiesta Spot.

I codici di stato della richiesta Spot sono i seguenti:

`az-group-constraint`

Amazon EC2 non può avviare tutte le istanze richieste nella stessa zona di disponibilità.

`bad-parameters`

Uno o più parametri della richiesta Spot non sono validi (per esempio, la AMI specificata non esiste). Il messaggio di stato indica quale dei parametri non è valido.

`canceled-before-fulfillment`

L'utente ha annullato la richiesta Spot prima che fosse soddisfatta.

`capacity-not-available`

Non è disponibile una capacità sufficiente per l'istanza richiesta.

`constraint-not-fulfillable`

La richiesta Spot non può essere soddisfatta poiché uno o più vincoli non sono validi (per esempio, la zona di disponibilità non esiste). Il messaggio di stato indica quale dei vincoli non è valido.

`fulfilled`

La richiesta Spot è `active`, e Amazon EC2 sta lanciando le tue Istanze spot.

`instance-stopped-by-price`

La tua istanza è stata arrestata perché il prezzo Spot ha superato il prezzo massimo.

`instance-stopped-by-user`

L'istanza è stata arrestata perché un utente ha arrestato l'istanza o ha eseguito il comando di arresto dall'istanza.

`instance-stopped-no-capacity`

L'istanza è stata arrestata a causa delle esigenze di gestione della capacità EC2.

`instance-terminated-by-price`

La tua istanza è stata interrotta perché il prezzo Spot ha superato il prezzo massimo. Se la richiesta è persistente, il processo viene riavviato, quindi la richiesta è in attesa di valutazione.

`instance-terminated-by-schedule`

La tua istanza spot è stata terminata alla fine della durata programmata.

`instance-terminated-by-service`

L'istanza è stata terminata da uno stato di arresto.

`instance-terminated-by-user` o `spot-instance-terminated-by-user`

È stata terminata un'istanza spot soddisfatta, quindi lo stato della richiesta è `closed` (a meno che non si tratti di una richiesta persistente) e lo stato dell'istanza è `terminated`.

`instance-terminated-launch-group-constraint`

Una o più istanze del gruppo di avvio è stata terminata, quindi il vincolo del gruppo di avvio non viene più soddisfatto.

`instance-terminated-no-capacity`

L'istanza è stata terminata a causa di processi di gestione della capacità standard.

`launch-group-constraint`

Amazon EC2 non può avviare tutte le istanze richieste nello stesso momento. Tutte le istanze in un gruppo di avvio vengono avviate e terminate insieme.

`limit-exceeded`

È stato superato il limite numerico dei volumi EBS o dello archiviazione del volume totale. Per ulteriori informazioni, consulta Quotas for Amazon EBS nella Guida per l'utente di Amazon EBS.

`marked-for-stop`

L'istanza spot è contrassegnata per l'arresto.

`marked-for-termination`

L'istanza spot è contrassegnata per la terminazione.

`not-scheduled-yet`

La richiesta Spot non viene valutata fino alla data programmata.

`pending-evaluation`

Dopo aver effettuato una richiesta di istanza spot, essa passa allo stato `pending-evaluation` mentre il sistema valuta i parametri della richiesta.

`pending-fulfillment`

Amazon EC2 sta tentando di assegnare le Istanze spot.

`placement-group-constraint`

La richiesta Spot non può essere ancora soddisfatta in quanto l'istanza spot non può essere aggiunta al gruppo di posizionamento in questo momento.

`price-too-low`

La richiesta non può essere ancora soddisfatta in quanto il prezzo massimo è inferiore al prezzo Spot. In questo caso, non viene avviata alcuna istanza e la richiesta rimane `open`.

`request-canceled-and-instance-running`

La richiesta Spot è stata annullata mentre le Istanze spot sono ancora in esecuzione. La richiesta è `cancelled`, ma le istanze rimangono `running`.

`schedule-expired`

La richiesta Spot è scaduta poiché non è stata soddisfatta prima della data specificata.

`system-error`

Si è verificato un errore di sistema imprevisto. Se si tratta di un problema ricorrente, contatta per ricevere assistenza. Supporto AWS

Evento di approvazione della richiesta di istanza spot EC2

Quando una richiesta di istanza Spot viene soddisfatta, Amazon EC2 invia un evento di evasione della richiesta di istanza Spot EC2 ad Amazon. EventBridge Puoi creare una regola per intraprendere un'azione ogni volta che si verifica questo evento, ad esempio richiamando una funzione Lambda o notificando un argomento Amazon SNS.

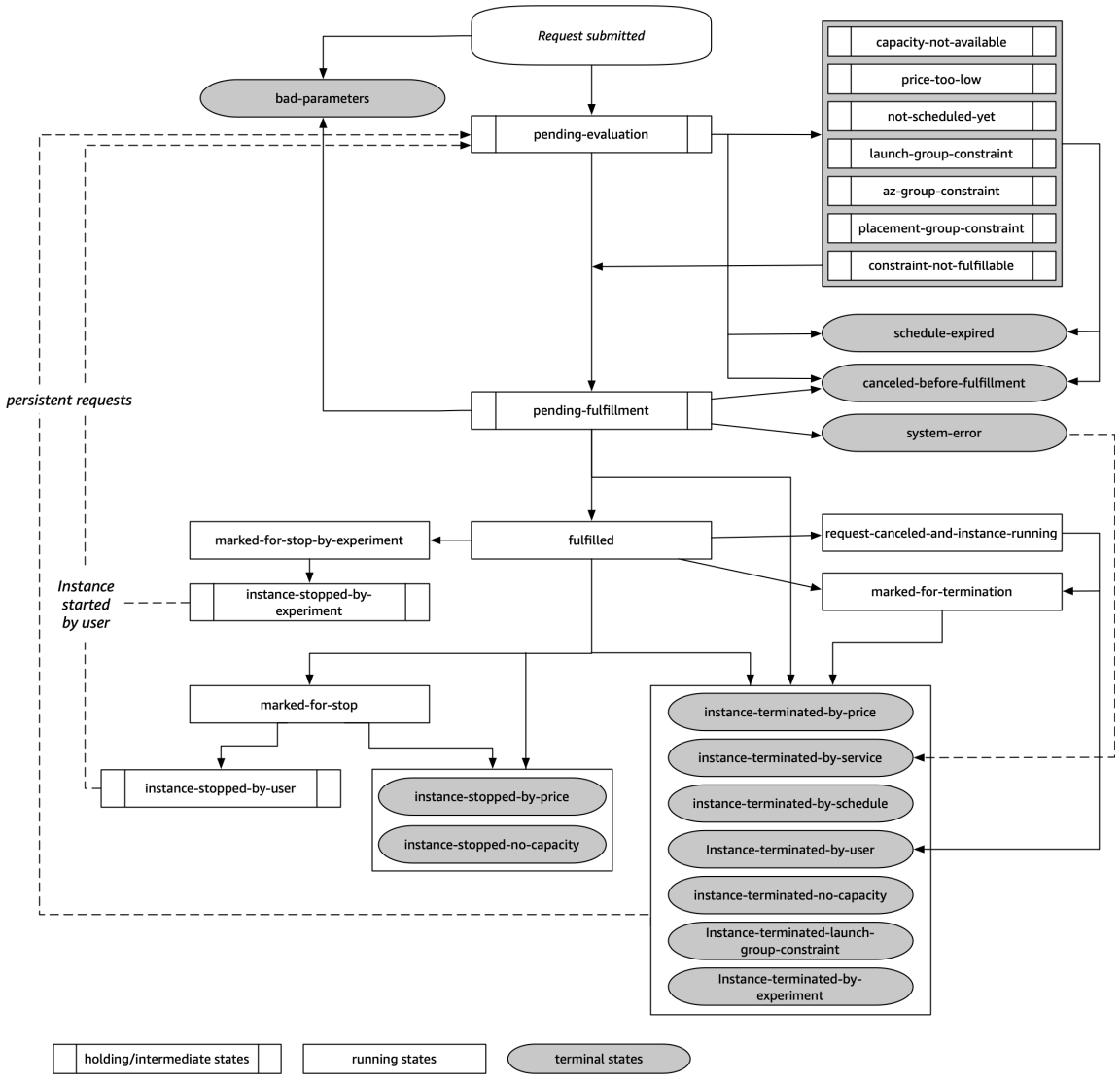
Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "01234567-1234-0123-1234-012345678901",
    "detail-type": "EC2 Spot Instance Request Fulfillment",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "spot-instance-request-id": "sir-0e54a519c9EXAMPLE",
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Per ulteriori informazioni, consulta la Amazon User Guide. EventBridge

Modifiche dello stato per una richiesta spot

Il diagramma seguente mostra i percorsi che la richiesta Spot può seguire durante tutto il suo ciclo di vita, dall'invio alla terminazione. Ogni fase è rappresentata come un nodo e il codice di stato per ogni nodo descrive lo stato della richiesta Spot e dell'istanza spot.



Valutazione in attesa

Appena creata, una richiesta di istanza spot passa allo stato `pending-evaluation`, a meno che uno o più parametri di richiesta non risultino non validi (`bad-parameters`).

Codice di stato	Stato della richiesta	Stato istanza
`pending-evaluation`	open	Non applicabile

Codice di stato	Stato della richiesta	Stato istanza
`bad-parameters`	`closed`	Non applicabile

Sospensione

Se uno o più vincoli di richiesta sono validi ma non possono ancora essere soddisfatti o se non c'è sufficiente capacità, la richiesta va in uno stato di sospensione in attesa che i vincoli vengano soddisfatti. Le opzioni di richiesta influiscono sulla probabilità che la richiesta venga soddisfatta. In assenza di capacità, ad esempio, la richiesta rimane in stato di attesa fino a quando è disponibile capacità. Se si specifica un gruppo di zona di disponibilità, la richiesta rimane in uno stato di sospensione finché il vincolo della zona di disponibilità non viene soddisfatto.

Nel caso si verifichi un'interruzione di una delle zone di disponibilità, è possibile che la capacità EC2 inutilizzata disponibile per le richieste di istanza spot in altre zone di disponibilità possa essere interessata.

Codice di stato	Stato della richiesta	Stato istanza
`capacity-not-available`	`open`	Non applicabile
`price-too-low`	`open`	Non applicabile
`not-scheduled-yet`	`open`	Non applicabile
`launch-group-constraint`	`open`	Non applicabile
`az-group-constraint`	`open`	Non applicabile
`placement-group-constraint`	`open`	Non applicabile
`constraint-not-fulfillable`	`open`	Non applicabile

Terminale in sospeso evaluation/fulfillment

La richiesta di istanza spot può passare allo stato `terminal` se si crea una richiesta valida solo durante un determinato periodo di tempo, che scade prima che la richiesta raggiunga la fase di evasione in sospeso. se si annulla la richiesta o se si verifica un errore di sistema.

Codice di stato	Stato della richiesta	Stato istanza
`schedule-expired`	`cancelled`	Non applicabile
`canceled-before-fulfillment` [1]	`cancelled`	Non applicabile
`bad-parameters`	`failed`	Non applicabile
`system-error`	`closed`	Non applicabile

[1] Se annulli la richiesta.

Adempimento in sospeso

Quando vengono soddisfatti eventuali vincoli specificati, la richiesta spot passa allo stato `pending-fulfillment`.

A questo punto, Amazon EC2 è quasi pronto ad assegnare le istanze richieste. Se il processo si arresta in questo momento, probabilmente è stato annullato dall'utente prima dell'avvio dell'istanza spot. o si è verificato un errore di sistema imprevisto.

Codice di stato	Stato della richiesta	Stato istanza
`pending-fulfillment`	`open`	Non applicabile

Soddisfatta

Quando tutte le specifiche delle istanze spot vengono soddisfatte, la richiesta Spot viene soddisfatta. Amazon EC2 avvia le istanze spot; ciò può richiedere alcuni minuti. Se un'istanza spot viene ibernata

o arrestata durante la sua interruzione, resta in questo stato finché la richiesta non può essere soddisfatta nuovamente o non viene annullata.

Codice di stato	Stato della richiesta	Stato istanza
`fulfilled`	`active`	`pending` → `running`
`fulfilled`	`active`	`stopped` → `running`

Se arresti un'istanza spot, la richiesta Spot passa allo stato `marked-for-stop` o `instance-stopped-by-user` fino a quando l'istanza spot può essere riavviata o la richiesta viene annullata.

Codice di stato	Stato della richiesta	Stato istanza
`marked-for-stop`	`active`	`stopping`
`instance-stopped-by-user`[1]	`disabled` o `cancelled` [2]	`stopped`

[1] Un'istanza spot passa allo stato `instance-stopped-by-user` se arresti l'istanza o esegui il comando di arresto dall'istanza. Dopo aver arrestato l'istanza, è possibile riavviarla. Al riavvio, la richiesta di istanza spot ritorna allo stato `pending-evaluation` e quindi Amazon EC2 avvia una nuova istanza spot quando vengono soddisfatti i vincoli.

[2] Lo stato della richiesta spot è `disabled` se l'istanza spot viene arrestata ma la richiesta non viene annullata. Lo stato della richiesta è `cancelled` se l'istanza spot viene arrestata e la richiesta scade.

Fulfilled-terminal

Le istanze spot continuano l'esecuzione fino a quando è disponibile capacità per il tuo tipo di istanza e non termini l'istanza. Se Amazon EC2 deve terminare le istanze spot, la richiesta spot passa a uno stato terminale. Una richiesta passa allo stato terminale anche se si annulla la richiesta Spot o si terminano le Istanze spot.

Codice di stato	Stato della richiesta	Stato istanza
request-canceled-and-instance-running	cancelled	running
marked-for-stop	active	running
marked-for-termination	active	running
instance-stopped-by-price	disabled	stopped
instance-stopped-by-user	disabled	stopped
instance-stopped-no-capacity	disabled	stopped
instance-terminated-by-price	closed (una tantum), open (persistente)	terminated
instance-terminated-by-schedule	closed	terminated
instance-terminated-by-service	cancelled	terminated
instance-terminated-by-user	closed o cancelled [1]	terminated
instance-terminated-no-capacity	closed (una tantum), open (persistente)	running †
instance-terminated-no-capacity	closed (una tantum), open (persistente)	terminated

Codice di stato	Stato della richiesta	Stato istanza
`instance-terminated-launch-group-constraint`	`closed` (una tantum), `open` (persistente)	`terminated`

[1] Lo stato della richiesta è `closed` se termini l'istanza ma non annulli la richiesta. Lo stato della richiesta è `cancelled` se si termina l'istanza e si annulla la richiesta. Anche se si termina un'istanza spot prima di annullarne la richiesta, potrebbe verificarsi un ritardo prima che Amazon EC2 rilevi che l'istanza spot è stata terminata. In tal caso, lo stato della richiesta può essere `closed` o `cancelled`.

† Quando Amazon EC2 interrompe un'istanza spot se ha bisogno di ripristinare la capacitàe l'istanza è configurata per essere terminata in caso di interruzione, lo stato viene impostato immediatamente su `instance-terminated-no-capacity` (non è impostato su `marked-for-termination`). Tuttavia, l'istanza rimane nella stato `running` per 2 minuti per riflettere il periodo di 2 minuti quando riceve l'avviso di interruzione dell'istanza spot. Dopo 2 minuti, lo stato dell'istanza è impostato su `terminated`.

Esperimenti di interruzione

Puoi utilizzarlo AWS Fault Injection Service per avviare un'interruzione dell'istanza Spot in modo da poter testare come rispondono le applicazioni sulle tue istanze Spot. Se AWS FIS interrompe un'istanza Spot, la tua richiesta Spot entra nello `marked-for-stop-by-experiment` stato e poi nello stato. `instance-stopped-by-experiment` Se AWS FIS termina un'istanza Spot, la tua richiesta Spot entra nello `instance-terminated-by-experiment` stato. Per ulteriori informazioni, consulta the section called "Avvia un'interruzione".

Codice di stato	Stato della richiesta	Stato istanza
`marked-for-stop-by-experiment`	`active`	`running`
`instance-stopped-by-experiment`	`disabled`	`stopped`
`instance-terminated-by-experiment`	`closed`	`terminated`

Richieste persistenti

Quando le istanze spot vengono terminate (dall'utente o da Amazon EC2), se la richiesta Spot è di tipo persistente, essa torna allo stato `pending-evaluation` e Amazon EC2 può avviare una nuova istanza spot quando vengono soddisfatti i vincoli.

Assegnare tag alle richieste di istanza spot

Per categorizzare e gestire le richieste di istanza spot, è possibile contrassegnarle con tag contenenti metadati personalizzati. È possibile assegnare un tag a una richiesta di istanza spot alla sua creazione o successivamente. È possibile assegnare tag utilizzando la console Amazon EC2 o lo strumento da riga di comando.

Quando applichi un tag a una richiesta di istanza spot, alle istanze e ai volumi che vengono avviati dalla richiesta di istanza spot non viene automaticamente applicato il tag. È necessario applicare esplicitamente il tag alle istanze e ai volumi avviati dalla richiesta di istanza spot. Puoi assegnare un tag a un'istanza spot e ai volumi durante l'avvio o successivamente.

Per ulteriori informazioni sul funzionamento dei tag, consultare Tagging delle risorse Amazon EC2..

Indice

- Prerequisiti
- Assegnare tag a una nuova richiesta di istanza spot
- Assegnare tag a una richiesta di istanza spot esistente
- Visualizzare i tag della richiesta di istanza spot

Prerequisiti

Concedi all'utente l'autorizzazione per taggare le risorse. Per ulteriori informazioni sulle policy IAM e sulle policy di esempio, consulta Esempio: aggiunta di tag alle risorse.

La policy IAM creata viene determinata dal metodo utilizzato per creare una richiesta di istanza spot.

- Se usi la procedura guidata per l'avvio dell'istanza o `run-instances` per richiedere le Istanze spot, consulta To grant a user the permission to tag resources when using the launch instance wizard or run-instances.
- Se utilizzi il comando `request-spot-instances` per richiedere istanze spot, consulta To grant a user the permission to tag resources when using request-spot-instances.

Per concedere a un utente l'autorizzazione ad applicare un tag alle risorse quando usa la procedura guidata per l'avvio dell'istanza o run-instances

Creare una policy IAM che include quanto segue:

- L'operazione `ec2:RunInstances`. Ciò concede all'utente l'autorizzazione per avviare un'istanza.
- Per `Resource`, specificare `spot-instances-request`. Ciò consente agli utenti di creare richieste di istanze spot che richiedono istanze spot.
- L'operazione `ec2:CreateTags`. Ciò concede all'utente l'autorizzazione per creare tag.
- Per `Resource`, specificare `*`. Ciò consente agli utenti di applicare un tag a tutte le risorse create durante l'avvio dell'istanza.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLaunchInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagSpotInstanceRequests",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
```

```
    ]
}
```

Quando utilizzi l' RunInstances azione per creare richieste di istanza Spot e taggare le richieste di istanza Spot al momento della creazione, devi essere consapevole del modo in cui Amazon EC2 valuta la `spot-instances-request` risorsa nella RunInstances dichiarazione in cui viene valutata nella policy IAM come segue:

- Se non tagghi una richiesta di istanza Spot al momento della creazione, Amazon EC2 non valuta la `spot-instances-request` risorsa nella dichiarazione. RunInstances
- Se tagghi una richiesta di istanza Spot al momento della creazione, Amazon EC2 valuta la `spot-instances-request` risorsa contenuta nell'istruzione. RunInstances

Pertanto, per la risorsa `spot-instances-request`, alla policy IAM si applicano le seguenti regole:

- Se lo utilizzi RunInstances per creare una richiesta di istanza Spot e non intendi etichettare la richiesta di istanza Spot al momento della creazione, non è necessario consentire esplicitamente la `spot-instances-request` risorsa; la chiamata avrà esito positivo.
- Se lo utilizzi RunInstances per creare una richiesta di istanza Spot e intendi etichettare la richiesta di istanza Spot al momento della creazione, devi includere la `spot-instances-request` risorsa nell'istruzione RunInstances allow, altrimenti la chiamata avrà esito negativo.
- Se lo usi RunInstances per creare una richiesta di istanza Spot e intendi etichettare la richiesta di istanza Spot al momento della creazione, devi specificare la `spot-instances-request` risorsa o includere un `*` carattere jolly nell'istruzione CreateTags allow, altrimenti la chiamata avrà esito negativo.

Per policy IAM di esempio, incluse le policy non supportate per le richieste di istanza spot, consulta Utilizzo delle Istanze spot.

Come concedere a un utente l'autorizzazione ad applicare un tag alle risorse quando si utilizza request-spot-instances

Creare una policy IAM che include quanto segue:

- L'operazione `ec2:RequestSpotInstances`. Ciò concede all'utente l'autorizzazione per creare una richiesta di istanza spot.

- L'operazione `ec2:CreateTags`. Ciò concede all'utente l'autorizzazione per creare tag.
- Per `Resource`, specificare `spot-instances-request`. Ciò consente agli utenti di applicare il tag solo alla richiesta di istanza spot.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotInstanceRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:RequestSpotInstances",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-instances-
request/*"
        }
    ]
}
```

Assegnare tag a una nuova richiesta di istanza spot

Negli PowerShell esempi seguenti AWS CLI , configura la richiesta di istanza Spot come segue:

- Per `ResourceType`, specificare `spot-instances-request`. Indicando un altro valore, la richiesta di istanza spot non riesce.
- Per `Tags`, specificare la coppia chiave-valore. È possibile specificare più coppie chiave-valore.

Console

Per assegnare tag a una nuova richiesta di istanza spot

1. Seguire la procedura Gestione delle istanze spot.
2. Per aggiungere un tag, scegli Aggiungi tag nella pagina Aggiungi tag e immetti la chiave e il valore per il tag. Scegli Aggiungi un altro tag per ogni tag aggiuntivo.

Per ogni tag, è possibile assegnare lo stesso tag alla richiesta di istanza spot, alle istanze spot e ai volumi. Per applicare tag a tutti e tre, assicurarsi che Instances (Istanze), Volumes (Volumi) e Requests (Richieste) siano selezionati. Per applicare solo uno o due tag, assicurati che le risorse a cui vuoi applicare il tag siano selezionate e che le altre risorse siano cancellate.

3. Completare i campi obbligatori per creare una richiesta di istanza spot, quindi scegliere Launch (Avvia). Per ulteriori informazioni, consulta Gestione delle istanze spot.

AWS CLI

Per assegnare tag a una nuova richiesta di istanza spot

Usa il comando request-spot-instances con l'opzione `--tag-specification`.

La specifica di tag aggiunge due tag alla richiesta di istanza spot: `Environment=Production` e `Cost-Center=123`.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json \
    --tag-specification 'ResourceType=spot-instances-
request,Tags=[{Key=Environment,Value=Production},{Key=Cost-Center,Value=123}]'
```

PowerShell

Per assegnare tag a una nuova richiesta di istanza spot

Utilizza il Request-EC2SpotInstance cmdlet con il `-TagSpecification` parametro.

```
-TagSpecification $tagspec
```

La specifica di tag è definita come indicato di seguito. Aggiunge due tag alla richiesta di istanza spot: `Environment=Production` e `Cost-Center=123`.

```
$tag1 = @{Key="Environment"; Value="Production"}
$tag2 = @{Key="Cost-Center"; Value="123"}
$tagspec = New-Object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "spot-instances-request"
```

```
$tagspec.Tags = @($tag1,$tag2)
```

Assegnare tag a una richiesta di istanza spot esistente

Console

Per assegnare tag a una richiesta di istanza spot esistente

Dopo aver creato una richiesta di istanza spot, è possibile aggiungere tag alla richiesta del parco istanze spot utilizzando la console.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di istanza spot.
4. Scegliere la scheda Tags e scegliere Create Tag (Crea tag).

Per assegnare tag a un'istanza spot esistente utilizzando la console

Dopo che la richiesta di istanza spot ha avviato l'istanza spot, puoi aggiungere i tag all'istanza utilizzando la console. Per ulteriori informazioni, consulta Aggiungere tag utilizzando la console.

AWS CLI

Per assegnare tag a una richiesta di istanza spot o istanza spot esistente

Utilizzare il comando create-tags per aggiungere un tag alle risorse esistenti. Nel seguente esempio, alla richiesta di istanza spot e all'istanza spot esistenti viene assegnato il tag `purpose=test`.

```
aws ec2 create-tags \
    --resources sir-0e54a519c9EXAMPLE i-1234567890abcdef0 \
    --tags Key=purpose,Value=test
```

PowerShell

Per assegnare tag a una richiesta di istanza spot o istanza spot esistente

Utilizza il cmdlet New-EC2Tag. Il seguente esempio aggiunge il tag `purpose=test` alla richiesta di istanza spot e all'istanza spot esistenti.

```
New-EC2Tag `
    -Resource sir-0e54a519c9EXAMPLE, i-1234567890abcdef0 `
    -Tag @{Key="purpose"; Value="test"}
```

Visualizzare i tag della richiesta di istanza spot

Console

Per visualizzare i tag della richiesta di istanza spot

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Selezionare la richiesta di istanza spot e scegliere la scheda Tags.

AWS CLI

Per descrivere i tag della richiesta di istanza spot

Utilizza il comando describe-spot-instance-requests per visualizzare la configurazione della richiesta di istanza spot specificata, che include tutti i tag specificati per la richiesta.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-0e54a519c9EXAMPLE \
    --query "SpotInstanceRequests[*].Tags"
```

Di seguito è riportato un output di esempio.

```
[
    [
        {
            "Key": "Environment",
            "Value": "Production"
        },
        {
            "Key": "Department",
            "Value": "101"
        }
    ]
]
```

PowerShell

Per descrivere i tag della richiesta di istanza spot

Utilizza il cmdlet Get-EC2SpotInstanceRequest.

```
(Get-EC2SpotInstanceRequest `
    -SpotInstanceRequestId sir-0e54a519c9EXAMPLE).Tags
```

Di seguito è riportato un output di esempio.

```
Key         Value
---         -----
Environment Production
Department  101
```

Annulla una richiesta di istanza spot

È possibile annullare la richiesta di istanza spot se non la si desidera più. È possibile annullare solo le richieste di istanza spot che risultano `open`, `active` o `disabled`.

- La richiesta di istanza spot risulta `open` quando la richiesta non è stata ancora soddisfatta e non è stata avviata alcuna istanza.
- La richiesta di istanza spot risulta `active` quando la richiesta è stata soddisfatta e, di conseguenza, sono state avviate le istanze spot.
- La richiesta di istanza spot risulta `disabled` quando si arresta l'istanza spot.

Se la richiesta di istanza spot risulta `active` e ha un'istanza spot associata in esecuzione, l'annullamento della richiesta non termina l'istanza. Per ulteriori informazioni sulla terminazione delle istanze spot, consulta Terminare un'istanza spot.

Console

Per annullare una richiesta di istanza spot

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di istanza spot.

4. Scegli Operazioni e Annulla richiesta.
5. (Facoltativo) Se si è finito con le Istanze spot associate, è possibile terminarle. Nella finestra di dialogo Elimina richiesta Spot seleziona Termina istanze, quindi scegli Conferma.

AWS CLI

Per annullare una richiesta di istanza spot

Usa il seguente comando cancel-spot-instance-requests.

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-
ids sir-0e54a519c9EXAMPLE
```

PowerShell

Per annullare una richiesta di istanza spot

Utilizza il cmdlet Stop-EC2SpotInstanceRequest.

```
Stop-EC2SpotInstanceRequest -SpotInstanceRequestId sir-0e54a519c9EXAMPLE
```

Gestione delle istanze spot

Amazon EC2 avvia un'istanza spot quando è disponibile capacità. Un'istanza spot viene eseguita fino a quando non viene interrotta o fino a quando non la si termina.

Indice

- Individuazione delle istanze spot
- Individuare le istanze avviate da una richiesta specifica
- Arrestare un'istanza spot
- Avviare un'istanza spot
- Terminare un'istanza spot

Individuazione delle istanze spot

Un'istanza Spot viene visualizzata nella pagina Istanze della console, insieme alle istanze. On-Demand Utilizza la procedura seguente per individuare le tue istanze spot.

Console

Per individuare le istanze spot

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Per trovare tutte le istanze spot, nel pannello di ricerca, scegli Ciclo di vita dell'istanza=spot.
4. Per verificare che un'istanza sia un'istanza spot, selezionala, scegli la scheda Dettagli e controlla il valore di Ciclo di vita. Il valore per un'istanza Spot è `spot` e il valore per un' On-Demand istanza è. `normal`

AWS CLI

Per individuare le istanze spot

Usa il seguente comando describe-instances.

```
aws ec2 describe-instances --filters "Name=instance-lifecycle,Values=spot"
```

Determinazione di un'istanza spot

Usa il seguente comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[*].InstanceLifecycle" \
    --output text
```

Se l'output è `spot`, l'istanza è di tipo spot. Se non è presente alcun output, l'istanza è un' On-Demand istanza.

PowerShell

Per individuare le istanze spot

Utilizza il cmdlet Get-EC2Instance.

```
Get-EC2Instance -Filter @{Name="instance-lifecycle"; Values="spot"}
```

Determinazione di un'istanza spot

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.InstanceLifecycle
```

Se l'output è `Spot`, l'istanza è di tipo spot. Se non è presente alcun output, l'istanza è un' On-Demand istanza.

Individuare le istanze avviate da una richiesta specifica

Utilizza la seguente procedura per individuare le istanze spot avviate da una richiesta specifica di istanza spot o parco istanze spot.

Console

Per individuare le istanze spot per una richiesta

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot). L'elenco contiene sia le richieste di istanza spot che le richieste di parco istanze spot.
3. Se una richiesta di istanza spot viene soddisfatta, l'ID dell'istanza spot è Capacità. Per un Parco istanze spot, Capacity (Capacità) indica quanta capacità richiesta è stata soddisfatta. Per visualizzare gli ID delle istanze in un Parco istanze spot, scegliere la freccia per l'espansione o selezionare il parco istanze e scegliere Instances (Istanze).
4. Per un parco istanze spot, Capacità indica quanta capacità richiesta viene soddisfatta. Per visualizzare gli ID delle istanze in un parco istanze spot, scegli l'ID del parco per aprire la relativa pagina dei dettagli e individuare il pannello Istanze.

AWS CLI

Per individuare le istanze spot per una richiesta

Usa il seguente comando describe-spot-instance-requests.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-0e54a519c9EXAMPLE \
    --query "SpotInstanceRequests[*].{ID:InstanceId}"
```

Di seguito è riportato un output di esempio:

```
[
    {
        "ID": "i-1234567890abcdef0"
    },
    {
        "ID": "i-0598c7d356eba48d7"
    }
]
```

PowerShell

Per individuare le istanze spot per una richiesta

Utilizza il cmdlet Get-EC2SpotInstanceRequest.

```
(Get-EC2SpotInstanceRequest -SpotInstanceRequestId sir-0e54a519c9EXAMPLE).InstanceId
```

Arrestare un'istanza spot

Se al momento non hai bisogno delle istanze spot, ma desideri riavviarle in un secondo momento senza perdere i dati persistenti nel volume Amazon EBS, puoi arrestarle. I passaggi per arrestare un'istanza Spot sono simili a quelli per arrestare un' On-Demand istanza.

> **Note**
>
> Durante l'arresto di un'istanza spot, è possibile modificare alcuni attributi dell'istanza, ma non il tipo di istanza.
> Non addebitiamo costi per l'utilizzo di un'istanza spot arrestata o per il trasferimento di dati, ma li addebitiamo per l'archiviazione di tutti i volumi Amazon EBS.

Limitazioni

- È possibile arrestare un'istanza spot solo se l'istanza spot è stata avviata da una richiesta Spot `persistent`.
- Non è possibile arrestare un'istanza spot se la richiesta Spot associata è stata annullata. Se la richiesta dell'istanza spot viene annullata, è possibile solo terminare l'istanza spot.
- Non è possibile interrompere un'istanza spot se fa parte di un parco istanze o un gruppo di avvio o di un gruppo di zone di disponibilità.

Console

Per arrestare un'istanza spot

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza spot. Se non hai salvato l'ID dell'istanza spot, consulta the section called "Individuazione delle istanze spot".
4. Scegli Instance state (Stato istanza), Stop instance (Arresta istanza).
5. Quando viene richiesta la conferma, selezionare Stop (Arresta).

AWS CLI

Per arrestare un'istanza spot

Utilizza il comando stop-instances per arrestare manualmente le istanze spot.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Per arrestare un'istanza spot

Utilizza il cmdlet Stop-EC2Instance.

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0
```

Avviare un'istanza spot

È possibile avviare un'istanza spot che hai arrestato in precedenza.

Prerequisiti

È possibile avviare un'istanza spot solo se:

- L'istanza spot è stata arrestata manualmente.
- L'istanza Spot è un' EBS-backed istanza.
- La capacità dell'istanza spot è disponibile.
- Il prezzo Spot è inferiore al prezzo massimo.

Limitazioni

- Non è possibile avviare un'istanza spot se fa parte del parco istanze o del gruppo di avvio o di un gruppo di zone di disponibilità.

I passaggi per avviare un'istanza Spot sono simili a quelli per avviare un' On-Demand istanza.

Console

Per avviare un'istanza spot

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza spot. Se non hai salvato l'ID dell'istanza spot, consulta the section called "Individuazione delle istanze spot".
4. Scegli Instance state (Stato istanza), Start instance (Avvia istanza).

AWS CLI

Per avviare un'istanza spot

Utilizza il comando start-instances per avviare manualmente le istanze spot.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Per avviare un'istanza spot

Utilizza il cmdlet Start-EC2Instance.

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

Terminare un'istanza spot

> **Warning**
>
> La terminazione di un'istanza è permanente e irreversibile.

Dopo aver terminato un'istanza, non puoi più connetterti a essa e non puoi ripristinarla. Inoltre, tutti i volumi Amazon EBS collegati e configurati per essere eliminati in caso di terminazione vengono eliminati in modo definitivo e non possono essere recuperati. Tutti i dati archiviati nei volumi di archivio dell'istanza vengono persi in modo definitivo. Per ulteriori informazioni, consulta Come funziona la terminazione delle istanze.
Prima di terminare un'istanza, assicurati di aver eseguito il backup di tutti i dati che devi mantenere dopo la terminazione sull'archivio persistente.

Se si termina un'istanza spot in esecuzione o arrestata che era stata avviata da una richiesta Spot persistente, la richiesta dell'istanza spot passa allo stato `open` per consentire che venga avviata una nuova istanza spot. Per garantire che non venga avviata una nuova istanza spot, è necessario annullare prima la richiesta Spot.

Se si annulla una richiesta dell'istanza spot `active` che ha un'istanza spot in esecuzione, l'istanza spot in esecuzione non viene terminata automaticamente ma sarà necessario terminarla manualmente.

Se si annulla una richiesta dell'istanza spot `disabled` che ha un'istanza spot interrotta, l'istanza spot interrotta viene terminata automaticamente dal servizio Spot di Amazon EC2. Potrebbe verificarsi un breve ritardo tra l'annullamento della richiesta dell'istanza spot e il momento in cui il servizio Spot termina l'istanza spot.

Per ulteriori informazioni, consulta Annulla una richiesta di istanza spot.

Console

Per terminare un'istanza spot manualmente

1. Prima di terminare l'istanza, verificare che l'operazione non comporti la perdita dei dati. A tale scopo, controllare che i volumi Amazon EBS non vengano eliminati dopo l'interruzione e assicurarsi di aver copiato i dati necessari dai volumi di archivio istanza nell'archiviazione persistente, ad esempio Amazon EBS o Amazon S3.
2. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
3. Nel riquadro di navigazione, scegliere Instances (Istanze).
4. Seleziona l'istanza spot. Se non hai salvato l'ID dell'istanza spot, consulta the section called "Individuazione delle istanze spot".
5. Scegli Stato dell'istanza, Termina (elimina) istanza.

6. Quando viene richiesta la conferma, scegli Termina (elimina).

AWS CLI

Per terminare un'istanza spot manualmente

Utilizza il comando terminate-instances per terminare manualmente le istanze spot.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

PowerShell

Per terminare un'istanza spot manualmente

Utilizza il cmdlet Remove-EC2Instance.

```
Remove-EC2Instance -InstanceId i-1234567890abcdef0
```

Interruzioni dell'istanza spot

È possibile lanciare Istanze spot sulla capacità EC2 di riserva per risparmi notevoli, per poi restituirle quando Amazon EC2 ha nuovamente bisogno della capacità. Quando Amazon EC2 recupera un'istanza Spot, chiamiamo questo evento un'interruzione dell'istanza Spot.

La richiesta di Istanze Spot può variare significativamente da un momento all'altro e anche la disponibilità di Istanze Spot può variare significativamente a seconda di quante istanze EC2 inutilizzate sono disponibili. È sempre possibile che l'istanza spot venga interrotta. Di seguito sono elencati i possibili motivi per cui Amazon EC2 potrebbe interrompere le Istanze spot:

Capacity

Amazon EC2 può interrompere l'istanza spot quando ne ha bisogno. EC2 recupera l'istanza principalmente per riutilizzare la capacità, ma il recupero può verificarsi anche per altri motivi, come la manutenzione dell'host o la disattivazione dell'hardware.

Prezzo

Il prezzo spot è inferiore al prezzo massimo.

Nella richiesta spot puoi specificare il prezzo massimo. Se specifichi un prezzo massimo, tuttavia, le tue istanze verranno interrotte con maggiore frequenza rispetto a quando non lo specifichi.

Vincoli

Se la richiesta include un vincolo, come un gruppo di avvio o un gruppo della zona di disponibilità, queste istanze spot vengono terminate come gruppo quando il vincolo non può più essere soddisfatto.

Quando Amazon EC2 interrompe un'istanza spot, termina, arresta o iberna l'istanza, a seconda del comportamento di interruzione specificato durante la creazione della richiesta spot.

Indice

- Comportamento delle interruzioni dell'istanza spot
- Preparazione alle interruzioni dell'istanza spot
- Avvio dell'interruzione di un'istanza spot
- Avvisi di interruzione dell'istanza spot
- Cercare Istanze spot interrotte
- Determinare se Amazon EC2 ha terminato un'istanza spot
- Fatturazione delle Istanze spot interrotte

Comportamento delle interruzioni dell'istanza spot

Puoi specificare il comportamento di interruzione quando crei una richiesta spot. Di seguito sono riportati i possibili comportamenti di interruzione:

- Interrompi
- Ibernazione
- Interruzione

Il comportamento predefinito per Amazon EC2 è terminare le istanze spot quando vengono interrotte.

Arrestare delle Istanze spot interrotte

È possibile specificare che Amazon EC2 arresti le istanze spot quando vengono interrotte. Il tipo di richiesta di istanza spot deve essere `persistent`. Non è possibile specificare un gruppo di avvio nella richiesta di istanza spot. Per EC2 Fleet o il parco istanze spot, la richiesta deve essere `maintain`.

Considerazioni

- Solo Amazon EC2 può riavviare un'istanza spot interrotta.
- Per un'istanza spot avviata da una richiesta di istanza spot `persistent` , Amazon EC2 riavvia l'istanza arrestata quando la capacità è disponibile nella stessa zona di disponibilità e per lo stesso tipo di istanza dell'istanza arrestata (è necessario utilizzare la stessa specifica).
- Durante l'arresto di un'istanza spot, è possibile modificare alcuni attributi dell'istanza, ma non il tipo di istanza. Se si distacca o si elimina un volume EBS, questo non è collegato all'avvio dell'istanza spot. Se si distacca il volume root e Amazon EC2 tenta di avviare l'istanza spot, l'istanza non verrà avviata e Amazon EC2 terminerà l'istanza arrestata.
- È possibile terminare un'istanza spot durante il suo arresto.
- Se si annulla una richiesta dell'istanza spot, un parco istanze EC2 o un parco istanze spot, Amazon EC2 termina tutte le istanze spot associate arrestate.
- Mentre un'istanza spot viene arrestata, il costo viene addebitato solo per i volumi EBS, che vengono conservati. Con il Parco istanze EC2 e il Parco istanze spot, se sono presenti molte istanze arrestate, è possibile superare il limite numerico di volumi EBS per il proprio account. Per ulteriori informazioni su come viene addebitato l'addebito quando un'istanza spot viene interrotta, consultare Fatturazione delle Istanze spot interrotte.
- Assicurarsi di avere familiarità con le implicazioni dell'arresto di un'istanza. Per ulteriori informazioni su cosa accade quando un'istanza viene arrestata, consultare Differenze tra gli stati dell'istanza.

Ibernare le Istanze spot interrotte

È possibile specificare che Amazon EC2 iberni le istanze spot quando vengono interrotte. Per ulteriori informazioni, consulta Metti in ibernazione la tua istanza Amazon EC2.

Amazon EC2 offre ora la stessa esperienza di ibernazione per le istanze Spot attualmente disponibile per le istanze. On-Demand Offre un supporto più ampio, dove per l'ibernazione delle istanze spot ora sono offerte le seguenti caratteristiche:

- Più AMI supportate
- Più famiglie di istanze supportate
- User-initiated ibernazione

Terminare le Istanze spot interrotte

Quando Amazon EC2 interrompe un'istanza spot, termina l'istanza per impostazione predefinita, a meno che non specifichi un comportamento di interruzione diverso, ad esempio l'arresto o l'ibernazione. Per ulteriori informazioni, consulta Terminare le istanze Amazon EC2.

Preparazione alle interruzioni dell'istanza spot

La richiesta di Istanze spot può variare significativamente da un momento all'altro e anche la disponibilità di Istanze spot può variare significativamente a seconda di quante istanze EC2 inutilizzate sono disponibili. È sempre possibile che l'istanza spot venga interrotta. Pertanto, è necessario assicurarsi che l'applicazione sia preparata per un'interruzione dell'istanza spot.

Consigliamo di seguire queste best practice in modo da essere pronti all'interruzione dell'istanza spot.

- Creare la propria richiesta Spot utilizzando un gruppo Auto Scaling. Se le istanze spot vengono interrotte, il gruppo Auto Scaling lancerà automaticamente le istanze sostitutive. Per ulteriori informazioni, consulta la sezione relativa ai Gruppi con dimensionamento automatico con più tipi di istanze e opzioni di acquisto nella Guida per l'utente di Amazon EC2 Auto Scaling.
- Accertarsi che l'istanza sia pronta non appena la richiesta viene soddisfatta utilizzando un'Amazon Machine Image (AMI) che contiene la configurazione software richiesta. È possibile anche utilizzare i dati dell'utente per eseguire i comandi al startup.
- Quando l'istanza viene arrestata o terminata, i dati nei volumi dell'archivio dell'istanza vengono persi. Esegui il backup di tutti i dati importanti contenuti nei volumi dell'archivio dell'istanza in un archivio più persistente, ad esempio Amazon S3, Amazon EBS o Amazon DynamoDB.
- È opportuno archiviare regolarmente i dati importanti in un luogo che non sia interessato dalla terminazione dell'istanza spot. Per esempio, è possibile utilizzare Amazon S3, Amazon EBS o DynamoDB.
- Dividere il lavoro in piccole attività (utilizzando un'architettura basata su griglia, Hadoop o coda) o utilizzare i checkpoint in modo da poter salvare il lavoro con frequenza.
- Amazon EC2 emette un segnale di suggerimento di ribilanciamento dell'istanza spot quando l'istanza presenta un rischio elevato di interruzione. È possibile fare affidamento sul suggerimento di ribilanciamento per gestire in modo proattivo le interruzioni dell'istanza spot senza dover attendere l'avviso di interruzione dell'istanza spot dopo due minuti. Per ulteriori informazioni, consulta Raccomandazioni per il ribilanciamento delle istanze EC2.
- Utilizzare gli avvisi di interruzione dell'istanza spot dopo due minuti per monitorare lo stato delle proprie istanze spot. Per ulteriori informazioni, consulta Avvisi di interruzione dell'istanza spot.

- Anche se compiamo ogni sforzo per fornire questi avvisi con il massimo anticipo possibile, può accadere che l'istanza spot venga terminata prima che gli avvisi siano inviati. Verificare l'applicazione per assicurarsi che gestisca correttamente un'interruzione improvvisa dell'istanza, anche se si stanno monitorando i segnali di raccomandazione di ribilanciamento e gli avvisi di interruzione. È possibile eseguire questa operazione eseguendo l'applicazione utilizzando un' On-Demand istanza e quindi terminando l' On-Demand istanza personalmente.
- Esegui un esperimento di iniezione controllata dei guasti AWS Fault Injection Service per verificare come risponde l'applicazione quando l'istanza Spot viene interrotta. Per ulteriori informazioni, consulta Tutorial: test delle interruzioni dell'istanza Spot tramite AWS FIS nella Guida per l'utente di AWS Fault Injection Service .

Avvio dell'interruzione di un'istanza spot

Puoi selezionare una richiesta di istanza spot o una richiesta di serie di istanze spot nella console di Amazon EC2 e avviare un'interruzione dell'istanza spot in modo da poter provare in che modo le applicazioni sulle tue istanze spot gestiscono le interruzioni. Quando avvii l'interruzione di un'istanza spot, Amazon EC2 segnala che l'istanza spot verrà interrotta entro due minuti e quindi, dopo due minuti, l'istanza spot viene interrotta.

Il servizio sottostante che esegue l'interruzione dell'istanza Spot è AWS Fault Injection Service ().AWS FIS Per informazioni su AWS FIS, consulta AWS Fault Injection Service.

> **Note**
>
> I comportamenti di interruzione sono `terminate`, `stop` e `hibernate`. Se imposti il comportamento di interruzione su `hibernate`, quando avvii l'interruzione di un'istanza spot il processo di ibernazione inizia immediatamente.

L'avvio di un'interruzione dell'istanza Spot è supportato in tutti Regioni AWS tranne Asia Pacifico (Jakarta), Asia Pacifico (Osaka), Cina (Pechino), Cina (Ningxia) e Medio Oriente (Emirati Arabi Uniti).

Indice

- Avvio dell'interruzione di un'istanza spot
- Verifica dell'interruzione dell'istanza spot
- Quote

Avvio dell'interruzione di un'istanza spot

Puoi usare la console EC2 per avviare rapidamente l'interruzione di un'istanza spot. Quando si seleziona una richiesta di istanza spot, è possibile avviare l'interruzione di un'istanza spot. Quando si seleziona una richiesta di una serie di istanze spot, è possibile avviare l'interruzione di più istanze spot in una sola volta.

Per esperimenti più avanzati per testare le interruzioni di Spot Instance, puoi creare i tuoi esperimenti utilizzando la console. AWS FIS

Avvio dell'interruzione di una istanza spot in una richiesta di istanza spot tramite la console EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Richieste spot.
3. Seleziona la richiesta di un'istanza spot e scegli Actions (Operazioni), Initiate interruption (Avvia interruzione). Per avviare un'interruzione non è possibile selezionare più richieste di istanza spot.
4. Nella finestra di dialogo Initiate Spot Instance interruption (Avvia interruzione istanza spot), in Service access (Accesso al servizio), usa il ruolo predefinito o scegli un ruolo esistente. Per scegliere un ruolo esistente, seleziona Usa un ruolo di servizio esistente quindi per Ruolo IAM seleziona il ruolo da utilizzare.
5. Quando sei pronto all'avvio dell'interruzione di un'istanza spot, scegli Initiate interruption (Avvia interruzione).

Avvio dell'interruzione di una o più istanze spot in una richiesta di istanze spot tramite la console EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Richieste spot.
3. Seleziona la richiesta di una serie di istanze spot e scegli Operazioni, Avvia interruzione. Per avviare un'interruzione non è possibile selezionare più richieste di serie di istanze spot.
4. Nella finestra di dialogo Specifica il numero di istanze spot, in Numero di istanze da interrompere, inserisci il numero di istanze spot da interrompere, quindi scegli Conferma.

> **Note**
>
> Il numero non può superare il numero di istanze Spot del parco istanze o la tua quota per il numero di istanze Spot che AWS FIS possono interrompere per esperimento.

5. Nella finestra di dialogo Initiate Spot Instance interruption (Avvia interruzione istanza spot), in Service access (Accesso al servizio), usa il ruolo predefinito o scegli un ruolo esistente. Per scegliere un ruolo esistente, seleziona Usa un ruolo di servizio esistente quindi per Ruolo IAM seleziona il ruolo da utilizzare.
6. Quando sei pronto all'avvio dell'interruzione di un'istanza spot, scegli Initiate interruption (Avvia interruzione).

Per creare esperimenti più avanzati per testare le interruzioni delle istanze Spot, utilizza AWS FIS console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Richieste spot.
3. Scegli Actions (Operazioni), Create advanced experiments (Crea esperimenti avanzati).

   Si apre la AWS FIS console. Per ulteriori informazioni, consulta Tutorial: Test delle interruzioni di istanze spot tramite AWS FIS nella Guida per l'utente di AWS Fault Injection Service .

Verifica dell'interruzione dell'istanza spot

Dopo l'avvio dell'interruzione, si verifica quanto segue:

- L'istanza spot riceve una raccomandazione di ribilanciamento dell'istanza.
- Un avviso di interruzione dell'istanza Spot viene emesso due minuti prima dell' AWS FIS interruzione dell'istanza.
- Dopo due minuti, l'istanza spot viene interrotta.
- Un'istanza Spot che è stata interrotta da AWS FIS rimane bloccata finché non la riavvii.

Verificare che l'istanza sia stata interrotta dopo l'avvio dell'interruzione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, apri Spot Requests (Richieste spot) e Instances (Istanze) in schede o finestre separate del browser.
3. Per le richieste Spot, seleziona la richiesta di istanza spot o la richiesta della serie di istanze spot. Lo stato iniziale è `fulfilled`. Dopo l'interruzione dell'istanza, lo stato cambia come segue, a seconda del comportamento dell'interruzione:

- `terminate`: lo stato diventa `instance-terminated-by-experiment`.
- `stop`: lo stato diventa `marked-for-stop-by-experiment` e poi `instance-stopped-by-experiment`.

4. Per Istanze, seleziona l'istanza spot. Lo stato iniziale è `Running`. Due minuti dopo la ricezione dell'avviso di interruzione dell'istanza spot, lo stato cambia come segue, a seconda del comportamento dell'interruzione:
   - `stop`: lo stato diventa `Stopping` e poi `Stopped`.
   - `terminate`: lo stato diventa `Shutting-down` e poi `Terminated`.

Quote

La tua Account AWS è la seguente quota predefinita per il numero di istanze Spot che AWS FIS possono essere interrotte per esperimento.

Nome	Predefinita	Adattabile	Description
Obiettivo SpotInstances per aws:ec2:send-spot-instance-interruptions	Ogni regione supportata: 5	Sì	Il numero massimo di istanze spot a cui aws:ec2:send-spot-instance-interruptions può puntare quando identifichi le destinazioni tramite i tag, per esperimento.

È possibile richiedere un aumento della quota. Per ulteriori informazioni, consulta Richiesta di un aumento delle quote nella Guida per l'utente di Service Quotas.

Per visualizzare tutte le quote per, apri la console Service Quotas. AWS FIShttps://console.aws.amazon.com/servicequotas/home Nel riquadro di navigazione, scegli Servizi AWS , quindi seleziona AWS Fault Injection Service. Puoi visualizzare tutte le quote di AWS Fault Injection Service anche nella Guida per l'utente di AWS Fault Injection Service .

Avvisi di interruzione dell'istanza spot

Una notifica di interruzione di istanza spot è un avviso che viene emesso due minuti prima che Amazon EC2 arresti o termini l'istanza spot. Se si specifica l'ibernazione come comportamento di interruzione, si riceve un avviso di interruzione ma senza i due minuti di preavviso perché il processo di ibernazione comincia immediatamente.

Il modo migliore per gestire nel modo appropriato le interruzioni delle istanze spot è progettare l'applicazione affinché sia tollerante ai guasti. A tale scopo, puoi sfruttare gli avvisi di interruzione dell'istanza spot. Si consiglia di controllare queste notifiche di interruzione ogni 5 secondi.

Le notifiche di interruzione sono rese disponibili come EventBridge evento e come elementi nei metadati dell'istanza sull'istanza Spot. Gli avvisi di interruzione vengono emessi in base al miglior sforzo possibile.

Avviso di interruzione dell'istanza spot EC2 evento

Quando Amazon EC2 sta per interrompere l'istanza spot, emette un evento due minuti prima dell'interruzione effettiva (tranne che per l'ibernazione, che riceve l'avviso di interruzione ma non con due minuti di anticipo, perché l'ibernazione inizia immediatamente). Questo evento può essere rilevato da Amazon EventBridge. Per ulteriori informazioni sugli EventBridge eventi, consulta la Amazon EventBridge User Guide. Per un esempio dettagliato che illustra come creare e utilizzare le regole degli eventi, consulta Taking Advantage of Amazon EC2 Spot Instance Interruption Notices.

Di seguito è illustrato un esempio dell'evento di interruzione dell'istanza spot. I valori possibili per `instance-action` sono `hibernate`, `stop` e `terminate`.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Spot Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2a:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0",
        "instance-action": "action"
    }
}
```

> **Note**
>
> Il formato dell'ARN dell'interruzione dell'istanza spot è `arn:aws:ec2:`*`availability-zone`*`:instance/`*`instance-id`*. Questo formato è diverso dal formato dell'ARN delle risorse EC2.

instance-action

La voce `instance-action` specifica l'azione e l'orario indicativo, in UTC, in cui si verificherà l'azione.

Se l'istanza spot è contrassegnata per essere arrestata o terminata dal Amazon EC2, nei metadati dell'istanza è presente la voce `instance-action`. In caso contrario, non è presente. Puoi recuperare `instance-action` utilizzando il servizio di metadati di istanza versione 2 (IMDSv2) con la seguente procedura.

Linux

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/spot/instance-action
```

Windows

```
[string]$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/instance-action
```

L'esempio seguente indica l'orario in cui questa istanza verrà arrestata.

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

L'esempio seguente indica l'orario in cui questa istanza verrà terminata.

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

Se Amazon EC2 non si sta preparando ad arrestare o terminare l'istanza o se l'istanza è stata terminata dall'utente stesso, `instance-action` non è presente nei metadati dell'istanza e viene restituito un errore HTTP 404 quando si cerca di recuperarla.

termination-time

L'elemento `termination-time` specifica l'orario indicativo, in UTC, in cui l'istanza riceve il segnale di arresto.

> **Note**
>
> Questa voce viene mantenuta per la compatibilità con le versioni precedenti; è necessario utilizzare `instance-action`.

Se la tua istanza spot è contrassegnata per la terminazione da Amazon EC2 (a causa di un'interruzione dell'istanza spot in cui il comportamento di interruzione è impostato su `terminate` o a causa dell'annullamento di una richiesta persistente di istanza spot), l'elemento `termination-time` è presente nei metadati dell'istanza. In caso contrario, non è presente. Puoi recuperare `termination-time` utilizzando IMDSv2 con la seguente procedura.

Linux

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
if curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo termination_scheduled; fi
```

Windows

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/termination-time
```

Di seguito è riportato un output di esempio.

```
2015-01-05T18:02:00Z
```

Se Amazon EC2 non si sta preparando a terminare l'istanza (perché non c'è un'interruzione dell'istanza spot o perché il comportamento di interruzione è impostato su `stop` o `hibernate`) o se hai terminato l'istanza spot, l'elemento `termination-time` non è presente nei metadati dell'istanza (quindi riceve un errore HTTP 404) o contiene un valore che non è un valore temporale.

Se Amazon EC2 non riesce a terminare l'istanza, lo stato della richiesta viene impostato su `fulfilled`. I valore `termination-time` rimane nei metadati di istanza con l'orario indicativo originario, che ora è in passato.

Cercare Istanze spot interrotte

Quando descrivi le istanze EC2, i risultati includono le istanze spot. Il ciclo di vita dell'istanza di un'istanza spot è `spot`. Lo stato dell'istanza di un'istanza spot è `stopped` o `terminated`, a seconda del comportamento di interruzione configurato. Per un'istanza spot ibernata, lo stato dell'istanza è `stopped`.

Per ulteriori dettagli sul motivo dell'interruzione, controlla il codice di stato della richiesta spot. Per ulteriori informazioni, consulta the section called "Ottenimento dello stato della richiesta di un'istanza spot".

Console

Per individuare un'istanza spot interrotta

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Applica il seguente filtro: Ciclo di vita dell'istanza=spot.
4. Applica il filtro Stato istanza=arrestata o IStato istanza=terminata a seconda del comportamento di interruzione che hai configurato.
5. Per ogni istanza spot, nella scheda Dettagli, in Dettagli istanza, trova Messaggio transizione stato. I codici seguenti indicano che l'istanza spot è stata interrotta.
   - `Server.SpotInstanceShutdown`
   - `Server.SpotInstanceTermination`

AWS CLI

Per individuare istanze spot interrotte

Utilizza il comando describe-instances con l'opzione `--filters`. Per elencare solo gli ID di istanza nell'output, includi l'opzione `--query`.

Se il comportamento di interruzione consiste nel terminare le istanze spot, usa il seguente esempio:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot \
              Name=instance-state-name,Values=terminated \
              Name=state-reason-code,Values=Server.SpotInstanceTermination \
    --query "Reservations[*].Instances[*].InstanceId"
```

Se il comportamento di interruzione consiste nell'arrestare le istanze spot, usa il seguente esempio:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot \
              Name=instance-state-name,Values=stopped \
              Name=state-reason-code,Values=Server.SpotInstanceShutdown \
    --query "Reservations[*].Instances[*].InstanceId"
```

PowerShell

Per individuare istanze spot interrotte

Utilizza il cmdlet Get-EC2Instance.

Se il comportamento di interruzione consiste nel terminare le istanze spot, usa il seguente esempio:

```
(Get-EC2Instance `
    -Filter @{Key="instance-lifecycle"; Values="spot"} `
            @{Key="instance-state-name"; Values="terminated"} `
            @{Key="state-reason-code";
 Values="Server.SpotInstanceTermination"}).Instances.InstanceId
```

Se il comportamento di interruzione consiste nell'arrestare le istanze spot, usa il seguente esempio:

```
(Get-EC2Instance `
    -Filter @{Key="instance-lifecycle"; Values="spot"} `
            @{Key="instance-state-name"; Values="stopped"} `
```

```
            @{Key="state-reason-code";
Values="Server.SpotInstanceTermination"}).Instances.InstanceId
```

Determinare se Amazon EC2 ha terminato un'istanza spot

Un'istanza Spot funziona fino a quando Amazon EC2 non la interrompe in risposta a un'interruzione dell'istanza spot o finché non viene interrotta dall'utente. Per ulteriori informazioni, consulta the section called "Comportamento di interruzione".

Una volta terminata un'istanza Spot, puoi utilizzarla AWS CloudTrail per vedere se Amazon EC2 l'ha interrotta. Se il CloudTrail log include un`BidEvictedEvent`, ciò indica che Amazon EC2 ha terminato l'istanza Spot. Se invece visualizzi un evento `TerminateInstances`, significa che un utente ha terminato l'istanza spot.

In alternativa, se desideri ricevere una notifica che Amazon EC2 sta per interrompere la tua istanza Spot, usa Amazon per rispondere EventBridge all'evento EC2 Spot Interruption Warning.

Per visualizzare BidEvictedEvent eventi in CloudTrail

1. Apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione scegliere Event history (Cronologia eventi).
3. Nell'elenco dei filtri, seleziona Nome evento, quindi nel campo filtro a destra inserisci **`BidEvictedEvent`**.
4. (Facoltativo) Seleziona un intervallo di tempo.
5. Se l'elenco non è vuoto, scegli BidEvictedEvent dalla voce risultante per aprirne la pagina dei dettagli. Puoi trovare informazioni sull'istanza spot nel pannello Record dell'evento, incluso l'ID dell'istanza spot. Di seguito è illustrato un esempio di questo record dell'evento.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "ec2.amazonaws.com"
    },
    "eventTime": "2016-08-16T22:30:00Z",
    "eventSource": "ec2.amazonaws.com",
    "userAgent": "ec2.amazonaws.com",
    "sourceIPAddress": "ec2.amazonaws.com",
    "eventName": "BidEvictedEvent",
```

```
    "awsRegion": "us-east-2",
    "eventID": "d27a6096-807b-4bd0-8c20-a33a83375054",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "RequestParameters": null,
    "ResponseElements": null,
    "serviceEventDetails": {
        "instanceIdSet": [
          "i-1eb2ac8eEXAMPLE"
        ]
    }
}
```

6. Se non hai individuato una voce per l'evento `BidEvictedEvent`, inserisci **`TerminateInstances`** come nome dell'evento. Per ulteriori informazioni sul formato del record dell'evento per `TerminateInstances`, consulta the section called "Esempi di eventi dell'API Amazon EC2".

Fatturazione delle Istanze spot interrotte

Quando un'istanza spot viene interrotta, l'addebito per l'utilizzo dell'istanza e dei volumi EBS, e di eventuali costi aggiuntivi, avviene come segue.

Utilizzo di istanze

Chi interrompe l'istanza spot	Sistema operativo	Interrotta nella prima ora	Interrotta in qualsiasi momento dopo la prima ora
Se l'istanza spot viene arrestata o terminata dall'utente	Windows e Linux (tranne SUSE)	Addebito dei secondi utilizzati	Addebito dei secondi utilizzati
	SUSE	Addebito dell'ora intera anche se utilizzata parzialmente.	Addebito delle ore intere utilizzate e addebito di un'ora intera per l'ora parziale interrotta.
	Windows e Linux (tranne SUSE)	Nessun addebito	Addebito dei secondi utilizzati

Chi interrompe l'istanza spot	Sistema operativo	Interrotta nella prima ora	Interrotta in qualsiasi momento dopo la prima ora
Se l'istanza spot viene interrotta da Amazon EC2	SUSE	Nessun addebito	Addebito delle ore intere utilizzate e nessun addebito per l'ora parziale interrotta.

Utilizzo del volume EBS

Mentre un'istanza spot viene arrestata, il costo viene addebitato solo per i volumi EBS, che vengono conservati.

Con il Parco istanze EC2 e il Parco istanze spot, se sono presenti molte istanze arrestate, è possibile superare il limite numerico di volumi EBS per il proprio account.

Raccomandazioni per il ribilanciamento delle istanze EC2

Un suggerimento di ribilanciamento dell'istanza EC2 è un segnale di notifica di un rischio elevato di interruzione per un'istanza spot. Il segnale può arrivare prima dell'avviso di interruzione dell'istanza spot di due minuti, dando la possibilità di gestire in modo proattivo la istanza spot. È possibile decidere di ribilanciare il carico di lavoro su Istanze spot nuove o esistenti che non presentano un rischio elevato di interruzione.

Per Amazon EC2 non è sempre possibile inviare il segnale di raccomandazione per il ribilanciamento prima dell'avviso di interruzione dell'istanza spot di due minuti. Pertanto, il segnale di raccomandazione di ribilanciamento può arrivare insieme all'avviso di interruzione di due minuti.

I consigli di ribilanciamento sono disponibili come EventBridge evento e come elemento nei metadati dell'istanza sull'istanza Spot. Gli eventi vengono emessi secondo il principio del massimo sforzo.

> **Note**
>
> Le raccomandazioni per il ribilanciamento sono supportate solo per le Istanze spot che sono state lanciate dopo il 5 novembre 2020 00:00 UTC.

Indice

- Ribilanciare le operazioni intraprese
- Monitorare i segnali di raccomandazione di ribilanciamento
- Servizi che utilizzano il segnale di raccomandazione per il ribilanciamento

Ribilanciare le operazioni intraprese

Queste sono alcune delle possibili operazioni di ribilanciamento che si possono intraprendere:

Arresto di tipo graceful

Quando si riceve il segnale di suggerimento di ribilanciamento per un'istanza spot, è possibile avviare le procedure di arresto dell'istanza, che potrebbero includere il completamento dei processi prima di arrestarli. Ad esempio, è possibile caricare i registri di sistema o applicativi su Amazon Simple Storage Service (Amazon S3), è possibile chiudere gli operatori di Amazon SQS o completare l'annullamento della registrazione dal Domain Name System (DNS). Inoltre, è possibile salvare il lavoro in una memoria esterna per poi riprenderlo in un secondo momento.

Impedire la pianificazione di nuove operazioni

Quando si riceve il segnale di suggerimento di ribilanciamento per un'istanza spot, è possibile impedire la programmazione di nuove operazioni sull'istanza, continuando a utilizzare l'istanza fino al completamento delle operazioni programmate.

Avvio proattivo di nuove istanze sostitutive

È possibile configurare i gruppi Auto Scaling, il Parco istanze EC2 o il Parco istanze spot per l'avvio automatico di istanze spot sostitutive quando viene emesso un segnale di suggerimento di ribilanciamento. Per maggiori informazioni, consulta Use Capacity Rebalancing to handle Amazon EC2 Spot interruptions nella Guida per l'utente di Amazon EC2 Auto Scaling, nonché Utilizza il ribilanciamento della capacità nel parco istanze EC2 e nel parco istanze spot per sostituire le istanze spot a rischio in questa guida per l'utente.

Monitorare i segnali di raccomandazione di ribilanciamento

È possibile monitorare il segnale di raccomandazione di ribilanciamento in modo che, quando viene emesso, è possibile eseguire le operazioni specificate nella sezione precedente. Il segnale di raccomandazione di ribalance è reso disponibile come evento inviato ad Amazon EventBridge

(precedentemente noto come Amazon CloudWatch Events) e come metadati dell'istanza sull'istanza Spot.

Monitorare i segnali di raccomandazione di ribilanciamento:

- Usa Amazon EventBridge
- Utilizzare i metadati delle istanze

Usa Amazon EventBridge

Quando il segnale di raccomandazione di ribilanciamento viene emesso per un'istanza Spot, l'evento relativo al segnale viene inviato ad Amazon. EventBridge Se EventBridge rileva un modello di evento che corrisponde a uno schema definito in una regola, EventBridge richiama uno o più obiettivi specificati nella regola.

Di seguito è riportato un evento di esempio per il segnale di raccomandazione di ribilanciamento.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Instance Rebalance Recommendation",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0"
    }
}
```

I campi seguenti costituiscono il modello di evento definito nella regola:

`"detail-type": "EC2 Instance Rebalance Recommendation"`

Identifica che l'evento è un evento di raccomandazione di ribilanciamento

`"source": "aws.ec2"`

Identifica che l'evento proviene da Amazon EC2

Crea una regola EventBridge

Puoi scrivere una EventBridge regola e automatizzare le azioni da intraprendere quando il modello di evento corrisponde alla regola.

L'esempio seguente crea una EventBridge regola per inviare un'e-mail, un messaggio di testo o una notifica push mobile ogni volta che Amazon EC2 emette un segnale di raccomandazione di ribilanciamento. Il segnale viene emesso come evento di `EC2 Instance Rebalance Recommendation`, che attiva l'azione definita dalla regola.

Prima di creare la EventBridge regola, devi creare l'argomento Amazon SNS per l'e-mail, il messaggio di testo o la notifica push mobile.

Per creare una EventBridge regola per un evento di raccomandazione di ribilanciamento

1. Apri la EventBridge console Amazon all'indirizzo. https://console.aws.amazon.com/events/
2. Scegli Crea regola.
3. Per Define rule detail (Definisci dettagli della regola), effettua le seguenti operazioni:
   a. Immettere un Name (Nome) per la regola e, facoltativamente, una descrizione.

      Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso bus di eventi.
   b. Per Event bus (Bus di eventi), scegli default. Quando un servizio AWS nell'account genera un evento, passa sempre al bus di eventi di default dell'account.
   c. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
   d. Scegli Next (Successivo).
4. Per Build event pattern (Crea modello di eventi), procedi come segue:
   a. Per Event source, scegli AWS Events o EventBridge Partner Events.
   b. Per Event pattern (Modello di eventi), ai fini di questo esempio, specifica il seguente modello di eventi in modo che corrisponda all'evento `EC2 Instance Rebalance Recommendation`, quindi scegli Save (Salva).

```
{
 "source": ["aws.ec2"],
 "detail-type": ["EC2 Instance Rebalance Recommendation"]
```

```
}
```

Per aggiungere il modello di eventi, puoi utilizzare un modello scegliendo Event pattern form (Formato del modello di eventi) o specificare il tuo modello scegliendo Custom pattern (JSON editor) (Modello personalizzato (editor JSON)), come segue:

i. Per utilizzare un modello per creare il modello di eventi, procedi come segue:

   A. Scegli Event pattern form (Formato del modello di eventi).

   B. Per Event source (Origine evento), scegli AWS services (Servizi).

   C. In AWS Service, scegli Serie di istanze spot EC2.

   D. Per Event type (Tipo di evento), scegli EC2 Instance Rebalance Recommendation (Suggerimento per il ribilanciamento dell'istanza EC2).

   E. Per personalizzare il modello, scegli Edit pattern (Modifica modello) e apporta le modifiche in modo che corrisponda al modello di eventi di esempio.

ii. (Alternativa) Per specificare un modello di eventi personalizzato, procedi come segue:

   A. Scegli Custom pattern (JSON editor) (Modello personalizzato (editor JSON)).

   B. Nella casella Event pattern (Modello di eventi), aggiungi il modello di eventi per questo esempio.

c. Scegli Next (Successivo).

5. Per Select target(s) (Seleziona destinazione/i), esegui queste operazioni:

   a. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).

   b. Per Select a target (Seleziona una destinazione, scegli SNS topic (Argomento SNS) per inviare un'e-mail, un messaggio di testo o una notifica push mobile quando si verifica l'evento.

   c. Per Argomento, scegliere un argomento esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) messaging (Utilizzo di Amazon SNS per la messaggistica da applicazione a persona (A2P)) nella Guida per lo sviluppatore di Amazon Simple Notification Service.

   d. (Facoltativo) In Additional settings (Impostazioni aggiuntive), facoltativamente puoi configurare impostazioni aggiuntive. Per ulteriori informazioni, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi (passaggio 16) nella Amazon EventBridge User Guide.

e. Scegli Next (Successivo).

6. (Opzionale) Per Tags (Tag), se desideri puoi assegnare uno o più tag alla regola, quindi scegli Next (Successivo).
7. Per Review and create (Verifica e crea), procedi come segue:

   a. Verifica i dettagli della regola e modificali se necessario.

   b. Scegli Crea regola.

Per ulteriori informazioni, consulta EventBridge le regole di Amazon e i modelli di EventBridge eventi Amazon nella Amazon EventBridge User Guide

Utilizzare i metadati delle istanze

La categoria Metadati istanza `events/recommendations/rebalance` fornisce l'ora approssimativa (fuso UTC) in cui il segnale di raccomandazione di ribilanciamento è stato emesso per un'istanza spot.

Ti consigliamo di controllare la presenza di segnali di raccomandazione di ribilanciamento ogni 5 secondi in modo da non perdere l'opportunità di agire in base alle raccomandazione di ribilanciamento.

Se l'istanza spot riceve un suggerimento di ribilanciamento, l'ora in cui il segnale è stato emesso sarà presente nei metadati dell'istanza. È possibile recuperare l'ora in cui il segnale è stato emesso come segue.

IMDSv2

Linux

Esegui il seguente comando dall'istanza Linux.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Windows

Esegui il seguente cmdlet dall'istanza Windows

```
[string]$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/events/recommendations/
rebalance
```

IMDSv1

Linux

Esegui il seguente comando dall'istanza Linux.

```
curl http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Windows

Esegui il seguente cmdlet dall'istanza Windows.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/events/
recommendations/rebalance
```

Di seguito è riportato un esempio di output, che indica l'ora (fuso UTC) in cui il segnale di suggerimento di ribilanciamento è stato emesso per l'istanza spot.

```
{"noticeTime": "2020-10-27T08:22:00Z"}
```

Se il segnale non è stato emesso per l'istanza, `events/recommendations/rebalance` non è presente e viene visualizzato un errore HTTP 404 quando si tenta di recuperarlo.

Servizi che utilizzano il segnale di raccomandazione per il ribilanciamento

Amazon EC2 Auto Scaling, i parchi istanze EC2 e i parchi istanze spot utilizzano il segnale di suggerimento di ribilanciamento per semplificare il mantenimento della disponibilità del carico di lavoro aumentando in modo proattivo il parco istanze con una nuova istanza spot prima che

un'istanza in esecuzione riceva l'avviso di interruzione dell'istanza spot dopo due minuti. È possibile fare in modo che questi servizi monitorino e rispondano in modo proattivo alle modifiche che influiscono sulla disponibilità delle proprie Istanze spot. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Utilizzo del ribilanciamento della capacità per gestire le interruzioni spot di Amazon EC2 nella Guida per l'utente di Amazon EC2 Auto Scaling
- Utilizza il ribilanciamento della capacità nel parco istanze EC2 e nel parco istanze spot per sostituire le istanze spot a rischio nell'argomento del parco istanze spot e di EC2 Fleet di questa guida per l'utente

Punteggio di posizionamento spot

La funzione di punteggio di posizionamento Spot può consigliare una AWS regione, una zona di disponibilità o una zona locale in base ai requisiti di capacità di Spot. La capacità spot fluttua e non si può essere sicuri che otterrai sempre la capacità di cui hai bisogno. Un punteggio di posizionamento spot indica quanto è probabile che una richiesta Spot abbia esito positivo in una regione o in una zona di disponibilità.

> **Note**
>
> Un punteggio di posizionamento spot non fornisce alcuna garanzia in termini di capacità disponibile o rischio di interruzione. Un punteggio di posizionamento spot serve solo come suggerimento.

Casi d'uso

È possibile utilizzare la funzione del punteggio di posizionamento spot per quanto segue:

- Per trasferire e scalare la capacità di calcolo Spot in una regione diversa, in base alle necessità, in risposta all'aumento del fabbisogno di capacità o alla diminuzione della capacità disponibile nella regione corrente.
- Per identificare la zona di disponibilità ottimale in cui eseguire carichi di lavoro a singola zona di disponibilità.
- Per simulare le esigenze future di capacità di Spot in modo da poter scegliere una regione ottimale per l'espansione dei carichi di Spot-based lavoro.

- Per trovare una combinazione ottimale di tipi di istanza per soddisfare le esigenze di capacità spot.

Indice

- Limitazioni
- Costi
- Come funziona il punteggio di posizionamento spot
- Autorizzazioni necessarie per il punteggio di posizionamento spot
- Calcolo del punteggio di posizionamento spot

Limitazioni

- Limite di capacità di destinazione – il limite di capacità di destinazione del punteggio di posizionamento spot si basa sul tuo recente utilizzo Spot, tenendo conto della potenziale crescita dell'utilizzo. Se non si ha un utilizzo Spot recente, forniamo un limite di default minimo allineato al limite della richiesta Spot.
- Limite di configurazioni di richieste: possiamo limitare il numero di nuove configurazioni di richieste a un periodo di 24 ore se rileviamo modelli non associati all'uso previsto della funzione del punteggio di posizionamento spot. Se si raggiunge il limite, è possibile riprovare le configurazioni delle richieste già utilizzate, ma non è possibile specificare nuove configurazioni di richiesta fino al successivo periodo di 24 ore.
- Numero minimo di tipi di istanza: se si specificano i tipi di istanza, è necessario specificare almeno tre tipi di istanza diversi, altrimenti Amazon EC2 restituirà un punteggio di posizionamento spot basso. Analogamente, se si specificano attributi di istanza, devono essere risolti con almeno tre tipi di istanza diversi. I tipi di istanza sono considerati diversi se hanno un nome diverso. Ad esempio, m5.8xlarge, m5a.8xlarge e m5.12xlarge sono considerati diversi.

Costi

L'utilizzo della funzione del punteggio di posizionamento spot non comporta costi supplementari.

Come funziona il punteggio di posizionamento spot

Quando si utilizza la funzione del punteggio di posizionamento spot, si specifica innanzitutto i requisiti di calcolo per le istanze spot, quindi Amazon EC2 restituisce le 10 principali regioni o zone di disponibilità in cui è probabile che la propria richiesta Spot abbia esito positivo. Ogni regione o zona di disponibilità viene valutata su una scala da 1 a 10, con 10 che indica che è molto probabile che

la tua richiesta Spot abbia esito positivo e 1 che indica invece che è improbabile che la tua richiesta Spot abbia esito positivo. I risultati zonali possono includere zone di disponibilità e zone locali.

Per utilizzare la funzione del punteggio di posizionamento spot, completare la seguente procedura:

- Fase 1: specifica dei requisiti Spot
- Fase 2: filtro della risposta del punteggio di posizionamento spot
- Fase 3: esame dei suggerimenti
- Fase 4: utilizzo dei suggerimenti

Fase 1: specifica dei requisiti Spot

Innanzitutto, è necessario specificare la capacità spot di destinazione desiderata e i requisiti di calcolo, come segue:

1. Specificare la capacità spot di destinazione e, facoltativamente, l'unità di capacità di destinazione.

   È possibile specificare la capacità spot di destinazione desiderata in termini di numero di istanze o vCPU o in termini di quantità di memoria in MiB. Per specificare la capacità di destinazione in numero di vCPU o in quantità di memoria, è necessario specificare l'unità di capacità di destinazione come `vcpu` o `memory-mib`. In caso contrario, per impostazione predefinita sarà impostato sul numero di istanze.

   Specificando la capacità di destinazione in termini di numero di vCPU o in quantità di memoria, potrai utilizzare queste unità per il conteggio della capacità totale. Ad esempio, se si desidera utilizzare un mix di istanze di dimensioni diverse, è possibile specificare la capacità di destinazione come numero totale di vCPU. La funzione del punteggio di posizionamento spot considera quindi ogni tipo di istanza nella richiesta in base al numero di vCPU e conta il numero totale di vCPU anziché il numero totale di istanze nel totale della capacità di destinazione.

   Ad esempio, si supponga di specificare una capacità di destinazione totale di 30 vCPU e che l'elenco dei tipi di istanza sia costituito da c5.xlarge (4 vCPU), m5.2xlarge (8 vCPU) e r5.large (2 vCPU). Per ottenere un totale di 30 vCPU, è possibile avere un mix di 2 vCPU c5.xlarge (2*4 vCPU), 2 m5.2xlarge (2*8 vCPU) e 3 vCPU r5.large (3*2 vCPU).
2. Specificare i tipi di istanza o gli attributi di istanza.

   È possibile specificare i tipi di istanza da utilizzare oppure specificare gli attributi di istanza necessari per i requisiti di calcolo e quindi consentire ad Amazon EC2 di identificare i tipi di istanza con tali attributi. Questo è noto come selezione del tipo di istanza basata su attributi.

Non è possibile specificare sia i tipi di istanza che gli attributi di istanza nella stessa richiesta di punteggio di posizionamento spot.

Se si specificano i tipi di istanza, è necessario specificare almeno tre tipi di istanza diversi, altrimenti Amazon EC2 restituirà un punteggio di posizionamento spot basso. Analogamente, se si specificano attributi di istanza, devono essere risolti con almeno tre tipi di istanza diversi.

Per esempi dei diversi modi per specificare i requisiti Spot, consultare Configurazioni di esempio.

Fase 2: filtro della risposta del punteggio di posizionamento spot

Amazon EC2 calcola il punteggio di posizionamento spot per ogni regione o zona di disponibilità e restituisce le 10 regioni o le 10 zone di disponibilità principali in cui è probabile che la tua richiesta Spot abbia esito positivo. Il valore di default restituisce un elenco di regioni con un punteggio. Se si prevede di avviare tutta la tua capacità spot in una singola zona di disponibilità, è utile richiedere un elenco di zone di disponibilità con punteggio.

È possibile specificare un filtro regione per limitare le regioni che verranno restituite nella risposta.

È possibile combinare il filtro regione e una richiesta di zone di disponibilità con punteggio. In questo modo, le zone di disponibilità con punteggio saranno limitate alle regioni per le quali si è applicato il filtro. Per trovare la zona di disponibilità con punteggio più alto in una regione, specificare solo quella regione e la risposta restituirà un elenco di tutte le zone di disponibilità in tale regione.

Per impostazione predefinita, il punteggio di posizionamento di Spot ignora le zone locali. Per includerle, imposta su`IncludeLocalZones`. `true` Per i punteggi regionali, la capacità della zona locale viene conteggiata nel punteggio della regione madre. Per i punteggi zonali, la risposta può includere punteggi individuali delle zone locali.

Fase 3: esame dei suggerimenti

Il punteggio di posizionamento su Spot per ciascuna regione o zona di disponibilità viene calcolato in base alla capacità target, alla composizione dei tipi di istanze, alle tendenze attuali di utilizzo di Spot e all'ora della richiesta. Poiché la capacità spot è costantemente fluttuante, la stessa richiesta di punteggio di posizionamento spot può produrre punteggi diversi se il punteggio viene calcolato in momenti diversi.

Le regioni e le zone di disponibilità vengono valutate su una scala da 1 a 10. Un punteggio di 10 indica che è molto probabile, ma non garantito, che la propria richiesta Spot abbia esito positivo.

Un punteggio di 1 indica che la tua richiesta Spot ha bassissime probabilità di successo. Lo stesso punteggio potrebbe essere restituito per diverse regioni o zone di disponibilità.

Se vengono restituiti punteggi bassi, è possibile modificare i requisiti di calcolo e ricalcolare il punteggio. È possibile anche richiedere suggerimenti sul punteggio di posizionamento spot per gli stessi requisiti di calcolo in diversi momenti della giornata.

Fase 4: utilizzo dei suggerimenti

Un punteggio di posizionamento spot è rilevante solo se la tua richiesta Spot ha esattamente la stessa configurazione della configurazione del punteggio di posizionamento spot (capacità di destinazione, unità di capacità di destinazione e tipi di istanza o attributi di istanza) ed è configurato per utilizzare la strategia di allocazione `capacity-optimized`. In caso contrario, la probabilità di ottenere la capacità spot disponibile non sarà in linea con il punteggio.

Se il tuo punteggio include le zone locali, configura la successiva richiesta Spot per utilizzare le stesse zone locali. Altrimenti, la probabilità di ottenere capacità potrebbe non essere in linea con il punteggio.

Mentre un punteggio di posizionamento spot funge da linea guida e nessun punteggio garantisce che la propria richiesta Spot sia pienamente o parzialmente soddisfatta, è possibile utilizzare le seguenti informazioni per ottenere i migliori risultati:

- Utilizzo della stessa configurazione: il punteggio di posizionamento spot è rilevante solo se la configurazione della richiesta Spot (capacità di destinazione, unità di capacità di destinazione e tipi di istanza o attributi di istanza) nel gruppo Auto Scaling, nel parco istanze EC2 o nella serie di istanze spot è uguale a quella immessa per ottenere il punteggio di posizionamento spot.

  Se nella richiesta di punteggio di posizionamento spot è stata utilizzata la selezione del tipo di istanza basata su attributi, è possibile utilizzare la selezione del tipo di istanza basata su attributi per configurare il gruppo Auto Scaling, il parco istanze EC2 o la serie di istanze spot. Per ulteriori informazioni, consulta Create mixed instances group using attribute-based instance type selection e Specifica gli attributi per la selezione del tipo di istanza per il parco del tipo per il parco istanze EC2 o il parco istanze Spot.

  > **Note**
  >
  > Se si è specificata la capacità di destinazione in termini di numero di vCPU o di quantità di memoria e hai specificato i tipi di istanza nella configurazione del punteggio di posizionamento spot, tenere presente che al momento non è possibile creare questa

configurazione nel gruppo Auto Scaling, nel parco istanze EC2 o nella serie di istanze spot. Invece, si dovrà impostare manualmente il peso dell'istanza utilizzando il parametro `WeightedCapacity`.

- Utilizzo della strategia di allocazione **`capacity-optimized`**: qualsiasi punteggio presuppone che la richiesta del parco istanze sia configurata per utilizzare tutte le zone di disponibilità (per richiedere la capacità tra le regioni) o una singola zona di disponibilità (se si richiede la capacità in una zona di disponibilità) e la strategia di allocazione spot `capacity-optimized` perché la propria richiesta di capacità spot abbia successo. Se si utilizzano altre strategie di allocazione, come `lowest-price`, la probabilità di ottenere la capacità spot disponibile non sarà in linea con il punteggio.
- Agire subito su un punteggio: il suggerimento del punteggio di posizionamento spot riflette la capacità spot disponibile al momento della richiesta e la stessa configurazione può produrre punteggi diversi se calcolati in momenti diversi a causa delle fluttuazioni della capacità spot. Mentre un punteggio di 10 significa che la propria richiesta di capacità spot è altamente probabile, ma non garantita, per ottenere risultati ottimali consigliamo di agire immediatamente su un punteggio. Consigliamo inoltre di ottenere un nuovo punteggio ogni volta che si prova a eseguire una richiesta di capacità.

Autorizzazioni necessarie per il punteggio di posizionamento spot

Per impostazione predefinita, le identità IAM (utenti, ruoli o gruppi) non dispongono dell'autorizzazione per utilizzare the section called “Punteggio di posizionamento spot”. Per consentire alle identità IAM di utilizzare il punteggio di posizionamento spot, devi creare una policy IAM che conceda l'autorizzazione per usare l'operazione API EC2 di `ec2:GetSpotPlacementScores`. Quindi è necessario collegare la policy alle identità IAM che richiedono questa autorizzazione.

Di seguito viene riportata una policy IAM di esempio che concede le autorizzazioni per l'operazione API di `ec2:GetSpotPlacementScores` EC2.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": "ec2:GetSpotPlacementScores",
            "Resource": "*"
        }
    ]
}
```

Per informazioni sulla modifica di una policy IAM, consultare Editing IAM policies (Modifica di policy IAM) nella Guida per l'utente di IAM.

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- 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 Create a role for a third-party identity provider (federation) della Guida per l'utente IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina Create a role for an IAM user della Guida per l'utente IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente IAM.

Calcolo del punteggio di posizionamento spot

Puoi calcolare un punteggio di posizionamento spot in base alla capacità di destinazione e ai requisiti di calcolo. Per ulteriori informazioni, consulta the section called "Come funziona il punteggio di posizionamento spot".

Autorizzazioni richieste

Assicurati di disporre delle autorizzazioni richieste. Per ulteriori informazioni, consulta the section called "Autorizzazioni richieste".

Opzioni

- Calcolo utilizzando gli attributi dell'istanza
- Calcolo utilizzando i tipi di istanza
- Calcola utilizzando AWS CLI

Cerchi una soluzione automatizzata? Invece di seguire i passaggi manuali di questa guida per l'utente, puoi creare una dashboard per il monitoraggio dei punteggi di posizionamento di Spot che acquisisca e memorizzi automaticamente i punteggi in Amazon. CloudWatch Per ulteriori informazioni, consulta Guidance for Building a Spot Placement Score Tracker Dashboard on AWS.

Local Zones

Per includere le zone locali quando usi la console Amazon EC2, il tuo account deve avere almeno una zona locale abilitata. Per ulteriori informazioni, consulta Nozioni di base sulle zone locali AWS nella Guida per l'utente delle zone locali AWS .

Calcolo utilizzando gli attributi dell'istanza

Come calcolare un punteggio di posizionamento spot specificando gli attributi di istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Scegli la freccia rivolta verso il basso accanto a Richiedi istanze spot e quindi Calcola punteggio di posizionamento spot.
4. Scegliere Enter requirements (Inserisci i requisiti).
5. Per Target capacity (Capacità di destinazione), inserire la capacità desiderata in termini di numero di istanze o vCPU o la quantità di memoria (MiB).
6. Per Instance type requirements (Requisiti per il tipo di istanza), per specificare i requisiti di calcolo e consentire ad Amazon EC2 di identificare i tipi di istanza ottimali con questi requisiti, scegliere Specify instance attributes that match your compute requirements (Specifica gli attributi di istanza che corrispondono ai requisiti di calcolo).
7. Per vCPUs (vCPU) inserire il numero minimo e massimo desiderato di vCPU. Per non specificare alcun limite, selezionare No minimum (Nessun minimo), No maximum (Nessun massimo) o entrambe le opzioni.
8. Per Memory (GiB) (Memoria [GiB]) inserire la quantità minima e massima di memoria desiderata. Per non specificare alcun limite, selezionare No minimum (Nessun minimo), No maximum (Nessun massimo) o entrambe le opzioni.

9. Per Architettura della CPU, seleziona l'architettura dell'istanza desiderata.
10. (Facoltativo) Per Additional instance attributes (Attributi istanza aggiuntivi), facoltativamente, è possibile specificare uno o più attributi per esprimere i requisiti di calcolo in modo più dettagliato. Ogni attributo aggiuntivo aggiunge ulteriori vincoli alla tua richiesta. È possibile omettere gli attributi aggiuntivi, nel qual caso saranno utilizzati i valori di default. Per una descrizione di ciascun attributo e dei relativi valori predefiniti, consulta get-spot-placement-scores.
11. (Facoltativo) Per visualizzare i tipi di istanza con gli attributi specificati, espandere Preview matching instance types (Anteprima tipi di istanza corrispondenti). Per escludere che i tipi di istanza vengano utilizzati nella valutazione del posizionamento, selezionare le istanze e quindi scegliereEscludi tipi di istanze.
12. Scegliere Load placement scores (Carica punteggi di posizionamento) e controllare i risultati.
13. (Facoltativo) Per visualizzare il punteggio di posizionamento spot per regioni specifiche, per Regions to evaluate (Regioni da valutare), selezionare le regioni da valutare, quindi scegliere Calculate placement scores (Calcola punteggi di posizionamento).
14. (Facoltativo) In Opzioni Score, seleziona Includi zone locali.
15. (Facoltativo) Per visualizzare il punteggio di posizionamento spot per le zone di disponibilità nelle regioni visualizzate, seleziona la casella di controllo Fornisci punteggi di posizionamento per zona di disponibilità. Un elenco delle zone di disponibilità con punteggio è utile se si desidera avviare tutta la tua capacità spot in una singola zona di disponibilità.
16. (Facoltativo) Per modificare i requisiti di calcolo e ottenere un nuovo punteggio di posizionamento, scegliere Edit (Modifica), apportare le modifiche necessarie e quindi scegliere Calculate placement scores (Calcola punteggi di posizionamento).

Calcolo utilizzando i tipi di istanza

Come calcolare un punteggio di posizionamento spot specificando i tipi di istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Scegli la freccia rivolta verso il basso accanto a Richiedi istanze spot e quindi Calcola punteggio di posizionamento spot.
4. Scegliere Enter requirements (Inserisci i requisiti).
5. Per Capacità di destinazione, inserire la capacità desiderata in termini di numero di istanze o vCPU o la quantità di memoria (MiB).

6. Per Instance type requirements (Requisiti del tipo di istanza), per specificare i tipi di istanza da utilizzare, scegliere Manually select instance types (Seleziona manualmente i tipi di istanza).
7. Scegliere Select instance types (Seleziona tipi di istanza), selezionare i tipi di istanza da utilizzare e quindi scegliere Select (Seleziona). Per trovare rapidamente i tipi di istanza, è possibile utilizzare la barra del filtro per filtrare i tipi di istanza in base a proprietà diverse.
8. Scegliere Carica punteggi di posizionamento e controllare i risultati.
9. (Facoltativo) Per visualizzare il punteggio di posizionamento spot per regioni specifiche, per Regions to evaluate (Regioni da valutare), selezionare le regioni da valutare, quindi scegliere Calculate placement scores (Calcola punteggi di posizionamento).
10. (Facoltativo) In Opzioni punteggio, seleziona Includi zone locali.
11. (Facoltativo) Per visualizzare il punteggio di posizionamento spot per le zone di disponibilità nelle regioni visualizzate, seleziona la casella di controllo Fornisci punteggi di posizionamento per zona di disponibilità. Un elenco delle zone di disponibilità con punteggio è utile se si desidera avviare tutta la tua capacità spot in una singola zona di disponibilità.
12. (Facoltativo) Per modificare l'elenco dei tipi di istanze e ottenere un nuovo punteggio di posizionamento, scegliere Edit (Modifica), apportare le modifiche necessarie e quindi scegliere Calculate placement scores (Calcola punteggi di posizionamento).

Calcola utilizzando AWS CLI

Come calcolare il punteggio di posizionamento spot

1. (Facoltativo) Per generare tutti i parametri possibili che possono essere specificati per la configurazione del punteggio di posizionamento spot, utilizzare il comando get-spot-placement-scores e il parametro `--generate-cli-skeleton`.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --generate-cli-skeleton
```

   Di seguito è riportato un output di esempio.

```
{
    "InstanceTypes": [
        ""
    ],
    "TargetCapacity": 0,
```

```
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "RegionNames": [
        ""
    ],
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": [
            "x86_64_mac"
        ],
        "VirtualizationTypes": [
            "hvm"
        ],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 0,
                "Max": 0
            },
            "MemoryMiB": {
                "Min": 0,
                "Max": 0
            },
            "CpuManufacturers": [
                "amd"
            ],
            "MemoryGiBPerVCpu": {
                "Min": 0.0,
                "Max": 0.0
            },
            "ExcludedInstanceTypes": [
                ""
            ],
            "InstanceGenerations": [
                "previous"
            ],
            "SpotMaxPricePercentageOverLowestPrice": 0,
            "OnDemandMaxPricePercentageOverLowestPrice": 0,
            "BareMetal": "excluded",
            "BurstablePerformance": "excluded",
            "RequireHibernateSupport": true,
            "NetworkInterfaceCount": {
                "Min": 0,
                "Max": 0
            },
            "LocalStorage": "included",
```

```
            "LocalStorageTypes": [
                "hdd"
            ],
            "TotalLocalStorageGB": {
                "Min": 0.0,
                "Max": 0.0
            },
            "BaselineEbsBandwidthMbps": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorTypes": [
                "fpga"
            ],
            "AcceleratorCount": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorManufacturers": [
                "amd"
            ],
            "AcceleratorNames": [
                "vu9p"
            ],
            "AcceleratorTotalMemoryMiB": {
                "Min": 0,
                "Max": 0
            }
        }
    },
    "DryRun": true,
    "MaxResults": 0,
    "NextToken": "",
    "IncludeLocalZones": true
}
```

2. Creare un file di configurazione JSON utilizzando l'output del passaggio precedente e configurarlo come segue:

   a. Per `TargetCapacity`, inserire la capacità spot desiderata in termini di numero di istanze o vCPU o quantità di memoria (MiB).

   b. Per `TargetCapacityUnitType`, inserire l'unità per la capacità di destinazione. Se si omette questo parametro, verrà utilizzato il parametro di default `units`.

Valori validi: `units` (che si traduce in numero di istanze) | `vcpu` | `memory-mib`

c. Per `SingleAvailabilityZone`, specificare `true` per una risposta che restituisce un elenco di zone di disponibilità con punteggio. Un elenco delle zone di disponibilità con punteggio è utile se si desidera avviare tutta la tua capacità spot in una singola zona di disponibilità. Se si omette questo parametro, verrà utilizzato il parametro di default `false` e la risposta restituirà un elenco di regioni con punteggio.

d. (Facoltativo) Per`IncludeLocalZones`, specificare `true` di includere le zone locali. Per i punteggi regionali, la capacità delle zone locali viene conteggiata per la regione principale. Per i punteggi zonali, la risposta può includere punteggi individuali delle zone locali. Se omessi o impostati su`false`, le zone locali vengono ignorate.

e. (Facoltativo) Per `RegionNames`, specificare le regioni da utilizzare come filtro. È necessario specificare il codice regione, ad esempio, `us-east-1`.

   Con un filtro regione, la risposta restituisce solo le regioni specificate. Se si è specificato `true` per `SingleAvailabilityZone`, la risposta restituisce solo le zone di disponibilità nelle regioni specificate.

f. È possibile includere `InstanceTypes` o `InstanceRequirements`, ma non entrambi nella stessa configurazione.

   Specificare una delle seguenti opzioni nella configurazione JSON:

   - Per specificare un elenco di tipi di istanze, specificare i tipi di istanza nel parametro `InstanceTypes`. Specificare almeno tre tipi di istanza diversi. Se si specificano solo uno o due tipi di istanza, il punteggio di posizionamento spot sarà un punteggio basso. Per l'elenco dei tipi di istanza, consultare Tipi di istanza di Amazon EC2.
   - Per specificare gli attributi dell'istanza in modo che Amazon EC2 identifichi i tipi di istanza che corrispondono a tali attributi, specificare gli attributi che si trovano nella struttura `InstanceRequirements`.

     È necessario fornire valori per `VCpuCount`, `MemoryMiB` e `CpuManufacturers`. È possibile omettere gli altri attributi, nel qual caso saranno utilizzati i valori di default. Per una descrizione di ciascun attributo e dei relativi valori predefiniti, consulta get-spot-placement-scores.

   Per gli esempi di configurazione, consulta Configurazioni di esempio.

3. Per ottenere il punteggio di posizionamento spot per i requisiti specificati nel file JSON, utilizzare il comando get-spot-placement-scores e specificare il nome e il percorso del file JSON utilizzando il parametro `--cli-input-json`.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Output di esempio se `SingleAvailabilityZone` è impostato su `false` oppure omesso (se omesso, viene utilizzato il valore predefinito `false`): viene restituito un elenco di Regioni con punteggio.

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "Score": 7
    },
    {
        "Region": "us-west-1",
        "Score": 5
    },
   ...
```

Esempio di output se `SingleAvailabilityZone` è impostato su`true`: viene restituito un elenco con punteggi delle zone di disponibilità e, se lo `IncludeLocalZones` è`true`, viene restituito un elenco di zone locali.

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "use1-az1",
        "Score": 8
    },
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "usw2-az3",
        "Score": 6
    },
   ...
```

Configurazioni di esempio

Quando si utilizza il AWS CLI, è possibile utilizzare le seguenti configurazioni di esempio.

Configurazioni di esempio

- Esempio: specifica dei tipi di istanza e della capacità di destinazione
- Esempio: specifica dei tipi di istanza e della capacità di destinazione in termini di memoria
- Esempio: specifica degli attributi per la selezione del tipo di istanza basata su attributi
- Esempio: specifica degli attributi per la selezione del tipo di istanza basata su attributi e restituzione di un elenco di zone di disponibilità con punteggio

Esempio: specifica dei tipi di istanza e della capacità di destinazione

La configurazione di esempio seguente specifica tre diversi tipi di istanza e una capacità spot di destinazione di 500 istanze spot.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500
}
```

Esempio: specifica dei tipi di istanza e della capacità di destinazione in termini di memoria

Il seguente esempio di configurazione specifica tre diversi tipi di istanza e una capacità spot di destinazione di 500.000 MiB di memoria, in cui il numero di istanze spot da avviare deve fornire un totale di 500.000 MiB di memoria.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500000,
    "TargetCapacityUnitType": "memory-mib"
}
```

Esempio: specifica degli attributi per la selezione del tipo di istanza basata su attributi

La seguente configurazione di esempio è configurata per la selezione del tipo di istanza basata su attributi ed è seguita da una spiegazione della configurazione di esempio.

```
{
    "TargetCapacity": 5000,
    "TargetCapacityUnitType": "vcpu",
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

`InstanceRequirementsWithMetadata`

Per utilizzare la selezione dell'istanza basata su attributi, è necessario includere la struttura `InstanceRequirementsWithMetadata` nella configurazione e specificare gli attributi desiderati per le istanze spot.

Nell'esempio precedente, vengono specificati i seguenti attributi di istanza:

- `ArchitectureTypes`: il tipo di architettura dei tipi di istanza deve essere `arm64`.
- `VirtualizationTypes`: il tipo di virtualizzazione dei tipi di istanza deve essere `hvm`.
- `VCpuCount`: i tipi di istanza devono avere un minimo di 1 e un massimo di 12 vCPU.
- `MemoryMiB`: i tipi di istanza devono avere un minimo di 512 MiB di memoria. Omettendo il parametro `Max`, si sta indicando che non esiste un limite massimo.

Si noti che sono disponibili diversi altri attributi facoltativi che è possibile specificare. Per l'elenco di attributi, consulta get-spot-placement-scores.

`TargetCapacityUnitType`

Il parametro `TargetCapacityUnitType` specifica l'unità per la capacità di destinazione. Nell'esempio, la capacità di destinazione è `5000` e il tipo di unità della capacità di destinazione è `vcpu`, che insieme specificano una capacità di destinazione desiderata di 5.000 vCPU, dove il numero di istanze spot da avviare deve fornire un totale di 5000 vCPU.

Esempio: specifica degli attributi per la selezione del tipo di istanza basata su attributi e restituzione di un elenco di zone di disponibilità con punteggio

La seguente configurazione di esempio è configurata per la selezione del tipo di istanza basata su attributi. Specificando `"SingleAvailabilityZone": true`, la risposta restituirà un elenco di zone di disponibilità con punteggio.

```
{
    "TargetCapacity": 1000,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

Monitoraggio dei costi delle istanze spot utilizzando il feed di dati delle istanze spot

Per facilitare la comprensione delle spese per le proprie istanze spot, Amazon EC2 fornisce un feed di dati che descrive l'utilizzo e i prezzi delle proprie istanze spot. Tale feed di dati viene inviato a un bucket Amazon S3 specificato al momento dell'iscrizione al feed di dati.

In genere, i file con il feed di dati arrivano nel bucket una volta all'ora. Se non si dispone di un'istanza spot in esecuzione durante una determinata ora, per quell'ora non si riceve un file di feed di dati.

In genere, ogni ora di utilizzo dell'istanza spot viene coperta da un singolo file di dati. Questi file vengono compressi (gzip) prima di essere consegnati al tuo bucket. Amazon EC2 può scrivere più file per una data ora di utilizzo in cui i file sono grandi (ad esempio, quando il contenuto del file per quell'ora supera i 50 MB prima della compressione).

> **Note**
>
> Puoi creare un solo data feed di istanze Spot per Account AWS.

Il data feed di Spot Instance è supportato in tutte le AWS regioni tranne Cina (Pechino), Cina (Ningxia), AWS GovCloud (Stati Uniti) e nelle regioni disattivate per impostazione predefinita.

Indice

- Nome e formato del file di feed di dati
- Requisiti bucket Amazon S3
- Iscriversi al feed di dati per l'istanza spot
- Visualizzare i dati nel feed di dati
- Eilminare il feed di dati per l'istanza spot

Nome e formato del file di feed di dati

Il nome del file di feed di dati dell'istanza spot utilizza il formato seguente (con data e ora in UTC):

```
bucket-name.s3.amazonaws.com/optional-prefix/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz
```

Per esempio, se il nome del proprio bucket è **amzn-s3-demo-bucket** e il proprio prefisso è **my-prefix**, i nomi dei propri file sono simili ai seguenti:

```
amzn-s3-demo-bucket.s3.amazonaws.com/my-prefix/111122223333.2023-12-09-07.001.b959dbc6.gz
```

Per ulteriori informazioni sui nomi dei bucket, consultare Regole per la denominazione dei bucket in Guida per l'utente di Amazon S3.

I file di feed di dati dell'istanza spot sono delimitati da tabulatori. Ogni riga del file di dati corrisponde a un'ora di utilizzo dell'istanza e contiene i campi elencati nella tabella seguente.

Campo	Descrizione
`Timestamp`	Il timestamp utilizzato per stabilire il prezzo applicato per l'utilizzo di questa istanza.
`UsageType`	Il tipo di utilizzo e il tipo di istanza per cui viene addebitato il costo. Per la `m1.small` Istanze spot, questo campo è impostato su `SpotUsage` . Per tutti gli altri tipi di istanza, questo campo è impostato su `SpotUsage:` {instance-type}. Ad esempio, `SpotUsage:c1.medium` .
`Operation`	Il prodotto per il quale viene richiesto il pagamento. Per le Istanze spot, di Linux, questo campo è impostato su `RunInstances` . Per le Istanze spot, di Windows, questo campo è impostato su `RunInstances:0002` . L'utilizzo dello Spot è raggruppato in base alla zona di disponibilità.
`InstanceID`	L'ID dell'istanza spot che ha generato l'utilizzo dell'istanza.
`MyBidID`	L'ID della richiesta di istanza spot che ha generato l'utilizzo dell'istanza.
`MyMaxPrice`	Il prezzo massimo specificato per questa richiesta .
`MarketPrice`	Il prezzo Spot nell'orario specificato nel campo `Timestamp` .
`Charge`	Prezzo addebitato per l'utilizzo di questa istanza.
`Version`	La versione del feed di dati. La versione possibile è 1.0.

Requisiti bucket Amazon S3

Al momento dell'iscrizione al feed di dati, bisogna specificare un bucket Amazon S3 in cui memorizzare i file di feed di dati.

Prima di scegliere un bucket Amazon S3 per il feed di dati, considerare quanto segue:

- È necessario disporre delle autorizzazioni `FULL_CONTROL` per il bucket. Se si è il proprietario del bucket, si è in possesso dell'autorizzazione per impostazione predefinita. Altrimenti, il proprietario del bucket deve concederti Account AWS questa autorizzazione.
- Quando ti iscrivi a un data feed, queste autorizzazioni vengono utilizzate per aggiornare l'ACL del bucket e concedere l'autorizzazione all'account del feed di AWS dati. `FULL_CONTROL` L'account del AWS data feed scrive i file del data feed nel bucket. Se il proprio account non dispone delle autorizzazioni necessarie, i file di feed di dati non possono essere scritti nel bucket. Per ulteriori informazioni, consulta i log inviati ad Amazon S3 nella Amazon CloudWatch Logs User Guide.

  Se aggiorni l'ACL e rimuovi le autorizzazioni per l'account del AWS data feed, i file del data feed non possono essere scritti nel bucket. Bisogna iscriversi nuovamente al feed di dati per ricevere i file di feed di dati.
- Ogni file di feed di dati ha il proprio ACL (separato da quello per il bucket). Il proprietario del bucket dispone dell'autorizzazione `FULL_CONTROL` ai file di dati. L'account del AWS data feed dispone delle autorizzazioni di lettura e scrittura.
- Se elimini l'abbonamento al data feed, Amazon EC2 non rimuove le autorizzazioni di lettura e scrittura per l'account del AWS data feed né sul bucket né sui file di dati. È necessario rimuovere tali autorizzazioni.
- Se crittografi il bucket Amazon S3 utilizzando la crittografia lato server con una AWS KMS chiave archiviata in AWS Key Management Service (SSE-KMS), devi utilizzare una chiave gestita dal cliente. Per ulteriori informazioni, consulta la crittografia lato server a bucket di Amazon S3 nella Amazon Logs User Guide. CloudWatch

Iscriversi al feed di dati per l'istanza spot

Puoi iscriverti al feed di dati dell'istanza spot in qualsiasi momento. Non puoi completare questa attività utilizzando la console Amazon EC2.

Se ricevi un errore che indica che il bucket non dispone di autorizzazioni sufficienti, consulta il seguente articolo per informazioni sulla risoluzione dei problemi: Troubleshoot the data feed for Spot Instances.

AWS CLI

Per iscriverti al feed di dati

Usa il comando create-spot-datafeed-subscription.

Per specificare un bucket con un prefisso, usa il seguente esempio:

```
aws ec2 create-spot-datafeed-subscription \
    --bucket amzn-s3-demo-bucket \
    --prefix my-prefix
```

Per specificare un bucket senza prefisso, usa il seguente esempio:

```
aws ec2 create-spot-datafeed-subscription \
    --bucket amzn-s3-demo-bucket
```

PowerShell

Per iscriverti al feed di dati

Utilizza il cmdlet New-EC2SpotDatafeedSubscription.

Per specificare un bucket con un prefisso, usa il seguente esempio:

```
New-EC2SpotDatafeedSubscription `
    -Bucket amzn-s3-demo-bucket `
    -Prefix my-prefix
```

Per specificare un bucket senza prefisso, usa il seguente esempio:

```
New-EC2SpotDatafeedSubscription `
    -Bucket amzn-s3-demo-bucket
```

Visualizzare i dati nel feed di dati

Nel, apri. Console di gestione AWS AWS CloudShell Utilizza il seguente comando s3 sync per ottenere i file .gz relativi al feed di dati dal bucket S3 e archiviarli nella cartella specificata.

```
aws s3 sync s3://amzn-s3-demo-bucket ./data-feed
```

Per visualizzare i contenuti di un file .gz, passare alla cartella in cui sono stati archiviati i contenuti del bucket S3.

```
cd data-feed
```

Utilizzare il comando ls per visualizzare i nomi dei file. Utilizzare il comando zcat con il nome del file per visualizzare i contenuti del file compresso. Il seguente è un comando di esempio.

```
zcat  111122223333.2023-12-09-07.001.b959dbc6.gz
```

Di seguito è riportato un output di esempio.

```
#Version: 1.0
#Fields: Timestamp UsageType Operation InstanceID MyBidID MyMaxPrice MarketPrice Charge
 Version
2023-12-09 07:13:47 UTC USE2-SpotUsage:c7a.medium       RunInstances:SV050
 i-0c3e0c0b046e050df     sir-pwq6nmfp    0.0510000000 USD        0.0142000000 USD
  0.0142000000 USD        1
```

Eilminare il feed di dati per l'istanza spot

Quando non hai più bisogno del feed di dati dell'istanza spot, puoi eliminarlo.

AWS CLI

Per eliminare il feed di dati

Usa il comando delete-spot-datafeed-subscription.

```
aws ec2 delete-spot-datafeed-subscription
```

PowerShell

Per eliminare il feed di dati

Utilizza il cmdlet Remove-EC2SpotDatafeedSubscription.

```
Remove-EC2SpotDatafeedSubscription
```

Service-linked ruolo per le richieste di istanza Spot

Amazon EC2 utilizza ruoli collegati ai servizi per le autorizzazioni di cui ha bisogno per eseguire chiamate ad altri servizi AWS per tuo conto. Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a un. Servizio AWS Service-linked i ruoli forniscono un modo sicuro

per delegare le autorizzazioni Servizi AWS perché solo il servizio collegato può assumere un ruolo collegato al servizio. Per ulteriori informazioni, consulta Service-linked i ruoli nella IAM User Guide.

Amazon EC2 utilizza il ruolo collegato al servizio denominato AWSServiceRoleForEC2Spot per avviare e gestire le istanze Spot per tuo conto.

Autorizzazioni concesse da AWSServiceRoleForEC2Spot

Amazon EC2 utilizza AWSServiceRoleForEC2Spot per completare le seguenti azioni:

- `ec2:DescribeInstances` - Descrive le istanze spot
- `ec2:StopInstances` - Arresta istanze spot
- `ec2:StartInstances` - Avvia istanze spot

Creazione del ruolo collegato ai servizi

In gran parte dei casi, non è necessario creare manualmente un ruolo collegato ai servizi. Amazon EC2 crea il ruolo AWSServiceRoleForEC2Spot collegato al servizio la prima volta che richiedi un'istanza Spot utilizzando la console.

Se avevi una richiesta di istanza Spot attiva prima di ottobre 2017, quando Amazon EC2 ha iniziato a supportare questo ruolo collegato al servizio, Amazon EC2 ha creato il ruolo nel tuo account. AWSServiceRoleForEC2Spot AWS Per ulteriori informazioni, consulta Visualizzazione di un nuovo ruolo nell'account nella Guida per l'utente di IAM.

Se utilizzi AWS CLI o un'API per richiedere un'istanza Spot, devi prima assicurarti che questo ruolo esista.

Per creare AWSServiceRoleForEC2Spot usando la console

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. Nella pagina Select type of trusted entity (Seleziona tipo di entità attendibile) selezionare EC2, EC2 - Spot Instances (EC2 – Istanze spot), quindi scegliere Next: Permissions (Successivo: Autorizzazioni).
5. Nella pagina successiva, scegli Next:Review.

6. Nella pagina Review (Revisione), scegliere Create Role (Crea ruolo).

Per creare AWSServiceRoleForEC2Spot utilizzando il AWS CLI

Utilizzare il comando create-service-linked-role come segue.

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

Se non hai più bisogno di usare le istanze Spot, ti consigliamo di eliminare il AWSServiceRoleForEC2Spot ruolo. Dopo che questo ruolo è stato eliminato dall'account, Amazon EC2 creerà di nuovo il ruolo se verranno richieste le Istanze spot.

Concessione dell'accesso alle chiavi gestite dal cliente per l'uso con le AMI crittografate e gli snapshot EBS

Se specifichi un'AMI crittografata o uno snapshot Amazon EBS crittografato per le tue istanze Spot e utilizzi una chiave gestita dal cliente per la crittografia, devi concedere al AWSServiceRoleForEC2Spot ruolo l'autorizzazione a utilizzare la chiave gestita dal cliente in modo che Amazon EC2 possa avviare le istanze Spot per tuo conto. Per farlo, occorre aggiungere una concessione alla chiave gestita dal cliente, come mostrato nella procedura seguente.

Nel processo di assegnazione delle autorizzazioni, le concessioni rappresentano un'alternativa alle policy delle chiavi. Per ulteriori informazioni, consulta Utilizzo delle concessioni e Utilizzo delle policy delle chiavi in AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .

Per concedere AWSServiceRoleForEC2Spot autorizzazioni di ruolo per utilizzare la chiave gestita dal cliente

- Utilizza il comando create-grant per aggiungere una concessione alla chiave gestita dal cliente e per specificare il principale (il ruolo AWSServiceRoleForEC2Spot collegato al servizio) a cui è concessa l'autorizzazione per eseguire le operazioni consentite dalla concessione. La chiave gestita dal cliente è specificata dal parametro `key-id` e dall'ARN della chiave gestita dal cliente. L'entità principale è specificata dal `grantee-principal` parametro e dall'ARN del ruolo collegato al servizio. AWSServiceRoleForEC2Spot

  ```
  aws kms create-grant \
      --region us-east-1 \
      --key-id arn:aws:kms:us-
  east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
  ```

```
    --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
spot.amazonaws.com/AWSServiceRoleForEC2Spot \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Quote di istanze Spot

Sono previste delle quote per il numero di istanze Spot in esecuzione e per le richieste di istanze Spot in sospeso per Account AWS per regione. Una volta soddisfatta una richiesta di istanza spot in sospeso, questa non viene più conteggiata ai fini del raggiungimento della quota, poiché a tal fine verrà conteggiata l'istanza in esecuzione.

Le quote delle istanze spot vengono gestiti in termini di numero di unità di elaborazione centrale virtuali (vCPU) che vengono utilizzate o verranno utilizzate dalle istanze spot in esecuzione in attesa dell'evasione delle richieste aperte. Se termini le istanze spot ma non annulli le richieste di istanze spot, le richieste vengono conteggiate ai fini della quota di vCPU delle istanze spot fino a quando Amazon EC2 non rileva la terminazione delle istanze spot e chiude le richieste.

Per le istanze spot forniamo i seguenti tipi di quota.

Nome	Predefinita	Adattabile
Tutte le richieste di istanza spot DL	0	Sì
Tutte le richieste di istanza spot F	0	Sì
Tutte le richieste di istanza spot G e VT	0	Sì
Tutte le richieste di istanza spot Inf	0	Sì
Tutte le richieste di istanza spot P	0	Sì
Tutte le richieste di istanza spot standard (A, C, D, H, I, M, R, T, Z)	5	Sì
Tutte le richieste di istanza spot Trn	0	Sì
Tutte le richieste di istanza spot X	0	Sì

Anche se Amazon EC2 modifica automaticamente le quote delle istanze spot in base all'utilizzo, se necessario puoi richiedere un aumento della quota. Ad esempio, se si intende avviare più istanze spot di quante consentite dalla quota corrente, è possibile richiedere un aumento della quota. Puoi richiedere un aumento della quota anche se invii una richiesta di istanza spot e ricevi l'errore `Max spot instance count exceeded`. Per richiedere un aumento di una quota, è possibile utilizzare la console Service Quotas descritta alla pagina Service Quotas di Amazon EC2.

È possibile avviare una qualsiasi combinazione di tipi di istanza che soddisfano le mutevoli esigenze dell'applicazione. Ad esempio, con una quota di richieste di istanze spot tutte standard di 256 vCPU, puoi avviare 32 istanze spot `m5.2xlarge` (32 x 8 vCPU) oppure 16 istanze spot `c5.4xlarge` (16 x 16 vCPU).

Con l'integrazione di Amazon CloudWatch Metrics, puoi monitorare l'utilizzo di EC2 rispetto alle tue quote. Puoi anche configurare gli allarmi per ricevere un avviso quando stai per raggiungere le quote. Per ulteriori informazioni, consulta Service Quotas and Amazon CloudWatch alarms nella Service Quotas User Guide

Host dedicati di Amazon EC2

Un Host dedicato Amazon EC2 è un server fisico completamente dedicato al tuo utilizzo. Facoltativamente, puoi scegliere di condividere la capacità dell'istanza con altri account AWS . Per ulteriori informazioni, consulta Cross-account Condivisione di host dedicati Amazon EC2.

Gli host dedicati forniscono visibilità e controllo sul posizionamento delle istanze e supportano l'affinità con gli host. Ciò significa che puoi avviare ed eseguire istanze su host specifici e assicurarti che le istanze vengano eseguite solo su host specifici. Per ulteriori informazioni, consulta Auto-posizionamento dell'host dedicato Amazon EC2 e affinità degli host.

Gli Host dedicati forniscono un supporto completo per l'uso di licenze proprie (BYOL). Ti consentono di utilizzare le licenze software esistenti per socket, per core o per macchina virtuale, inclusi Windows Server, SQL Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux o altre licenze software che sono legate a macchine virtuali, socket o core fisici, in base alle condizioni della licenza.

Se le tue istanze devono essere eseguite su hardware dedicato, ma non hai bisogno di visibilità o controllo sul posizionamento delle istanze, e non hai bisogno di utilizzare licenze software per socket o per core, puoi prendere in considerazione l'utilizzo di istanze dedicate. Istanze dedicate e host dedicati possono essere entrambi utilizzati per avviare istanze Amazon EC2 su server fisici dedicati. Non ci sono differenze di prestazioni, sicurezza o fisiche tra le Istanze dedicate e le istanze negli Host

dedicati. Tuttavia, ci sono alcune differenze chiave tra di loro. La tabella seguente evidenzia alcune differenze chiave tra istanze dedicate e host dedicati:

	Dedicated Host	Dedicated Instance
Server fisico dedicato	Server fisico con capacità di istanza completamente dedicata.	Server fisico dedicato a un singolo account cliente.
Condivisione della capacità di istanza	Possibilità di condividere la capacità di istanza con altri account.	Non supportata
Fatturazione	Per-host fatturazione	Per-instance fatturazione
Visibilità di socket, core e ID host	Fornisce la visibilità del numero di socket e core fisici	Nessuna visibilità
Affinità a livello di host e istanza	Consente di distribuire in modo omogeneo le istanze sullo stesso server fisico nel tempo	Non supportato
Posiziona mento delle istanze interessate	Fornisce ulteriore visibilità e controllo sul posizionamento delle istanze su un server fisico	Non supportato
Ripristino automatico dell'istanza	Supportato. Per ulteriori informazioni, consulta Ripristino host dedicato di Amazon EC2.	Supportata
Modello di licenza Bring Your Own License (BYOL)	Supportata	Supporto parziale*
Prenotazioni della capacità	Non supportata	Supportata

* Le licenze Microsoft SQL Server con mobilità delle licenze tramite Software Assurance e Windows Virtual Desktop Access (VDA) possono essere utilizzate con l'istanza dedicata.

Per ulteriori informazioni sulle istanze dedicate, consulta la pagina Istanze dedicate Amazon EC2.

Restrizioni degli Host dedicati

Prima di allocare le occorrenze degli Host dedicati, considera le seguenti limitazioni e restrizioni:

- Per eseguire RHEL e SUSE Linux su Host dedicati, devi portare le tue AMI. Non è possibile utilizzare le AMI RHEL e SUSE Linux offerte AWS o disponibili con host dedicati. Marketplace AWS Per ulteriori informazioni su come creare un'AMI personalizzata, consulta Uso di licenze software proprie negli host dedicati Amazon EC2.

  Questa restrizione non si applica agli host allocati per istanze di memoria elevata (`u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` e `u-24tb1.metal`). Le AMI RHEL e SUSE Linux offerte da AWS o disponibili su Marketplace AWS possono essere utilizzate con questi host.
- È previsto un limite per il numero di host dedicati in esecuzione per famiglia di istanze per account AWS per regione. Le quote si applicano solo alle istanze in esecuzione. Se l'istanza è in sospeso, in arresto o arrestata, non viene conteggiata ai fini della quota. Per visualizzare le quote del tuo account o richiederne un aumento, utilizza la console Service Quotas.
- I gruppi Auto Scaling sono supportati solo quando si utilizza un modello di avvio che specifica un gruppo di risorse host. Per ulteriori informazioni, consulta Creazione di un modello di avvio con impostazioni avanzate nella Guida per l'utente di Amazon EC2 Auto Scaling.
- Le istanze di Amazon RDS non sono supportate.
- Il livello di utilizzo AWS gratuito non è disponibile per gli host dedicati.
- Il controllo del posizionamento delle istanze fa riferimento alla gestione degli avvii delle istanze sulle occorrenze degli Host dedicati. Non puoi avviare Host dedicati nei gruppi di collocazione.
- Se assegni un host per un tipo di istanza virtualizzata, successivamente non potrai modificare il tipo di istanza in `.metal`. Ad esempio, se assegni un host per il tipo di istanza `m5.large`, non puoi modificare il tipo di istanza in `m5.metal`.

  Allo stesso modo, se assegni un host per un tipo di istanza `.metal`, successivamente non potrai modificare il tipo di istanza in un'istanza virtualizzata. Ad esempio, se assegni un host per il tipo di istanza `m5.metal`, non puoi modificare il tipo di istanza in `m5.large`.

Indice

- Prezzi e fatturazione degli host dedicati di Amazon EC2
- Configurazioni di capacità di istanza per host dedicati di Amazon EC2
- Istanze T3 espandibili su host dedicati Amazon EC2
- Uso di licenze software proprie negli host dedicati Amazon EC2
- Auto-posizionamento dell'host dedicato Amazon EC2 e affinità degli host
- Alloca un host dedicato di Amazon EC2 per l'uso nel tuo account
- Avvia le istanze Amazon EC2 su un host dedicato Amazon EC2
- Avvio di istanze Amazon EC2 in un gruppo di risorse host
- Modifica l'impostazione di auto-posizionamento per un host dedicato Amazon EC2 esistente
- Modifica i tipi di istanza supportati per un host dedicato di Amazon EC2 esistente
- Modifica la tenancy e l'affinità dell'host dedicato Amazon EC2 per un'istanza Amazon EC2
- Rilascio di un host dedicato di Amazon EC2
- Esegui la migrazione verso host dedicati Nitro-based Amazon EC2
- Acquista prenotazioni di host dedicato per gli sconti di fatturazione per gli Host dedicati
- Cross-account Condivisione di host dedicati Amazon EC2
- Host dedicati Amazon EC2 su AWS Outposts
- Ripristino host dedicato di Amazon EC2
- Manutenzione degli host per host dedicati di Amazon EC2
- Monitora lo stato degli host dedicati di Amazon EC2
- Tieni traccia delle modifiche alla configurazione degli host dedicati di Amazon EC2 utilizzando AWS Config

Prezzi e fatturazione degli host dedicati di Amazon EC2

Il prezzo di un Host dedicato varia in base all'opzione di pagamento.

Opzioni di pagamento

- On-Demand Host dedicati
- Dedicated Host Reservations
- Savings Plans
- Prezzi per Windows Server su Host dedicati

On-Demand Host dedicati

On-Demand la fatturazione viene attivata automaticamente quando assegni un host dedicato al tuo account.

Il On-Demand prezzo per un host dedicato varia in base alla famiglia di istanze e alla regione. Il pagamento è al secondo (con un minimo di 60 secondi) per Host dedicato attivo, indipendentemente dalla quantità o dalla dimensione delle istanze che scegli di avviare su di esso. Per ulteriori informazioni sui On-Demand prezzi, consulta i On-Demand prezzi degli host dedicati di Amazon EC2.

Puoi rilasciare un Host On-Demand dedicato in qualsiasi momento per evitare che vengano addebitati costi. Per informazioni sul rilascio di un Host dedicato, consulta Rilascio di un host dedicato di Amazon EC2.

Dedicated Host Reservations

Le prenotazioni con host dedicati offrono uno sconto sulla fatturazione rispetto agli host dedicati che gestiscono On-Demand . Le prenotazioni sono disponibili con tre diverse opzioni di pagamento:

- Nessun pagamento anticipato —Le prenotazioni di questo tipo garantiscono uno sconto sull'uso dell'Host dedicato in un determinato periodo e non richiedono alcun pagamento anticipato. Opzione disponibile per un periodo di un anno o di tre anni. Solo alcune famiglie di istanze supportano il periodo di tre anni per Nessuna prenotazione anticipata.
- Pagamento anticipato parziale — Una parte della prenotazione deve essere pagata in anticipo, mentre le restanti ore nel periodo scelto vengono fatturate in base a una tariffa scontata. Opzione disponibile per un periodo di un anno o di tre anni.
- Pagamento anticipato intero costo — Questa soluzione offre il prezzo effettivo più basso. Si tratta di un'opzione disponibile per un periodo di un anno e di tre anni, che copre l'intero costo anticipato del periodo, senza costi aggiuntivi futuri.

Prima di poter acquistare le prenotazioni, devi disporre di occorrenze degli Host dedicati attive nel tuo account. Ogni prenotazione può coprire uno o più host che supportano la stessa famiglia di istanze in una singola zona di disponibilità. Le prenotazioni vengono applicate alla famiglia di istanze presenti sull'host e non alle dimensioni delle istanze. Se hai tre Host dedicati con dimensioni di istanze diverse (`m4.xlarge`, `m4.medium` e `m4.large`) puoi associare un'unica prenotazione `m4` con tutti gli Host

dedicati. La famiglia di istanze e la zona di disponibilità della prenotazione devono corrispondere a quelle degli host dedicati a cui intendi associarla.

Quando una prenotazione è associata a un Host dedicato, l'Host dedicato può essere rilasciato solo dopo il termine della prenotazione.

Per ulteriori informazioni sui prezzi delle prenotazioni, consulta la pagina dei Prezzi degli Host dedicati di Amazon EC2.

Savings Plans

I piani di risparmio sono un modello tariffario flessibile che offre risparmi significativi rispetto alle On-Demand Istanze. Con i Savings Plans, ti impegni a garantire una quantità di utilizzo coerente, in USD all'ora, per un periodo di uno o tre anni. Questo ti offre la flessibilità di utilizzare il Host dedicati che più si adatta alle tue esigenze e di continuare a risparmiare denaro, piuttosto che impegnarsi con un Host dedicato specifico. Per ulteriori informazioni, consulta la Guida per l'utente dei Savings Plans di AWS.

> **Note**
>
> I Savings Plans non sono supportati con `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` e host dedicati `u-24tb1.metal`.

Prezzi per Windows Server su Host dedicati

Conformemente alle condizioni di licenza di Microsoft, puoi portare le tue licenze per Windows Server e SQL Server negli Host dedicati. Non sono previsti costi aggiuntivi per l'uso del software se decidi di portare le tue licenze personali.

Inoltre, puoi anche usare le AMI di Windows Server fornite da Amazon per eseguire le versioni più recenti di Windows Server sui Host dedicati. Ciò è comune per i contesti in cui disponi di licenze SQL Server idonee per l'esecuzione su Host dedicati ma serve Windows Server per eseguire il carico di lavoro di SQL Server. Le AMI di Windows Server fornite da Amazon sono supportate soltanto sui tipi di istanza della generazione corrente. Per maggiori informazioni, consulta Prezzi degli host dedicati di Amazon EC2.

Configurazioni di capacità di istanza per host dedicati di Amazon EC2

Gli host dedicati supportano diverse configurazioni (core fisici, socket e vCPU) che consentono di eseguire istanze di famiglie e dimensioni diverse.

Quando assegni un host dedicato nel tuo account, puoi scegliere una configurazione che supporti o un tipo di istanza singola, oppure più tipi di istanze appartenenti alla stessa famiglia di istanze. Il numero di istanze che puoi eseguire su un host dipende dalla configurazione scelta.

Indice

- Supporto per tipi di istanza singola
- Supporto per più tipi di istanze

Supporto per tipi di istanza singola

Puoi allocare un host dedicato che supporti un solo tipo di istanza. Con questa configurazione, ogni istanza che lanci sull'host dedicato deve essere dello stesso tipo dell'istanza specificata al momento dell'allocazione dell'host.

Ad esempio, puoi allocare un host che supporti solo il tipo di istanza `m5.4xlarge`. In questo caso, puoi eseguire solo istanze `m5.4xlarge` su quell'host.

Il numero di istanze che puoi avviare sull'host dipende dal numero di core fisici forniti dall'host e dal numero di core consumati dal tipo di istanza specificato. Ad esempio, se assegni un host per istanze `m5.4xlarge` l'host fornisce 48 core fisici e ciascuna `m5.4xlarge`istanza consuma 8 core fisici. Ciò significa che puoi avviare fino a 6 istanze su quell'host (48 core fisici/ 8 core per istanza = 6 istanze).

Supporto per più tipi di istanze

È possibile allocare un host dedicato che supporti più tipi di istanze all'interno della stessa famiglia di istanze. Ciò ti consente di eseguire diversi tipi di istanze sullo stesso host, purché le istanze siano della stessa famiglia e l'host disponga di una capacità di istanza sufficiente.

Ad esempio, puoi allocare un host che supporti tipi di istanze diverse all'interno della famiglia di istanze `R5`. In questo caso, puoi lanciare determinate combinazioni di tipi di istanza `R5`, come `r5.large`, `r5.xlarge`, `r5.2xlarge` e `r5.4xlarge`, su quell'host, entro la capacità fisica principale dell'host.

Le seguenti famiglie di istanze supportano gli host dedicati con supporto per più tipi di istanze:

- Scopo generale: A1 | M5 | M5n | M6i | M7i | T3
- Ottimizzate per il calcolo: C5 | C5n | C6i | C7i

- Memoria ottimizzata: R5 | R5b | R5n | R6i | R7i | R7iZ | X2iEDN

Il numero di istanze che è possibile eseguire sull'host dipende dal numero di core fisici forniti dall'host e dal numero di core consumati da ogni tipo di istanza che viene eseguita sull'host. Ad esempio, se assegni un host R5 che fornisce 48 core fisici, e tu esegui due istanze `r5.2xlarge` (4 core x 2 istanze) e tre istanze `r5.4xlarge` (8 core x 3 istanze), queste istanze consumano un totale di 32 core e quindi potresti essere in grado di eseguire determinate combinazioni di istanze R5 purché rientrino nei 16 core rimanenti.

Tuttavia, per ogni famiglia di istanze, esiste un limite al numero di istanze che è possibile eseguire per ogni tipo di istanza. Ad esempio, un Host dedicato R5 supporta fino a 2 istanze `r5.8xlarge`, utilizzando 32 core fisici. In questo caso, è quindi possibile utilizzare istanze R5 aggiuntive di tipi più piccoli per riempire l'host fino alla capacità core. Per il numero supportato di tipi di istanze di ogni famiglia di istanze, consulta Dedicated Hosts Configuration Table.

La tabella seguente mostra esempi di combinazioni di istanze:

Famiglia di istanze	Combinazioni di tipi di istanza di esempio	
R5	• Esempio 1: 4 x `r5.4xlarge` + 4 x `r5.2xlarge` • Esempio 2: 1 x `r5.12xlarge` + 1 x `r5.4xlarge` + 1 x `r5.2xlarge` + 5 x `r5.xlarge` + 2 x `r5.large`	
C5	• Esempio 1: 1 x `c5.9xlarge` + 2 x `c5.4xlarge` + 1 x `c5.xlarge` • Esempio 2: 4 x `c5.4xlarge` + 1 x `c5.xlarge` + 2 x `c5.large`	
M5	• Esempio 1: 4 x `m5.4xlarge` + 4 x `m5.2xlarge` •	

Famiglia di istanze	Combinazioni di tipi di istanza di esempio	
	Esempio 2: 1 x `m5.12xlarge` + 1 x `m5.4xlarge` + 1 x `m5.2xlarge` + 5 x `m5.xlarge` + 2 x `m5.large`	

Considerazioni

Tieni presente che quando lavori con host dedicati che supportano più tipi di istanze:

- L'utilizzo di più tipi di istanza sullo stesso host è possibile solo all'interno della stessa famiglia di istanze.
- Quando si combinano tipi di istanze, per massimizzare l'utilizzo dell'host, consigliamo di avviare prima tipi di istanze più grandi, seguiti da tipi di istanze più piccoli.
  - A seconda della combinazione e dell'ordine di avvio dei tipi di istanza su un host dedicato, potrebbe non essere fisicamente possibile massimizzare l'utilizzo dell'host. Quando si combinano tipi di istanze su un host, una parte della capacità potrebbe essere disponibile sull'host ma non utilizzabile. Ad esempio, potresti vedere 16 vCPU disponibili su un host r5n ma potresti non essere in grado di avviare un'istanza 4xlarge sull'host anche se r5n.4xlarge viene eseguito su 16 vCPU.

> **Note**
>
> Se abiliti un host dedicato A1 per più tipi di istanze, puoi avviare solo un mix di istanze `a1.xlarge` e `a1.2xlarge` su quell'host. Se avvii un'istanza `a1.medium` o `a1.large` su quell'host, sarai limitato ad avviare solo altre istanze dello stesso tipo sull'host. Una singola istanza `a1.4xlarge` consuma tutta la capacità dell'host. Se hai bisogno di un host per istanze `a1.medium` o `a1.large`, ti consigliamo di allocare host separati per quei tipi di istanze.

Istanze T3 espandibili su host dedicati Amazon EC2

Gli host dedicati supportano istanze T3 con prestazioni espandibili. Le istanze T3 forniscono un modo efficiente nei costi per utilizzare il software di licenza BYOL idoneo su hardware dedicato. Le

dimensioni ridotte della vCPU delle istanze T3 consentono di consolidare i carichi di lavoro su un numero inferiore di host e ottimizzare l'utilizzo delle licenze per core.

Gli host dedicati T3 sono più adatti per l'esecuzione del software BYOL con utilizzo della CPU da basso a moderato. Sono incluse le licenze software idonee per socket, core o macchina virtuale, quali Windows Server, Windows Desktop, SQL Server, SUSE Enterprise Linux Server, Red Hat Enterprise Linux e Oracle Database. Esempi di carichi di lavoro adatti per gli host dedicati T3 sono database di dimensioni medie e ridotte, desktop virtuali, ambienti di sviluppo e test, archivi di codice e prototipi di prodotto. Gli host dedicati T3 non sono consigliati per carichi di lavoro con un utilizzo prolungato della CPU o per carichi di lavoro che subiscono espansioni della CPU mentre è in uso.

Le istanze T3 sugli host dedicati utilizzano lo stesso modello di credito delle istanze T3 sull'hardware di tenancy condiviso. Tuttavia, supportano solo la modalità di credito `standard`, mentre non supportano la modalità di credito `unlimited`. Nella modalità `standard`, le istanze T3 su host dedicati possono guadagnare, spendere e accumulare crediti nello stesso modo previsto per le istanze espandibili sull'hardware di tenancy condiviso. Le istanze espandibili forniscono un livello di base di prestazioni della CPU, con la possibilità di superare temporaneamente questo livello. Per superare la baseline, l'istanza spende i crediti accumulati nel suo saldo del credito CPU. Una volta esauriti i crediti accumulati, l'utilizzo della CPU viene ridotto al livello di base. Per ulteriori informazioni sulla modalità `standard`, consulta la pagina Come funzionano le istanze a prestazioni espandibili Standard.

Gli host dedicati T3 supportano tutte le funzionalità offerte dagli host dedicati Amazon EC2, incluse le dimensioni di istanze multiple su un singolo host, gruppi di risorse host e BYOL.

Dimensioni e configurazioni dell'istanza T3 supportate

Gli host dedicati T3 eseguono istanze T3 espandibili di scopo generico che condividono le risorse della CPU dell'host, fornendo prestazioni della CPU di base e la possibilità di passare a un livello superiore quando necessario. Ciò consente agli host dedicati T3, che possiedono 48 core, di supportare fino a un massimo di 192 istanze per host. Per utilizzare in modo efficiente le risorse dell'host e fornire le migliori prestazioni delle istanze, l'algoritmo di posizionamento delle istanze di Amazon EC2 calcola automaticamente il numero supportato di istanze e le combinazioni di dimensioni delle istanze che possono essere avviate sull'host.

Gli host dedicati T3 supportano più tipi di istanza sullo stesso host. Tutte le istanze T3 sono supportate su host dedicati. È possibile eseguire diverse combinazioni di istanze T3 fino al limite della CPU dell'host.

Nella tabella seguente sono riportati i tipi di istanze supportati, le prestazioni di ciascun tipo di istanza e il numero massimo di istanze di ogni dimensione che è possibile avviare.

Tipo di istan	vCPU	Memoria (GiB)	Utilizzo di base della CPU per vCPU	Larghezza di banda burst di rete (Gbps)	Larghezza di banda burst Amazon EBS (Mbps)	Numero massimo di istanze per host dedicato
t3.na	2	0,5	5%	5	Fino a 2.085	192
t3.m	2	1	10%	5	Fino a 2.085	192
t3.sn	2	2	20%	5	Fino a 2.085	192
t3.m	2	4	20%	5	Fino a 2.085	192
t3.la	2	8	30%	5	2.780	96
t3.xl	4	16	40%	5	2.780	48
t3.2x e	8	32	40%	5	2.780	24

Monitorare l'utilizzo della CPU per gli host dedicati T3

Puoi utilizzare la CloudWatch metrica `DedicatedHostCPUUtilization` Amazon per monitorare l'utilizzo della vCPU di un host dedicato. Il parametri è disponibile nel namespace `EC2` e nella dimensione `Per-Host-Metrics`. Per ulteriori informazioni, consulta Parametri degli host dedicati.

Uso di licenze software proprie negli host dedicati Amazon EC2

Gli Host dedicati ti consentono di utilizzare licenze software esistenti per socket, core o macchina virtuale. Quando utilizzi la tua licenza, sei responsabile della sua gestione. Amazon EC2 offre tuttavia caratteristiche che aiutano a rispettare la conformità delle licenze, come l'affinità e il posizionamento delle istanze interessate.

Questi sono i passaggi generali da seguire per importare la propria immagine di macchina con multilicenza in Amazon EC2.

1. Verificare che le condizioni di licenza che determinano l'uso delle immagini di macchine virtuali ne consentano l'utilizzo in un ambiente cloud virtualizzato. Per ulteriori informazioni sui programmi di licenze Microsoft, consulta l'argomento relativo alle opzioni di licenza per i software Microsoft su Amazon Web Services.
2. Dopo aver verificato che l'immagine della macchina può essere utilizzata in Amazon EC2, importala tramite VM. Import/Export Per informazioni su come importare l'immagine della macchina, consulta la VM Import/Export User Guide.
3. Dopo avere importato l'immagine della macchina virtuale, da questa è possibile avviare le istanze negli Host dedicati attivi dell'account.
4. Quando vengono eseguite queste istanze, in base al sistema operativo in uso, potrebbe venire richiesto di attivare queste istanze mediante il server KMS (ad esempio, Windows Server o Windows SQL Server). Non è possibile attivare l'AMI Windows importata nel server Amazon KMS per Windows.

> **Note**
>
> Per tenere traccia di come vengono utilizzate le immagini in AWS, abilita la registrazione host in AWS Config. È possibile AWS Config utilizzarlo per registrare le modifiche alla configurazione su un host dedicato e utilizzare l'output come fonte di dati per la segnalazione delle licenze. Per ulteriori informazioni, consulta Tieni traccia delle modifiche alla configurazione degli host dedicati di Amazon EC2 utilizzando AWS Config.

Auto-posizionamento dell'host dedicato Amazon EC2 e affinità degli host

Il controllo del posizionamento per Host dedicati viene eseguito sia a livello di istanza che a livello di host.

Auto-placement

Auto-placement è configurato a livello di host. e consente di gestire se le istanze vengono avviate su un host specifico o su qualsiasi host disponibile che dispone di configurazioni corrispondenti.

Quando l'auto-posizionamento è disabilitato per un host dedicato, sono accettati solo gli avvii di istanza della tenancy host in cui sia specificato il relativo ID host univoco. Questa rappresenta l'impostazione di default per le nuove occorrenze degli Host dedicati.

Quando l'auto-posizionamento è abilitato per un Host dedicato, è accettato qualsiasi avvio di istanza della tenancy host non mirato che corrisponde alla relativa configurazione del tipo di istanza.

Quando viene avviata un'istanza, devi configurare la relativa tenancy. L'avvio di un'istanza in un Host dedicato senza definire un valore specifico per `HostId` consente l'avvio dell'istanza su qualsiasi Host dedicato con l'auto-posizionamento abilitato e con il tipo di istanza corrispondente.

Affinità host

L'affinità host viene configurata a livello di istanza. Definisce la relazione di avvio tra un'istanza e un Host dedicato.

Quando l'affinità è impostata su `Host`, un'istanza avviata su un host specifico, se arrestata, verrà sempre riavviata sullo stesso host. Ciò è valido sia per gli avvii mirati che per quelli non mirati.

Quando l'affinità è impostata su `Default`, se si arresta e quindi riavvia un'istanza, tale istanza può essere riavviata su qualsiasi host disponibile. Tuttavia, l'istanza eseguirà un tentativo di riavvio sull'ultimo Host dedicato su cui è stata avviata (sulla base del miglior tentativo).

Alloca un host dedicato di Amazon EC2 per l'uso nel tuo account

Per iniziare a utilizzare un Host dedicato, per prima cosa devi allocarlo nel tuo account. Dopo aver allocato l'Host dedicato, la capacità Host dedicato viene resa immediatamente disponibile nell'account e puoi iniziare ad avviare istanze sull'Host dedicato.

Quando assegni un host dedicato nel tuo account, puoi scegliere una configurazione che supporti o un tipo di istanza singola, oppure più tipi di istanze appartenenti alla stessa famiglia di istanze. Il numero di istanze che puoi eseguire su un host dipende dalla configurazione scelta. Per ulteriori informazioni, consulta Configurazioni di capacità di istanza per host dedicati di Amazon EC2.

Console

Per allocare un Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati), quindi Allocate Host dedicato (Alloca host dedicati).
3. Per Instance family (Famiglia di istanze), scegliere la famiglia di istanze per l'Host dedicato.
4. Specificare se l'Host dedicato supporta più dimensioni di istanze all'interno della famiglia di istanze selezionata o solo un tipo di istanza specifico. Scegli una delle seguenti operazioni.

- Per configurare l'Host dedicato per supportare più tipi di istanze nella famiglia di istanze selezionata, per Support multiple instance types (Supporto per più tipi di istanza) selezionare Enable (Abilita). L'abilitazione di questa opzione consente di avviare diverse dimensioni di istanza dalla stessa famiglia di istanze sull'Host dedicato. Ad esempio, se si sceglie la famiglia di istanze `m5` e si seleziona questa opzione, è possibile avviare le istanze `m5.xlarge` e `m5.4xlarge` sull'Host dedicato.
- Per configurare l'Host dedicato per supportare un tipo di istanza singolo all'interno della famiglia di istanze selezionata, deselezionare Support multiple instance types (Supporto per più tipi di istanze), quindi per Instance type (Tipo di istanza), scegliere il tipo di istanza da supportare. L'abilitazione di questa opzione consente di avviare un singolo tipo di istanza sull'Host dedicato. Ad esempio, se si sceglie questa opzione e si specifica `m5.4xlarge` come il tipo di istanza supportato, è possibile avviare solo istanze `m5.4xlarge` sull'Host dedicato.

5. Per Zona di disponibilità, scegliere la zona di disponibilità in cui allocare l'Host dedicato.
6. Per consentire all'Host dedicato di accettare avvii di istanze non mirati che corrispondono a questo tipo di istanza, per Instance auto-placement (Autoposizionamento istanza), scegliere Attiva. Per ulteriori informazioni sull'auto-posizionamento, consulta Auto-posizionamento dell'host dedicato Amazon EC2 e affinità degli host.
7. Per abilitare il ripristino per l'Host dedicato, per Host recovery (Ripristino host), scegliere Enable (Attiva). Per ulteriori informazioni, consulta Ripristino host dedicato di Amazon EC2.
8. Per Quantity (Quantità), immettere il numero di Host dedicati da allocare.
9. (Facoltativo) Seleziona Aggiungi nuovo tag e immetti una chiave e un valore di tag.
10. Selezionare Alloca.

AWS CLI

Per allocare un Host dedicato

Utilizza il comando allocate-hosts. L'esempio seguente consente di allocare un Host dedicato che supporta più tipi di istanza della famiglia di istanze `m5` nella zona di disponibilità `us-east-1a`. Consente inoltre il ripristino dell'host e disabilita il posizionamento automatico.

```
aws ec2 allocate-hosts \
    --instance-family "m5" \
    --availability-zone "us-east-1a" \
```

```
    --auto-placement "off" \
    --host-recovery "on" \
    --quantity 1
```

L'esempio seguente alloca un Host dedicato che supporta avvii di istanze non mirati nella zona di disponibilità specificata, abilita il ripristino dell'host e il posizionamento automatico.

```
aws ec2 allocate-hosts \
    --instance-type "m5.large" \
    --availability-zone "eu-west-1a" \
    --auto-placement "on" \
    --host-recovery "on" \
    --quantity 1
```

PowerShell

Per allocare un Host dedicato

Utilizza il cmdlet New-EC2Host. L'esempio seguente consente di allocare un Host dedicato che supporta più tipi di istanza della famiglia di istanze `m5` nella zona di disponibilità `us-east-1a`. L'host ha il ripristino dell'host abilitato e il posizionamento automatico disabilitato.

```
New-EC2Host `
    -InstanceFamily m5 `
    -AvailabilityZone us-east-1a `
    -AutoPlacement Off `
    -HostRecovery On `
    -Quantity 1
```

Il comando seguente alloca un Host dedicato che supporta avvii di istanze non mirati nella zona di disponibilità specificata e abilita il ripristino dell'host.

```
New-EC2Host `
    -InstanceType m5.large `
    -AvailabilityZone eu-west-1a `
    -AutoPlacement On `
    -HostRecovery On `
    -Quantity 1
```

Avvia le istanze Amazon EC2 su un host dedicato Amazon EC2

Dopo aver allocato un Host dedicato, puoi avviare istanze su tale host. Non puoi avviare istanze con la tenancy `host` se non disponi di occorrenze attive degli Host dedicati con una capacità disponibile sufficiente per il tipo di istanza che stai avviando.

Considerazioni

- Le AMI di SQL Server, SUSE e RHEL fornite da Amazon EC2 non possono essere utilizzate con le occorrenze degli Host dedicati.
- Per gli host dedicati che supportano più dimensioni di istanza, si consiglia di avviare prima le istanze di grandi dimensioni e di riempire la capacità di istanza rimanente con le istanze di dimensioni più piccole in base alle esigenze.
- Prima di avviare le istanze, considera le seguenti limitazioni. Per ulteriori informazioni, consulta Restrizioni degli Host dedicati.

Console

Per avviare un'istanza su un Host dedicato specifico dalla pagina Host dedicati

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Host dedicati (Host dedicati).
3. Nella pagina Dedicated Hosts (Host dedicati), seleziona un host e scegli Operazioni, Avvia istanze sull'host.
4. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona un'AMI dall'elenco.
5. Nella sezione Tipo di istanza, seleziona il tipo di istanza da avviare.

> **Note**
>
> Se l'Host dedicato supporta solo un singolo tipo di istanza, il tipo di istanza supportato viene selezionato per impostazione predefinita e non può essere modificato.
> Se l'Host dedicato supporta più tipi di istanza, occorre selezionare un tipo di istanza all'interno della famiglia di istanze supportata in base alla capacità di istanze disponibile dell'Host dedicato. Si consiglia di avviare prima le istanze di grandi

dimensioni e di riempire la capacità di istanza rimanente con le istanze di dimensioni più piccole in base alle esigenze.

6. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da associare all'istanza.
7. Nella sezione Dettagli avanzati, per Affinità di tenancy scegli una delle operazioni seguenti:
   - Disattivata – L'affinità host è disabilitata. L'istanza viene avviata sull'host specificato, ma non è garantito il riavvio sullo stesso Host dedicato se l'istanza viene arrestata.
   - Un ID host dedicato – Affinità host abilitata. Se viene arrestata, l'istanza viene sempre riavviata su questo host specificato, se dispone di capacità. Se l'host non dispone di capacità, l'istanza non può essere riavviata; è necessario stabilire un'affinità con un host diverso.

   Per ulteriori informazioni sull'affinità, consulta Auto-posizionamento dell'host dedicato Amazon EC2 e affinità degli host.

   > **Note**
   >
   > Le opzioni Tenancy e Host sono preconfigurate in base all'host selezionato.

8. Configura le opzioni rimanenti dell'istanza in base alla necessità. Per ulteriori informazioni, consulta Riferimento per i parametri di configurazione delle EC2 istanze Amazon.
9. Scegliere Launch Instance (Avvia istanza).

Per avviare un'istanza su un Host dedicato tramite la procedura guidata di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Istanze, Avvia istanza.
3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona un'AMI dall'elenco.
4. Nella sezione Tipo di istanza, seleziona il tipo di istanza da avviare.
5. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da associare all'istanza.
6. Nella sezione Avanzate, effettua le operazioni seguenti:

a. Per Tenancy, scegli Host dedicato.

b. Per Target host by (Host di destinazione per), seleziona Host ID (ID host).

c. Per Target host ID (ID host di destinazione), seleziona l'host su cui avviare l'istanza.

d. Per Affinità di tenancy, scegli una delle operazioni seguenti:

- Disattivata – L'affinità host è disabilitata. L'istanza viene avviata sull'host specificato, ma non è garantito il riavvio sullo stesso Host dedicato se l'istanza viene arrestata.
- Un ID host dedicato – Affinità host abilitata. Se viene arrestata, l'istanza viene sempre riavviata su questo host specificato, se dispone di capacità. Se l'host non dispone di capacità, l'istanza non può essere riavviata; è necessario stabilire un'affinità con un host diverso.

Per ulteriori informazioni sull'affinità, consulta Auto-posizionamento dell'host dedicato Amazon EC2 e affinità degli host.

7. Configura le opzioni rimanenti dell'istanza in base alla necessità. Per ulteriori informazioni, consulta Riferimento per i parametri di configurazione delle EC2 istanze Amazon.
8. Scegliere Launch Instance (Avvia istanza).

AWS CLI

Per avviare un'istanza su un'Host dedicato

Utilizza il comando run-instances e specifica l'affinità dell'istanza, la tenancy e l'host nell'opzione `--placement`.

Per avviarsi su un host dedicato specifico con affinità con l'host (l'istanza si riavvia sempre sullo stesso host se viene interrotta):

```
--placement Affinity=host,Tenancy=host,HostId=h-07879acf49EXAMPLE
```

Per avviarsi su un host dedicato specifico senza affinità con l'host (l'istanza può riavviarsi su qualsiasi host disponibile):

```
--placement Tenancy=host,HostId=h-07879acf49EXAMPLE
```

Per eseguire l'avvio su qualsiasi host dedicato disponibile con il posizionamento automatico abilitato e il tipo di istanza corrispondente:

```
--placement Tenancy=host
```

PowerShell

Per avviare un'istanza su un'Host dedicato

Utilizza il New-EC2Instance cmdlet e specifica l'affinità, la tenancy e l'host dell'istanza nel parametro. `-Placement`

Per avviarsi su un host dedicato specifico con affinità host (l'istanza si riavvia sempre sullo stesso host se viene interrotta):

```
-Placement_Affinity host `
-Placement_Tenancy host `
-Placement_HostId h-07879acf49EXAMPLE
```

Per avviarsi su un host dedicato specifico senza affinità con l'host (l'istanza può riavviarsi su qualsiasi host disponibile):

```
-Placement_Tenancy host `
-Placement_HostId h-07879acf49EXAMPLE
```

Per eseguire l'avvio su qualsiasi host dedicato disponibile con il posizionamento automatico abilitato e il tipo di istanza corrispondente:

```
-Placement_Tenancy host
```

Avvio di istanze Amazon EC2 in un gruppo di risorse host

Gli host dedicati sono inoltre integrati con AWS License Manager. Con License Manager, è possibile creare un gruppo di risorse host, ovvero una raccolta di Host dedicati gestiti come una singola entità. Quando si crea un gruppo di risorse host, si specificano le preferenze di gestione host, ad esempio l'allocazione automatica e il rilascio automatico, per gli Host dedicati. In questo modo è possibile avviare le istanze in Host dedicati senza allocare e gestire manualmente tali host. Per ulteriori

informazioni, consulta la sezione relativa ai Host Resource Groups nella Guida per l'utente di AWS License Manager .

Quando si avvia un'istanza in un gruppo di risorse host che include un Host dedicato con capacità di istanze disponibile, Amazon EC2 avvia l'istanza su tale host. Se il gruppo di risorse host non include un host con capacità di istanze disponibile, Amazon EC2 alloca automaticamente un nuovo host nel gruppo di risorse host e quindi avvia l'istanza su tale host. Per ulteriori informazioni, consulta la sezione relativa ai gruppi di risorse host nella Guida per l'utente di AWS License Manager .

Requisiti e limiti

- La creazione di configurazioni di licenza (licenze autogestite) per i gruppi di risorse host è facoltativa:
  - Se hai richiesto le configurazioni di licenza durante la creazione del gruppo di risorse host, puoi avviare istanze solo dalle AMI con una configurazione di licenza basata su core o socket corrispondente.
  - Se hai creato il gruppo di risorse host per non richiedere configurazioni di licenza, non è necessario impostare licenze autogestite o associare un'AMI.
- Non è possibile utilizzare le AMI di SQL Server, SUSE o RHEL fornite da Amazon EC2 con Host dedicati.
- Non è possibile scegliere un host specifico scegliendo un ID host e non è possibile abilitare l'affinità di istanza quando si avvia un'istanza in un gruppo di risorse host.

Console

Per avviare un'istanza in un gruppo di risorse host

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Istanze, Avvia istanza.
3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona un'AMI dall'elenco.
4. Nella sezione Tipo di istanza, seleziona il tipo di istanza da avviare.
5. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da associare all'istanza.
6. Nella sezione Avanzate, effettua le operazioni seguenti:

   a. Per Tenancy, scegli Dedicated Host (Host dedicato).

b. Per Target host by (Host di destinazione per), seleziona Host resource group (Gruppo di risorse host).

c. Per Tenancy host resource group (Gruppo di risorse host di tenancy), scegli il gruppo di risorse host in cui avviare l'istanza.

d. Per Tenancy affinity (Affinità locazione), effettua una delle operazioni seguenti:

- Seleziona Disattivata: l'istanza viene avviata sull'host specificato ma non è garantito che venga riavviata sullo stesso host dedicato se viene arrestata.
- Seleziona l'ID host dedicato: se viene arrestata, l'istanza viene sempre riavviata su questo host specifico.

Per ulteriori informazioni sull'affinità, consulta Auto-posizionamento dell'host dedicato Amazon EC2 e affinità degli host.

7. Configura le opzioni rimanenti dell'istanza in base alla necessità. Per ulteriori informazioni, consulta Riferimento per i parametri di configurazione delle EC2 istanze Amazon.
8. Scegliere Launch Instance (Avvia istanza).

AWS CLI

Per avviare un'istanza in un gruppo di risorse host

Utilizzare il comando run-instances. Nell'opzione `--placement`, ometti la tenancy e specifica l'ARN del gruppo di risorse dell'host.

```
--placement HostResourceGroupArn=arn:aws:resource-groups:us-
east-2:123456789012:group/my-resource-group
```

PowerShell

Per avviare un'istanza in un gruppo di risorse host

Utilizza il cmdlet New-EC2Instance. Nel parametro `-Placement`, ometti la tenancy e specifica l'ARN del gruppo di risorse dell'host.

```
-Placement_HostResourceGroupArn arn:aws:resource-groups:us-
east-2:123456789012:group/my-resource-group
```

Modifica l'impostazione di auto-posizionamento per un host dedicato Amazon EC2 esistente

Puoi modificare le impostazioni di posizionamento automatico di un host dedicato dopo averlo assegnato al tuo account. AWS

Console

Per modificare il posizionamento automatico di un Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Selezionare un host e scegliere Actions (Operazioni), Modify host (Modifica host).
4. In instance auto-placement (auto-posizionamento istanza), scegliere Enable (Abilita) per abilitare l'auto-posizionamento oppure deselezionare Enable (Abilita) per disabilitare l'auto-posizionamento. Per ulteriori informazioni, consulta Auto-posizionamento dell'host dedicato Amazon EC2 e affinità degli host.
5. Seleziona Salva.

AWS CLI

Per modificare il posizionamento automatico di un Host dedicato

Utilizza il comando modify-hosts.

```
aws ec2 modify-hosts \
    --auto-placement on \
    --host-ids h-012a3456b7890cdef
```

PowerShell

Per modificare il posizionamento automatico di un Host dedicato

Utilizza il cmdlet Edit-EC2Host.

```
Edit-EC2Host `
    -AutoPlacement 1 `
    -HostId h-012a3456b7890cdef
```

Modifica i tipi di istanza supportati per un host dedicato di Amazon EC2 esistente

Puoi modificare un Host dedicato per cambiare i tipi di istanza supportati. Se attualmente supporta un singolo tipo di istanza, puoi modificarlo per supportare più tipi di istanza all'interno di tale famiglia di istanze. Analogamente, se attualmente supporta più tipi di istanza, puoi modificarlo per supportare solo un tipo di istanza specifico.

Per modificare un Host dedicato per supportare più tipi di istanza, occorre innanzitutto interrompere tutte le istanze in esecuzione sull'host. Il completamento di questa modifica richiede circa 10 minuti. L'Host dedicato passa allo stato `pending` mentre è in corso la modifica. Non è possibile avviare istanze interrotte o lanciare nuove istanze sull'Host dedicato mentre si trova nello stato `pending`.

Per modificare un Host dedicato che supporta più tipi di istanza per supportare solo un tipo di istanza singolo, l'host non deve avere istanze in esecuzione o il tipo delle istanze in esecuzione deve essere supportato dall'host. Ad esempio, per modificare un host che supporta più tipi di istanza nella famiglia di istanze `m5` per supportare solo istanze `m5.large`, non devono esserci istanze in esecuzione sull'Host dedicato o quelle in esecuzione devono essere solo istanze `m5.large`.

Se assegni un host per un tipo di istanza virtualizzata, successivamente non potrai modificare il tipo di istanza in `.metal`. Ad esempio, se assegni un host per il tipo di istanza `m5.large`, non puoi modificare il tipo di istanza in `m5.metal`. Allo stesso modo, se assegni un host per un tipo di istanza `.metal`, successivamente non potrai modificare il tipo di istanza in un'istanza virtualizzata. Ad esempio, se assegni un host per il tipo di istanza `m5.metal`, non puoi modificare il tipo di istanza in `m5.large`.

Console

Per modificare i tipi di istanza supportati per un Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Dedicated Host (Host dedicato).
3. Selezionare l'Host dedicato da modificare e scegliere Actions (Operazioni), Modify host (Modifica host).
4. In base alla configurazione corrente dell'Host dedicato, eseguire una delle operazioni riportate di seguito:

   - Se l'Host dedicato attualmente supporta un tipo di istanza specifico, l'opzione Support multiple instance types (Supporto per più tipi di istanza) non è abilitata e Instance type (Tipo di istanza) elenca il tipo di istanza supportato. Per modificare l'host per supportare più

tipi nella famiglia di istanze corrente, per Support multiple instance types (Supporto per più tipi di istanza), selezionare Enable (Abilita).

Prima di modificare un host per supportare più tipi di istanza, è necessario innanzitutto interrompere tutte le istanze in esecuzione su di esso.

- Se l'Host dedicato attualmente supporta più tipi di istanza in una famiglia di istanze, l'opzione Enabled (Abilitato) è selezionata per Support multiple instance types (Supporto per più tipi di istanza). Per modificare l'host per supportare un tipo di istanza specifico, per Support multiple instance types (Supporto per più tipi di istanza), deselezionare Enable (Abilita), quindi per Instance type (Tipo di istanza), selezionare il tipo di istanza da supportare.

  Non è possibile modificare la famiglia di istanze supportata da Host dedicato.

5. Seleziona Salva.

AWS CLI

Per modificare i tipi di istanza supportati per un Host dedicato

Utilizza il comando modify-hosts.

L'esempio seguente consente di modificare un Host dedicato per supportare più tipi di istanza all'interno della famiglia di istanze `m5`.

```
aws ec2 modify-hosts \
    --instance-family m5 \
    --host-ids h-012a3456b7890cdef
```

L'esempio seguente consente di modificare un Host dedicato per supportare solo istanze `m5.xlarge`.

```
aws ec2 modify-hosts \
    --instance-type m5.xlarge \
    --instance-family --host-ids h-012a3456b7890cdef
```

PowerShell

Per modificare i tipi di istanza supportati per un Host dedicato

Utilizza il cmdlet Edit-EC2Host.

L'esempio seguente consente di modificare un Host dedicato per supportare più tipi di istanza all'interno della famiglia di istanze `m5`.

```
Edit-EC2Host `
    -InstanceFamily m5 `
    -HostId h-012a3456b7890cdef
```

L'esempio seguente consente di modificare un Host dedicato per supportare solo istanze `m5.xlarge`.

```
Edit-EC2Host `
    -InstanceType m5.xlarge `
    -HostId h-012a3456b7890cdef
```

Modifica la tenancy e l'affinità dell'host dedicato Amazon EC2 per un'istanza Amazon EC2

Puoi modificare la tenancy di un'istanza dopo averla avviata. Puoi anche modificare l'affinità della tua istanza per indirizzarla a un host specifico o consentirne l'avvio su qualsiasi host dedicato disponibile con attributi corrispondenti nel tuo account. Per modificare la tenancy o l'affinità dell'istanza, lo stato dell'istanza deve essere `stopped`.

I dettagli del sistema operativo dell'istanza e l'eventuale installazione di SQL Server influiscono sulle conversioni supportate. Per ulteriori informazioni sui percorsi di conversione di tenancy disponibili per la tua istanza, consulta Conversione di tenancy nella Guida per l'utente di License Manager.

> **Note**
>
> Per le istanze T3, è necessario avviare l'istanza su un host dedicato per utilizzare una tenancy di `host`. Per le istanze T3, non è possibile modificare la tenancy da `host` a `dedicated` o `default`. Se si prova ad apportare una di queste modifiche di tenancy non supportate, verrà visualizzato il codice di errore `InvalidRequest`.

Console

Per modificare la tenancy o l'affinità dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Scegliere Instances (Istanze) e selezionare l'istanza da modificare.
3. Scegli Instance state (Stato istanza), Stop (Arresta).
4. Con l'istanza selezionata, scegli Operazioni, Impostazioni istanza, Modifica posizionamento delle istanze.
5. Nella pagina Modifica posizionamento istanza, configurare quanto segue:

   - Tenancy — Scegliere una delle opzioni indicate di seguito.
     - Run a dedicated hardware instance (Esegui un'istanza hardware dedicata) — Avvia l'istanza sotto forma di Istanza dedicata. Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2.
     - Launch the instance on a Host dedicato (Avvia istanza su un host dedicato) — Avvia l'istanza su un Host dedicato con l'affinità configurabile.
   - Affinity (Affinità) — Scegliere una delle opzioni indicate di seguito.
     - This instance can run on any one of my hosts (Questa istanza può essere eseguita su uno qualsiasi dei miei host) – L'istanza viene avviata su qualsiasi Host dedicato disponibile nell'account che supporti il relativo tipo di istanza.
     - This instance can only run on the selected host (Questa istanza può essere eseguita solo sull'host selezionato) – L'istanza può essere eseguita solo sull'Host dedicato selezionato per l'opzione Target Host (Host target).
   - Target Host (Host target) — Selezionare l'Host dedicato su cui deve essere eseguita l'istanza. Se nell'elenco non è presente alcun host target, è possibile che l'account non includa degli Host dedicati compatibili disponibili.

   Per ulteriori informazioni, consulta Auto-posizionamento dell'host dedicato Amazon EC2 e affinità degli host.
6. Seleziona Salva.

AWS CLI

Per modificare la tenancy o l'affinità dell'istanza

Utilizzare il comando modify-instance-placement. Gli esempi seguenti illustrano la modifica dell'affinità dell'istanza specificata da `default` in `host` e l'impostazione dell'Host dedicato con cui l'istanza ha affinità.

```
aws ec2 modify-instance-placement \
    --instance-id i-1234567890abcdef0 \
    --affinity host \
    --tenancy host \
    --host-id h-012a3456b7890cdef
```

PowerShell

Per modificare la tenancy o l'affinità dell'istanza

Utilizza il cmdlet Edit-EC2InstancePlacement. Gli esempi seguenti illustrano la modifica dell'affinità dell'istanza specificata da `default` in `host` e l'impostazione dell'Host dedicato con cui l'istanza ha affinità.

```
Edit-EC2InstancePlacement `
    -InstanceId i-1234567890abcdef0 `
    -Affinity host `
    -Tenancy host `
    -HostId h-012a3456b7890cdef
```

Rilascio di un host dedicato di Amazon EC2

Se un host dedicato non è più necessario, puoi arrestare le istanze eseguite su di esso, impostarne l'avvio su un host diverso e quindi rilasciare l'host.

Prima di poter rilasciare l'host, è necessario arrestare tutte le istanze in esecuzione sull'Host dedicato. È possibile eseguire la migrazione di queste istanze su altre occorrenze degli Host dedicati nel tuo account in modo da consentirti di continuare a utilizzarle. Questi passaggi si applicano solo agli host On-Demand dedicati.

Console

Per rilasciare un Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Nella pagina Host dedicati, selezionare il Host dedicato da rilasciare.
4. Scegliere Actions (Operazioni), Release host (Rilascia host).

5. Scegliere Release (Rilascia).

AWS CLI

Per rilasciare un Host dedicato

Utilizza il comando release-hosts.

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

PowerShell

Per rilasciare un Host dedicato

Utilizza il cmdlet Remove-EC2Host.

```
Remove-EC2Host -HostId h-012a3456b7890cdef
```

Dopo aver rilasciato un host dedicato, non puoi riutilizzare nuovamente lo stesso host o ID host e non ti verranno più addebitate le relative tariffe di On-Demand fatturazione. Lo stato dell'Host dedicato viene cambiato in `released` e su tale host non sarà più possibile avviare istanze.

> **Note**
>
> Nel caso di Host dedicati rilasciati di recente, potrebbe essere necessario un po' di tempo prima che vengano esclusi dal conteggio del limite. Durante questo periodo di tempo, potresti riscontrare errori di tipo `LimitExceeded` quando cerchi di allocare nuove occorrenze degli Host dedicati. Se questo è il caso, prova ad allocare nuovi host dopo pochi minuti.

Le istanze precedentemente arrestate continuano a essere disponibili per l'uso e sono elencate nella pagina Instances (Istanze). Relativamente alla tenancy, tali istanze conservano l'impostazione `host`.

Esegui la migrazione verso host dedicati Nitro-based Amazon EC2

Il sistema Nitro è una raccolta di componenti hardware e software creati per AWS garantire alte prestazioni, alta disponibilità e alta sicurezza. Nitro-based Gli host dedicati offrono un rapporto

prezzo/prestazioni migliorate rispetto agli host Xen-based dedicati. Se nel tuo account sono presenti host Xen-based dedicati, ti consigliamo di migrare i carichi di lavoro verso host Nitro-based dedicati. Per ulteriori informazioni, consulta Sistema AWS Nitro.

Per migrare da un host Xen-based dedicato a un host Nitro-based dedicato, devi migrare Xen-based le istanze sull'host dedicato ai tipi di istanze, allocare un nuovo host Nitro-based dedicato e quindi spostare le Nitro-based istanze migrate Nitro-based sul nuovo host dedicato. Nitro-based

Questo argomento fornisce i passaggi dettagliati per la migrazione da host dedicati a host dedicati. Xen-based Nitro-based

Fasi della migrazione

- Fase 1: Identifica i tuoi host Xen-based dedicati
- Fase 2: migrazione delle istanze verso Xen-based tipi di istanze Nitro-based
- Fase 3: allocare un host dedicato Nitro-based
- Passaggio 4: sposta le istanze migrate su un nuovo host dedicato Nitro-based
- Passaggio 5: rilascia l'host Xen-based dedicato inutilizzato

Fase 1: Identifica i tuoi host Xen-based dedicati

I seguenti host dedicati sono Xen-based e sono idonei alla migrazione verso host Nitro-based dedicati.

- Scopo generico: M3 | M4
- Ottimizzati per il calcolo: C3 | C4
- Ottimizzati per la memoria: R3 | R4 | X1 | X1e
- Ottimizzate per l'archiviazione: D2 | H1 | I2 | I3
- Elaborazione accelerata: G3 | P3

Per verificare se nel tuo account sono Xen-based presenti host dedicati

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, seleziona Host dedicati.
3. Nel campo Cerca, utilizza il filtro della famiglia di istanze per cercare gli host Xen-based dedicati sopra indicati. Ad esempio, Famiglia di istanze = m3.

Fase 2: migrazione delle istanze verso Xen-based tipi di istanze Nitro-based

Lo sono anche le istanze eseguite su host Xen-based dedicati. Xen-based È necessario migrare queste istanze verso tipi di Nitro-based istanze prima di poterle spostare su host dedicati Nitro-based .

> **Important**
>
> Prima di iniziare la migrazione delle istanze, consigliamo di eseguire il backup dei dati. Per ulteriori informazioni, consulta Creare snapshot Amazon EBS multi-volume da un'istanza Amazon EC2.

Per trovare le istanze in esecuzione sui tuoi host dedicati Xen-based

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, seleziona Host dedicati.
3. Seleziona l' Xen-based host che intendi migrare, quindi seleziona la scheda Istanze in esecuzione. La scheda elenca tutte le istanze in esecuzione sull'host selezionato.

Per migrare le istanze Linux, consulta Modifiche del tipo di istanza Amazon EC2.

Per migrare le istanze Windows, consulta Esegui la migrazione di un'istanza EC2 per Windows a un tipo di istanza Nitro-based.

> **Note**
>
> Assicurati di migrare le tue istanze su un tipo di istanza che corrisponda Nitro-based all'host dedicato a cui intendi migrare. Ad esempio, se intendi effettuare la migrazione verso un host dedicato M7i, assicurati di migrare le istanze verso un tipo di istanza M7i.

Fase 3: allocare un host dedicato Nitro-based

Per trovare host Nitro-based dedicati supportati

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, seleziona Tipi di istanza.

3. Applica i seguenti filtri:

   - Hypervisor = nitro
   - Supporto host dedicato = true

Dopo aver trovato un tipo di Nitro-based istanza adatto, assegna un nuovo host dedicato.

Passaggio 4: sposta le istanze migrate su un nuovo host dedicato Nitro-based

Dopo aver allocato l'host Nitro-based dedicato e aver raggiunto lo `available` stato, puoi spostare le istanze precedentemente migrate ai tipi di Nitro-based istanza nel nuovo host dedicato.

Per spostare le istanze sul nuovo host dedicato Nitro-based

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, Istanze.
3. Seleziona l'istanza migrata e scegli Operazioni, Impostazioni istanza, Modifica posizionamento dell'istanza.
4. Per l'host dedicato di Target, seleziona il nuovo host Nitro-based dedicato, quindi scegli Salva.
5. Riavvia l'istanza. Seleziona l'istanza e scegli Stato istanza, Avvia istanza.

Passaggio 5: rilascia l'host Xen-based dedicato inutilizzato

Dopo aver migrato i carichi di lavoro dall'host Xen-based dedicato al nuovo host Nitro-based dedicato, puoi rilasciare l'host Xen-based dedicato se non ti serve più.

Acquista prenotazioni di host dedicato per gli sconti di fatturazione per gli Host dedicati

Le prenotazioni con host dedicati ti offrono uno sconto fino al 70 percento rispetto ai prezzi degli host On-Demand dedicati. Prima di poter acquistare le prenotazioni di host dedicato, devi disporre host dedicati attivi allocati nel tuo account. Per ulteriori informazioni, consulta Dedicated Host Reservations.

Console

Per acquistare le prenotazioni

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Scegliere Host dedicati, Prenotazioni di host dedicati, Purchase (Acquista) Prenotazioni di host dedicati.
3. Nella schermata Trova offerte, effettua le seguenti operazioni:

   a. Per Famiglia di istanze, seleziona la famiglia di istanze dell'host dedicato per cui acquistare la prenotazione di un host dedicato.

   b. Per Opzione di pagamento, seleziona e configura l'opzione di pagamento preferita.
4. Scegli Next (Successivo).
5. Scegli gli Host dedicati con cui associare la prenotazione di host dedicati e poi scegli Avanti.
6. (Facoltativo) Assegna tag alla prenotazione di host dedicati.
7. Esamina l'ordine e scegli Acquista.

AWS CLI

Per acquistare le prenotazioni

1. Utilizza il comando describe-host-reservation-offerings per elencare le offerte disponibili che corrispondono alle tue esigenze. Nel seguente esempio sono elencate le offerte che supportano le istanze appartenenti alla famiglia di istanze `m4` e il cui termine è un anno.

   Il termine è specificato in secondi. Un anno pertanto corrisponde a 31.536.000 secondi, mentre tre anni corrispondono a 94.608.000.

   ```
   aws ec2 describe-host-reservation-offerings \
       --filter Name=instance-family,Values=m4 \
       --max-duration 31536000
   ```

   Il comando restituisce l'elenco di offerte corrispondenti ai criteri impostati. Annota l'ID dell'offerta da acquistare.
2. Utilizza il comando purchase-host-reservation per acquistare l'offerta e fornire il valore `offeringId` indicato nel passaggio precedente. L'esempio seguente acquista la prenotazione specificata e la associa a uno specifico host dedicato già assegnato nell' AWS account e applica un tag con una chiave di `purpose` e un valore di. `production`

   ```
   aws ec2 purchase-host-reservation \
       --offering-id hro-03f707bf363b6b324 \
       --host-id-set h-013abcd2a00cbd123 \
   ```

```
    --tag-specifications 'ResourceType=host-
reservation,Tags={Key=purpose,Value=production}'
```

PowerShell

Per acquistare le prenotazioni

1. Utilizza il Get-EC2HostReservationOffering cmdlet per elencare le offerte disponibili che soddisfano le tue esigenze. Negli esempi seguenti sono elencate le offerte che supportano le istanze appartenenti alla famiglia di istanze `m5` e il cui termine è un anno.

   Il termine è specificato in secondi. Un anno pertanto corrisponde a 31.536.000 secondi, mentre tre anni corrispondono a 94.608.000.

   ```
   $filter = @{Name="instance-family"; Values="m5"}
   Get-EC2HostReservationOffering `
       -Filter $filter `
       -MaxDuration 31536000
   ```

   Il comando restituisce l'elenco di offerte corrispondenti ai criteri impostati. Annota l'ID dell'offerta da acquistare.
2. Utilizza il New-EC2HostReservation cmdlet per acquistare l'offerta e fornire l'ID dell'offerta indicato nel passaggio precedente. L'esempio seguente acquista la prenotazione specificata e la associa a uno specifico host dedicato già allocato nell'account. AWS

   ```
   New-EC2HostReservation `
       -OfferingId hro-03f707bf363b6b324 `
       -HostIdSet h-013abcd2a00cbd123
   ```

Cross-account Condivisione di host dedicati Amazon EC2

La condivisione di host dedicati consente ai proprietari di host dedicati di condividere i propri host dedicati con altri AWS account o all'interno di un' AWS organizzazione. Ciò consente di creare e gestire gli host dedicati centralmente e di condividere l'host dedicato su più AWS account o all'interno della propria AWS organizzazione.

In questo modello, l' AWS account proprietario dell'host dedicato (proprietario) lo condivide con altri AWS account (consumatori). I consumatori possono avviare istanze negli Host dedicati condivisi con

loro così come le avvierebbero negli Host dedicati che allocano nel proprio account. Il proprietario è responsabile della gestione dell'Host dedicato e delle istanze avviate in esso. I proprietari non possono modificare le istanze avviate dai consumatori negli Host dedicati condivisi. I consumatori sono responsabili della gestione delle istanze che avviano negli Host dedicati condivisi con loro. I consumatori non possono visualizzare o modificare le istanze appartenenti ad altri consumatori o al proprietario dell'Host dedicato e non possono modificarle gli Host dedicati condivisi con loro.

Il proprietario di un Host dedicato può condividere un Host dedicato con:

- AWS Account specifici all'interno o all'esterno della sua AWS organizzazione
- Un'unità organizzativa all'interno della sua AWS organizzazione
- La sua intera AWS organizzazione

Indice

- Prerequisiti per la condivisione di Host dedicati
- Limitazioni per la condivisione di Host dedicato
- Servizi correlati
- Condivisione tra zone di disponibilità
- Autorizzazioni di Host dedicato condivisi
- Fatturazione e misurazione
- Limiti di Host dedicato
- Ripristino host e condivisione di Host dedicato
- Condividi un host dedicato Amazon EC2 tra AWS account
- Annullare la condivisione di un host dedicato condiviso con altri AWS account
- Visualizza gli host dedicati Amazon EC2 condivisi nel tuo AWS account

Prerequisiti per la condivisione di Host dedicati

- Per condividere un host dedicato, devi possederlo nel tuo AWS account. Non puoi condividere un Host dedicato che è stato condiviso con te.
- Per condividere un host dedicato con la tua AWS organizzazione o un'unità organizzativa AWS della tua organizzazione, devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta Abilitare la condivisione con AWS Organizations nella Guida per l'utente AWS RAM .

Limitazioni per la condivisione di Host dedicato

Non è possibile condividere Host dedicati che sono stati allocati per i seguenti tipi di istanza: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` e `u-24tb1.metal`.

Servizi correlati

AWS Resource Access Manager

La condivisione di un host dedicato si integra con AWS Resource Access Manager (AWS RAM). AWS RAM è un servizio che ti consente di condividere AWS le tue risorse con qualsiasi AWS account o tramite AWS Organizations. Con AWS RAM, condividi le risorse che possiedi creando una condivisione di risorse. Una condivisione delle risorse specifica le risorse da condividere e gli utenti con cui condividerle. I consumatori possono essere singoli AWS account, unità organizzative o un'intera organizzazione di AWS Organizations.

Per ulteriori informazioni AWS RAM, consulta la Guida AWS RAM per l'utente .

Condivisione tra zone di disponibilità

Per garantire che le risorse siano distribuite nelle zone di disponibilità di una regione, le zone di disponibilità sono mappate in modo indipendente ai nomi di ciascun account. Questo potrebbe comportare una diversa denominazione delle zone di disponibilità tra i diversi account. Ad esempio, la zona `us-east-1a` di disponibilità del tuo AWS account potrebbe non avere la stessa posizione `us-east-1a` di un altro AWS account.

Per individuare la posizione dell'Host dedicati relativamente ai tuoi account, devi utilizzare l'ID della zona di disponibilità. L'ID della zona di disponibilità è un identificatore univoco e coerente per una zona di disponibilità in tutti gli AWS account. Ad esempio, `use1-az1` è un ID di zona di disponibilità per la regione `us-east-1` e identifica la stessa posizione in ogni account AWS .

Per visualizzare gli ID delle zone di disponibilità nel tuo account

1. Apri la AWS RAM console all'indirizzo. https://console.aws.amazon.com/ram/home
2. Gli ID delle zone di disponibilità per la regione corrente sono visualizzati nel pannello Your AZ ID (Il tuo ID zona di disponibilità) sul lato destro dello schermo.

Autorizzazioni di Host dedicato condivisi

Autorizzazioni per i proprietari

I proprietari sono responsabili della gestione dei propri Host dedicati condivisi e delle istanze che avviano su di essi. I proprietari possono vedere tutte le istanze in esecuzione sull'Host dedicato condiviso, incluse quelle avviate dai consumatori. Non possono però eseguire alcuna operazione sulle istanze in esecuzione che sono state avviate dai consumatori.

Autorizzazioni per i consumatori

I consumatori sono responsabili della gestione delle istanze che avviano su un Host dedicato condiviso con loro. Non possono modificare l'Host dedicato condiviso in nessun modo e non possono visualizzare o modificare le istanze appartenenti ad altri consumatori o al proprietario dell'Host dedicato.

Fatturazione e misurazione

Non sono previsti costi aggiuntivi per la condivisione di Host dedicati.

Ai proprietari vengono addebitati gli Host dedicati che condividono. Ai consumatori non viene addebitato alcun costo per le istanze che avviano sugli Host dedicati condivisi.

Le Prenotazioni di host dedicati continuano a fornire sconti di fatturazione per gli Host dedicati condivisi. Solo i proprietari di Host dedicato possono acquistare Prenotazioni di host dedicati per gli Host dedicati condivisi che possiedono.

Limiti di Host dedicato

Gli Host dedicati condivisi vengono conteggiati solo ai fini dei limiti di Host dedicati del proprietario. I limiti di Host dedicati dei consumatori non sono influenzati dagli Host dedicati che sono stati condivisi con loro. Allo stesso modo, le istanze che i consumatori avviano sugli Host dedicati condivisi non vengono conteggiate ai fini dei loro limiti di istanze.

Ripristino host e condivisione di Host dedicato

Il ripristino host recupera le istanze avviate dal proprietario dell'Host dedicato e dai consumatori con cui è stato condiviso. L'Host dedicato sostitutivo viene allocato all'account del proprietario. Viene aggiunto alle stesse condivisioni di risorse dell'Host dedicato originale e viene condiviso con gli stessi consumatori.

Per ulteriori informazioni, consulta Ripristino host dedicato di Amazon EC2.

Condividi un host dedicato Amazon EC2 tra AWS account

Quando un proprietario condivide un Host dedicato, consente ai consumatori di avviare istanze sull'host. I consumatori possono avviare sull'host condiviso il numero di istanze consentito dalla capacità disponibile.

> **Important**
>
> L'utente deve assicurarsi di disporre dei diritti di licenza appropriati per condividere qualsiasi licenza BYOL sugli Host dedicati.

Se condividi un Host dedicato con il posizionamento automatico abilitato, tieni presente quanto segue perché potrebbe portare a un utilizzo indesiderato di Host dedicato:

- Se i consumatori avviano istanze con tenancy Host dedicato e non hanno capacità su un Host dedicato che possiedono nel loro account, l'istanza viene avviata automaticamente sull'Host dedicato condiviso.

Per condividere un Host dedicato, devi aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una AWS RAM risorsa che ti consente di condividere le tue risorse tra più AWS account. Un condivisione di risorse specifica le risorse da condividere e i consumatori con cui sono condivise. Puoi aggiungere l'Host dedicato a una risorsa esistente oppure a una nuova condivisione di risorse.

Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno della tua organizzazione è abilitata, ai consumatori dell'organizzazione viene automaticamente concesso l'accesso all'host dedicato condiviso. In caso contrario, i consumatori ricevono l'invito a partecipare alla condivisione di risorse e, dopo averlo accettato, ottengono l'accesso all'Host dedicato condiviso.

> **Note**
>
> Dopo la condivisione di un Host dedicato, possono essere necessari alcuni minuti perché i consumatori possano accedervi.

Console

Per condividere un Host dedicato di cui sei proprietario tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Scegliere Host dedicato per condividere e scegliere Azioni, Condividi prenotazione.
4. Selezionare la condivisione di risorse a cui aggiungere Host dedicato e scegliere Condividi host.

   Prima dell'accesso all'host condiviso possono essere necessari alcuni minuti.

Per condividere un host dedicato di tua proprietà utilizzando AWS RAM console

Consulta Create a resource share nella Guida per l'utente di AWS RAM .

AWS CLI

Per condividere un Host dedicato di cui sei proprietario

Utilizza il comando create-resource-share.

```
aws ram create-resource-share \
    --name my-resource-share \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:dedicated-
host/h-07879acf49EXAMPLE
```

PowerShell

Per condividere un Host dedicato di cui sei proprietario

Utilizza il cmdlet New-RAMResourceShare.

```
New-RAMResourceShare `
    -Name my-resource-share `
    -ResourceArn arn:aws:ec2:us-east-2:123456789012:dedicated-
host/h-07879acf49EXAMPLE
```

Annullare la condivisione di un host dedicato condiviso con altri AWS account

Il proprietario dell'Host dedicato può annullare la condivisione di un Host dedicato condiviso in qualsiasi momento. Quando annulli la condivisione di un Host dedicato condiviso, si applicano le regole seguenti:

- I consumatori con cui l'Host dedicato è stato condiviso non possono più avviare nuove istanze su di esso.
- Le istanze di proprietà dei consumatori che erano in esecuzione sull'Host dedicato al momento dell'annullamento della condivisione continuano a essere eseguite ma sono destinate al ritiro. I consumatori ricevono notifiche di ritiro per le istanze e hanno due settimane di tempo per intervenire. Se però l'Host dedicato viene condiviso nuovamente con il consumatore entro il termine di preavviso del ritiro, i ritiri delle istanze vengono annullati.

Per annullare la condivisione di un Host dedicato condiviso di cui sei proprietario, devi rimuoverlo dalla condivisione di risorse.

Console

Per annullare la condivisione di un Host dedicato condiviso di cui sei proprietario

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Scegliere la Host dedicato per la quale annullare la condivisione e scegliere la scheda Condivisione.
4. La scheda Condivisione elenca le condivisioni di risorse a cui Host dedicato è stato aggiunto. Selezionare la condivisione di risorse da cui eliminare Host dedicato e selezionare Elimina dalla condivisione di risorse.

Per annullare la condivisione di un host dedicato condiviso di tua proprietà utilizzando AWS RAM console

Consulta Update a resource share nella Guida per l'utente di AWS RAM .

AWS CLI

Per annullare la condivisione di un Host dedicato condiviso di cui sei proprietario

Utilizza il comando disassociate-resource-share.

```
aws ram disassociate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
 --resource-arns arn:aws:ec2:us-east-2:123456789012:dedicated-host/h-07879acf49EXAMPLE
```

PowerShell

Per annullare la condivisione di un Host dedicato condiviso di cui sei proprietario

Utilizza il cmdlet Disconnect-RAMResourceShare.

```
Disconnect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:dedicated-host/h-07879acf49EXAMPLE"
```

Visualizza gli host dedicati Amazon EC2 condivisi nel tuo AWS account

Puoi visualizzare l'host dedicato che stai condividendo con altri account e gli host dedicati che sono condivisi con te. Se non possiedi l'host dedicato, puoi vedere tutte le istanze in esecuzione sull'host, comprese le istanze avviate dai consumatori. Se l'host dedicato è condiviso con te, puoi vedere solo le istanze che hai avviato sull'host condiviso e non quelle lanciate da altri consumatori.

Proprietari e consumatori possono identificare Host dedicati condivise utilizzando uno dei seguenti metodi.

Console

Per identificare un Host dedicato condiviso

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati). La schermata elenca gli Host dedicati di cui sei proprietario e gli Host dedicati che sono condivisi con te.
3. Nella colonna Owner (Proprietario) è indicato l'ID dell'account AWS del proprietario dell'Host dedicato.
4. Per visualizzare le istanze in esecuzione sugli host, seleziona la scheda Istanze.

AWS CLI

Per identificare un Host dedicato condiviso

Usa il comando describe-hosts. Il comando restituisce gli Host dedicati di cui sei proprietario e gli Host dedicati che sono condivisi con te. Il valore di `Owner` è l'ID dell'account del proprietario dell'Host dedicato. L'elenco `Instances` descrive le istanze in esecuzione sull'host.

```
aws ec2 describe-hosts --filter "Name=state,Values=available"
```

PowerShell

Per identificare un Host dedicato condiviso

Utilizza il cmdlet Get-EC2host. Il cmdlet restituisce gli Host dedicati di cui sei proprietario e gli Host dedicati che sono condivisi con te. Il valore di `Owner` nella risposta è l'ID dell'account del proprietario dell'Host dedicato. L'elenco `Instances` descrive le istanze in esecuzione sull'host.

```
Get-EC2Host -Filter @{Name="state"; Values="available"}
```

Host dedicati Amazon EC2 su AWS Outposts

AWS Outposts è un servizio completamente gestito che estende AWS l'infrastruttura, i servizi, le API e gli strumenti alla tua sede. Fornendo l'accesso locale all'infrastruttura AWS gestita, AWS Outposts consente di creare ed eseguire applicazioni in locale utilizzando le stesse interfacce di programmazione AWS delle regioni, utilizzando al contempo risorse di elaborazione e archiviazione locali per esigenze di latenza inferiore e di elaborazione locale dei dati.

Un Outpost è un pool di capacità di AWS elaborazione e archiviazione distribuito presso la sede del cliente. AWS opera, monitora e gestisce questa capacità come parte di una regione. AWS

Puoi allocare host dedicati sugli outpost che hai nel tuo account. In questo modo è più facile portare le licenze software e i carichi di lavoro esistenti che richiedono un server fisico dedicato su AWS Outposts. Puoi anche indirizzare risorse hardware specifiche su un Outpost per ridurre al minimo la latenza tra i tuoi carichi di lavoro.

Gli host dedicati consentono di utilizzare le licenze software idonee su Amazon EC2, in modo da ottenere la flessibilità e l'efficacia in termini di costi dell'utilizzo delle proprie licenze. Anche altre

licenze software associate a macchine virtuali, socket o core fisici possono essere utilizzate su host dedicati, in base alle condizioni di licenza. Sebbene gli outpost siano sempre stati ambienti single-tenant idonei per i carichi di lavoro BYOL, gli host dedicati consentono di limitare le licenze necessarie a un singolo host anziché all'intera implementazione degli outpost.

Inoltre, l'utilizzo di host dedicati su un outpost offre una maggiore flessibilità nella distribuzione del tipo di istanza e un controllo più granulare sul posizionamento delle istanze. Si può puntare a un host specifico per il lancio di un'istanza e usare l'affinità di host per garantire che l'istanza venga sempre eseguita su quell'host, oppure si può usare il posizionamento automatico per lanciare un'istanza su qualsiasi host disponibile che abbia configurazioni corrispondenti e capacità disponibile.

Indice

- Prerequisiti
- Funzionalità supportate
- Considerazioni
- Assegna un host dedicato Amazon EC2 su AWS Outposts

Prerequisiti

Devi avere un Outpost installato nel tuo sito. Per ulteriori informazioni, consulta Creazione di un Outpost e ordinazione della capacità Outpost nella Guida per l'utente di AWS Outposts .

Funzionalità supportate

- Sono supportate le seguenti famiglie di istanze:
  - Uso generico: M5 | M5d | M7i | M8i
  - Ottimizzato per il calcolo: C5 | C5d | C7i | C8i
  - Memoria ottimizzata: R5 | R5d | R7i | R8i
  - Archiviazione ottimizzata: I3en
  - Calcolo accelerato: G4dn
- Gli host dedicati sugli outpost possono essere configurati per supportare più dimensioni di istanza. Il supporto per più dimensioni di istanza è disponibile per le seguenti famiglie di istanze.
  - Uso generale: M5 | M5d | M7i
  - Ottimizzato per il calcolo: C5 | C5d | C7i
  - Memoria ottimizzata: R5 | R5d | R7i

Per ulteriori informazioni, consulta Configurazioni di capacità di istanza per host dedicati di Amazon EC2.

- Gli host dedicati sugli outpost supportano il posizionamento automatico e il lancio di istanze mirate. Per ulteriori informazioni, consulta Auto-posizionamento dell'host dedicato Amazon EC2 e affinità degli host.
- Gli host dedicati sugli outpost supportano l'affinità degli host. Per ulteriori informazioni, consulta Auto-posizionamento dell'host dedicato Amazon EC2 e affinità degli host.
- Gli host dedicati su Outposts supportano la condivisione con. AWS RAM Per ulteriori informazioni, consulta Cross-account Condivisione di host dedicati Amazon EC2.

Considerazioni

- Le prenotazioni di host dedicati non sono supportate sugli outpost.
- Ospita gruppi di risorse e non AWS License Manager sono supportati su Outposts.
- Gli host dedicati sugli outpost non supportano istanze T3 espandibili.
- Gli host dedicati sugli outpost non supportano il ripristino dell'host.
- Il ripristino automatico semplificato non è supportato per istanze con tenancy di host dedicati su Outposts.

Assegna un host dedicato Amazon EC2 su AWS Outposts

Puoi allocare e utilizzare gli host dedicati sugli outpost nello stesso modo in cui faresti con gli host dedicati in una regione AWS .

Prerequisiti

Creare una sottorete nell'Outpost. Per ulteriori informazioni, consulta Creazione di una sottorete nella Guida per l'utente di AWS Outposts .

Per allocare un host dedicato su un Outpost, utilizza uno dei metodi descritti di seguito:

Console

Per allocare un host dedicato su un avamposto utilizzando il AWS Outposts console

1. Apri la AWS Outposts console all'indirizzo. https://console.aws.amazon.com/outposts/

2. Nel riquadro di navigazione, scegli Outpost. Seleziona l'outpost e scegli Actions (Operazioni), Allocate Dedicated Host (Alloca host dedicato).
3. Configura l'host dedicato secondo necessità. Per ulteriori informazioni, consulta Alloca un host dedicato di Amazon EC2 per l'uso nel tuo account.

> **Note**
>
> I campi Availability Zone (Zona di disponibilità) e Outpost ARN (ARN dell'Outpost) dovrebbero essere precompilati con la zona di disponibilità e l'ARN dell'Outpost selezionato.

4. Scegli Alloca.

Per allocare un Host dedicato su un outpost usando la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Dedicated Hosts (Host dedicati), quindi Allocate Dedicated Host (Alloca host dedicato).
3. In Availability Zone (Zona di disponibilità), seleziona la zona di disponibilità associata all'Outpost.
4. In Outpost ARN (ARN dell'Outpost), inserisci l'ARN dell'Outpost.
5. Per scegliere come target risorse hardware specifiche sull'Outpost, per Scegli risorse hardware specifiche sull'Outpost seleziona Abilita. Per ogni risorsa hardware da utilizzare come target, scegli Aggiungi ID risorsa, quindi inserisci l'ID della risorsa hardware.

> **Note**
>
> Il valore specificato per Quantità deve essere uguale al numero di ID degli asset specificati. Ad esempio, se specifichi 3 ID di asset, anche Quantità deve essere 3.

6. Configura le impostazioni rimanenti dell'host dedicato secondo necessità. Per ulteriori informazioni, consulta Alloca un host dedicato di Amazon EC2 per l'uso nel tuo account.
7. Scegli Alloca.

AWS CLI

Per allocare un Host dedicato su un outpost

Utilizza il comando allocate-hosts. In `--availability-zone`, specifica la zona di disponibilità associata all'Outpost. In `--outpost-arn`, specifica l'ARN dell'Outpost. Facoltativamente, per `--asset-ids`, specifica gli ID delle risorse hardware dell'Outpost da scegliere come target.

```
aws ec2 allocate-hosts \
    --availability-zone "us-east-1a" \
    --outpost-arn "arn:aws:outposts:us-east-1a:111122223333:outpost/
op-4fe3dc21baEXAMPLE" \
    --asset-ids asset_id \
    --instance-family "m5" \
    --auto-placement "off" \
    --quantity 1
```

PowerShell

Per allocare un Host dedicato su un outpost

Utilizza il cmdlet New-EC2Host. Specifica la zona di disponibilità associata all'Outpost. Facoltativamente, per `-AssetId`, specifica gli ID delle risorse hardware dell'Outpost da scegliere come target.

```
New-EC2Host `
    -AvailabilityZone "us-east-1a" `
    -OutpostArn "arn:aws:outposts:us-east-1a:111122223333:outpost/
op-4fe3dc21baEXAMPLE" `
    -AssetId asset_id `
    -InstanceFamily "m5" `
    -AutoPlacement "off" `
    -Quantity 1
```

Per avviare un'istanza su un host dedicato su un Outpost

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati). Seleziona l'host dedicato che hai allocato nel passaggio precedente e scegli Actions (Operazioni), Launch instance onto host (Avvia l'istanza sull'host).

3. Configura l'istanza secondo necessità e quindi avvia l'istanza. Per ulteriori informazioni, consulta Avvia le istanze Amazon EC2 su un host dedicato Amazon EC2.

Ripristino host dedicato di Amazon EC2

Il ripristino automatico dell'host dedicato riavvia le istanze su un nuovo host sostitutivo, se sull'host dedicato vengono rilevate delle condizioni problematiche. Il ripristino host riduce la necessità di intervento manuale e il carico operativo in caso di errore imprevisto dell'host dedicato relativamente a eventi di sistema o connettività di rete. Altri problemi relativi all'host dedicato richiederanno un intervento manuale da cui eseguire il ripristino.

Indice

- Come funziona il ripristino host dedicato di Amazon EC2
- Tipi di istanze supportati
- Prezzi
- Gestisci ripristino dell'host dedicato di Amazon EC2
- Visualizza l'impostazione di ripristino dell'host per il tuo host dedicato di Amazon EC2
- Ripristina manualmente le istanze non supportate dal ripristino di host dedicati di Amazon EC2

Come funziona il ripristino host dedicato di Amazon EC2

Gli host dedicati e il processo di recupero dei gruppi di risorse host utilizzano i controlli dell'integrità a livello di host per valutare la disponibilità degli host dedicati e per rilevare errori di sistema sottostanti. Il tipo di errore dell'host dedicato determina se è possibile il ripristino automatico dell'host dedicato. Esempi di problemi che causano il mancato superamento dei controlli dello stato di integrità a livello di host includono:

- Perdita di connettività di rete
- Perdita di alimentazione elettrica del sistema
- Problemi hardware e software sull'host fisico

> **Important**
>
> Il ripristino automatico dell'host dedicato non si verifica quando l'host è programmato per il ritiro.

Ripristino automatico dell'host dedicato

Quando sull'host dedicato viene rilevato un errore di sistema o di connettività di rete, viene avviato il ripristino automatico dell'host dedicato e Amazon EC2 alloca automaticamente un host dedicato sostitutivo nella stessa zona di disponibilità dell'host dedicato originale. L'Host dedicato sostitutivo riceve un nuovo ID host ma mantiene gli stessi attributi dell'Host dedicato originale, inclusi:

- Zona di disponibilità
- Tipo di istanza
- Tag
- Impostazioni di posizionamento automatico
- Prenotazione

Una volta allocato l'host dedicato sostitutivo, su tale host vengono ripristinate le istanze. Le istanze ripristinate mantengono gli stessi attributi delle istanze originali, inclusi:

- ID istanza
- Indirizzi IP privati
- Indirizzi IP elastici
- Allegati dei volumi EBS
- Tutti i metadati delle istanze

Inoltre, l'integrazione integrata con AWS License Manager automatizza il monitoraggio e la gestione delle licenze.

> **Note**
>
> AWS L'integrazione di License Manager è supportata solo nelle regioni in cui AWS License Manager è disponibile.

Se le istanze hanno una relazione di affinità host con l'Host dedicato danneggiato, le istanze ripristinate stabiliscono un'affinità host con l'Host dedicato sostitutivo.

Una volta che tutte le istanze sono state ripristinate sull'Host dedicato sostitutivo, l'Host dedicato danneggiato viene rilasciato e l'Host dedicato sostitutivo diventa disponibile per l'utilizzo.

Quando viene avviato il ripristino dell'host, il proprietario dell' AWS account viene avvisato tramite e-mail e tramite un Dashboard AWS Health evento. Al completamento del ripristino viene dell'host inviata una seconda notifica.

Se si utilizza AWS License Manager per tenere traccia delle licenze, AWS License Manager assegna nuove licenze per l'host dedicato sostitutivo in base ai limiti di configurazione delle licenze. Se la configurazione della licenza presenta limiti rigidi che verranno violati a seguito del ripristino dell'host, il processo di ripristino non è consentito e all'utente viene notificato l'errore di ripristino dell'host tramite una notifica Amazon SNS (se le impostazioni di notifica sono state configurate per License Manager). AWS Se la configurazione delle licenze presenta limiti software che verranno superati come conseguenza del ripristino host, il ripristino viene consentito e ricevi una notifica Amazon SNS relativa al superamento del limite. Per ulteriori informazioni, consulta Utilizzo delle configurazioni di licenza e Impostazioni in License Manager nella Guida per l'utente di AWS License Manager.

Stati del ripristino host

Quando viene rilevato un errore dell'Host dedicato, sull'Host dedicato danneggiato viene attivato lo stato `under-assessment` e su tutte le istanze viene attivato lo stato `impaired`. Non è possibile avviare istanze sull'Host dedicato danneggiato mentre si trova nello stato `under-assessment`.

Una volta allocato, sull'Host dedicato sostitutivo viene attivato lo stato `pending`. L'host rimane in questo stato fino al completamento del processo di ripristino host. Non è possibile avviare istanze sull'Host dedicato sostitutivo mentre si trova nello stato `pending`. Le istanze ripristinate sull'Host dedicato sostitutivo rimangono nello stato `impaired` durante il processo di ripristino.

Una volta completato il ripristino host, sull'Host dedicato sostitutivo viene attivato lo stato `available`le istanze ripristinate tornato allo stato `running`. È possibile avviare istanze sull'Host dedicato sostitutivo dopo che è stato attivato lo stato `available`. L'Host dedicato danneggiato originale viene rilasciato definitivamente e viene attivato lo stato `released-permanent-failure`.

Se l'Host dedicato compromesso presenta istanze che non supportano il ripristino host, ad esempio le istanze con volumi root di archivio dell'istanza, l'Host dedicato non viene rilasciato. Viene invece contrassegnato per il ritiro e viene attivato lo stato `permanent-failure`.

Scenari senza il ripristino automatico dell'host dedicato

Il ripristino automatico dell'host dedicato non si verifica quando l'host è programmato per il ritiro. Riceverai una notifica di ritiro nel corso di un CloudWatch evento Amazon e l' Dashboard AWS Health indirizzo email del proprietario dell' AWS account riceverà un messaggio relativo all'errore dell'host

dedicato. Segui le procedure di correzione descritte nella notifica di ritiro entro il periodo di tempo specificato per ripristinare manualmente le istanze sull'host che desideri ritirare.

Le istanze arrestate non vengono ripristinate sull'Host dedicato sostitutivo. Se si prova ad avviare un'istanza arrestata destinata all'Host dedicato danneggiato, l'avvio non riesce. Consigliamo di modificare l'istanza arrestata specificando un Host dedicato di destinazione diverso oppure di avviarla su un Host dedicato disponibile con configurazioni corrispondenti abilitato per il posizionamento automatico.

Le istanze con archiviazione dell'istanza non vengono ripristinate sull'Host dedicato sostitutivo. Come misura di correzione, l'Host dedicato danneggiato viene contrassegnato per il ritiro e riceverai una notifica di ritiro una volta completato il ripristino host. Segui le procedure di correzione descritte nella notifica di ritiro entro il periodo di tempo specificato per ripristinare manualmente le istanze rimanenti sull'Host dedicato danneggiato.

Tipi di istanze supportati

Il ripristino dell'host è supportato per le seguenti famiglie di istanze:

- Uso generale: A1 | M3 | M4 | M5 | M5n | M5zn | M6a | M6g | M6i | T3 | Mac1 | Mac2 | | | | M6in | M7a | M7g | M7i | | | | Mac2-m1ultra Mac2-m2 Mac2-m2pro Mac-m4 Mac-m4pro Mac-m4max Mac-m3ultra
- Ottimizzato per il calcolo: C3 | C4 | C5 | C5n | C6a | C6g | C6i | C6gn | C6in | C7g | C7gn | C7i
- Memoria ottimizzata: R3 | R4 | R5 | R5b | R5n | R6g | R6i | U-6tb1 | U-9tb1 | U-12tb1 | U-18tb1 | U-24tb1 | X1 | X1e | X2iezn | R6a | R6in | R7g | R7i | R7iZ
- Calcolo accelerato: Inf1 | G3 | G5g | P3

Per ripristinare le istanze non supportate, consulta Ripristina manualmente le istanze non supportate dal ripristino di host dedicati di Amazon EC2.

> **Note**
>
> Il ripristino automatico dell'host dedicato dei tipi di istanza metal supportati richiederà più tempo per rilevare e ripristinare i tipi di istanze non metal.

Prezzi

L'uso del ripristino host non prevede costi aggiuntivi, solo i normali costi dell'Host dedicato. Per maggiori informazioni, consulta Prezzi degli host dedicati di Amazon EC2.

Appena viene avviato il ripristino host, non riceverai più l'addebito per l'Host dedicato danneggiato. La fatturazione per l'host dedicato sostitutivo inizia solo dopo che viene attivato lo stato `available`.

Se l'Host dedicato con disabilità è stato fatturato utilizzando la On-Demand tariffa, anche l'Host dedicato sostitutivo viene fatturato utilizzando la tariffa. On-Demand Se l'Host dedicato danneggiato presenta un Prenotazioni di host dedicati attivo, questo viene trasferito nell'Host dedicato sostitutivo.

Gestisci ripristino dell'host dedicato di Amazon EC2

Il ripristino automatico dell'host dedicato riavvia le istanze su un nuovo host sostitutivo, se sull'host dedicato vengono rilevate delle condizioni problematiche. Puoi abilitare il ripristino dell'host quando allochi l'Host dedicato oppure dopo l'allocazione.

Utilizza le seguenti procedure per abilitare il ripristino dell'host durante l'allocazione dell'host.

Console

Per abilitare il ripristino dell'host all'allocazione

Quando si alloca un host dedicato utilizzando la console Amazon EC2, per Ripristino host, scegli Abilita. Per ulteriori informazioni, consulta Alloca un host dedicato di Amazon EC2 per l'uso nel tuo account.

AWS CLI

Per abilitare il ripristino dell'host all'allocazione

Utilizza il comando allocate-hosts.

```
aws ec2 allocate-hosts \
    --instance-type m5.large \
    --availability-zone eu-west-1a \
    --auto-placement on \
    --host-recovery on \
    --quantity 1
```

PowerShell

Per abilitare il ripristino dell'host all'allocazione

Utilizza il cmdlet New-EC2Host.

```
New-EC2Host `
    -InstanceType m5.large `
    -AvailabilityZone eu-west-1a `
    -AutoPlacement on `
    -HostRecovery on `
    -Quantity 1
```

Utilizza le seguenti procedure per gestire il ripristino dell'host per un host dedicato.

Console

Per gestire il ripristino dell'host dopo l'allocazione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Seleziona l'host dedicato.
4. Scegli Operazioni, Modifica host.
5. Per Ripristino host, seleziona o deseleziona Abilita.
6. Scegli Save (Salva).

AWS CLI

Per abilitare il ripristino dell'host dopo l'allocazione

Utilizza il comando modify-hosts.

```
aws ec2 modify-hosts \
    --host-recovery on \
    --host-ids h-012a3456b7890cdef
```

Per disabilitare il ripristino dell'host dopo l'allocazione

Utilizza il comando modify-hosts e specifica il parametro `host-recovery` con un valore di `off`.

```
aws ec2 modify-hosts \
```

```
    --host-recovery off \
    --host-ids h-012a3456b7890cdef
```

PowerShell

Per abilitare il ripristino dell'host dopo l'allocazione

Utilizza il cmdlet Edit-host.

```
Edit-EC2Host `
    -HostRecovery on `
    -HostId h-012a3456b7890cdef
```

Per disabilitare il ripristino dell'host dopo l'allocazione

Utilizza il cmdlet Edit-EC2Host.

```
Edit-EC2Host `
    -HostRecovery off `
    -HostId h-012a3456b7890cdef
```

Visualizza l'impostazione di ripristino dell'host per il tuo host dedicato di Amazon EC2

È possibile visualizzare la configurazione del ripristino host per un Host dedicato in qualsiasi momento.

Console

Per visualizzare la configurazione del ripristino host per un Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Selezionare l'Host dedicato, quindi nella scheda Descrizione rivedere il campo Host Recovery (Ripristino host).

AWS CLI

Per visualizzare la configurazione del ripristino host per un Host dedicato

Usa il comando describe-hosts.

```
aws ec2 describe-hosts \
    --host-ids h-012a3456b7890cdef \
    --query Hosts[].HostRecovery
```

Di seguito è riportato un output di esempio.

```
on
```

PowerShell

Per visualizzare la configurazione del ripristino host per un Host dedicato

Utilizza il cmdlet Get-EC2Host.

```
(Get-EC2Host -HostId h-012a3456b7890cdef).Hosts | Select HostRecovery
```

Di seguito è riportato un output di esempio.

```
HostRecovery
------------
on
```

Ripristina manualmente le istanze non supportate dal ripristino di host dedicati di Amazon EC2

Il ripristino host non supporta il ripristino delle istanze che utilizzano volumi di instance store. Segui le istruzioni riportate di seguito per ripristinare manualmente le istanze che potrebbero non essere ripristinate automaticamente.

> **Warning**
>
> Quando un'istanza viene arrestata, ibernata o terminata, i dati nei volumi di archivio dell'istanza vengono persi. Ciò include i volumi dell'archivio dell'istanza collegati a un'istanza che ha un volume root EBS. Per proteggere i dati dei volumi di archivio dell'istanza, è opportuno creare una copia di backup nell'archiviazione persistente prima che l'istanza venga arrestata o terminata.

Recupera manualmente le istanze EBS-backed

Per EBS-backed le istanze che non possono essere ripristinate automaticamente, ti consigliamo di arrestare e avviare manualmente le istanze per ripristinarle su un nuovo host dedicato. Per ulteriori informazioni sull'arresto dell'istanza e sulle modifiche alla configurazione dell'istanza quando viene arrestata, consulta Avvio e arresto di un'istanza Amazon EC2.

Recupera manualmente le istanze con volumi root di archivio dell'istanza

Per le istanze con volumi root di archivio dell'istanza che potrebbero non essere ripristinate automaticamente, consigliamo di effettuare quanto segue:

1. Avviare un'istanza sostitutiva su un nuovo Host dedicato dall'AMI più recente.
2. Migrare tutti i dati necessari nell'istanza sostituiva.
3. Terminare l'istanza originale nell'Host dedicato danneggiato.

Manutenzione degli host per host dedicati di Amazon EC2

Con la manutenzione dell'host, nel raro caso in cui un host dedicato si danneggi, Amazon EC2 migra automaticamente le istanze in esecuzione su di esso su un host dedicato sostitutivo funzionante. Questo aiuta a ridurre al minimo il tempo di inattività del carico di lavoro e a semplificare la gestione degli host dedicati. La manutenzione degli host viene eseguita anche per la manutenzione pianificata e ordinaria di Amazon EC2.

Amazon EC2 supporta due tipi di manutenzione degli host:

- Manutenzione degli host con migrazione live: le istanze vengono migrate automaticamente all'host sostitutivo entro 24 ore, senza arrestarle e riavviarle.
- Reboot-based manutenzione dell'host: le istanze sono programmate, ad esempio eventi programmati di riavvio, durante i quali vengono automaticamente arrestate e riavviate sull'host sostitutivo.

Indice

- Confronto tra manutenzione degli host e ripristino degli host
- Considerazioni
- Servizi correlati

- Prezzi
- Come funziona la manutenzione degli host per host dedicati di Amazon EC2
- Configura l'impostazione di manutenzione degli host per host dedicati di Amazon EC2

Confronto tra manutenzione degli host e ripristino degli host

Nella tabella seguente vengono illustrate le differenze principali tra il ripristino degli host e la manutenzione degli host.

	Ripristino host	Manutenzione degli host
Raggiungibilità delle istanze	Irraggiungibile	Raggiungibile
Stato degli host dedicati	`under-assessment`	`permanent-failure`
Gruppo di risorse host	Supportata	Non supportata

Per ulteriori informazioni sul ripristino degli host, consulta Ripristino degli host.

Considerazioni

- La manutenzione dell'host è disponibile in tutti Regioni AWS, ad eccezione delle regioni della Cina e. AWS GovCloud (US) Regions
- La manutenzione dell'host non è supportata nelle AWS Outposts zone AWS locali e nelle zone a lunghezza AWS d'onda.
- La manutenzione degli host non può essere attivata o disattivata per gli host già inclusi in un gruppo di risorse host. Gli host aggiunti a un gruppo di risorse host mantengono le impostazioni di manutenzione degli host. Per ulteriori informazioni, consulta Gruppi di risorse host.
- La manutenzione degli host non è supportata con i seguenti tipi di istanza, perché dispongono di volumi root di archivio dell'istanza: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

Servizi correlati

L'host dedicato si integra con AWS License Manager: tiene traccia delle licenze tra gli host dedicati Amazon EC2 (supportato solo nelle regioni in cui AWS è disponibile License Manager). Per ulteriori informazioni, consulta la Guida per l'utente di AWS License Manager.

È necessario disporre di licenze sufficienti Account AWS per il nuovo host dedicato. Le licenze associate all'host degradato vengono rilasciate quando l'host viene rilasciato dopo il completamento dell'evento pianificato.

Prezzi

L'uso della manutenzione degli host non prevede costi aggiuntivi, solo i normali costi dell'host dedicato. Per maggiori informazioni, consulta Prezzi degli host dedicati di Amazon EC2.

Appena viene avviata la manutenzione degli host, non riceverai più l'addebito per l'host dedicato degradato. La fatturazione per l'host dedicato sostitutivo inizia solo dopo che viene attivato lo stato `available`.

Se l'Host dedicato scaduto è stato fatturato utilizzando la On-Demand tariffa, anche l'Host dedicato sostitutivo viene fatturato utilizzando la tariffa. On-Demand Se l'host dedicato degradato presenta una Prenotazione di host dedicati attiva, questo viene trasferito nel nuovo host dedicato.

Come funziona la manutenzione degli host per host dedicati di Amazon EC2

Quando viene rilevata una degradazione su un host dedicato abilitato alla manutenzione dell'host, nel tuo account viene assegnato automaticamente un host dedicato sostitutivo. L'Host dedicato sostitutivo riceve un nuovo ID host ma mantiene gli stessi attributi dell'Host dedicato originale, inclusi:

- Impostazioni di posizionamento automatico
- Zona di disponibilità
- Associazione della prenotazione di host dedicato
- Affinità host
- Impostazioni di manutenzione degli host
- Impostazioni del ripristino degli host
- Tipo di istanza
- Tag

Dopo l'allocazione dell'host sostitutivo, le istanze vengono migrate utilizzando la manutenzione dell'host di migrazione in tempo reale o la manutenzione dell'host basata sul riavvio, a seconda dell'istanza.

Dopo che l'host degradato non ha più istanze in esecuzione, viene rimosso definitivamente dal tuo account.

Manutenzione degli host con migrazione live

Le istanze che richiedono la manutenzione dell'host con migrazione live vengono migrate automaticamente all'host sostitutivo entro 24 ore, senza arrestarle e riavviarle. Le istanze migrate mantengono gli attributi esistenti, fra cui:

- ID istanza
- Metadati delle istanze
- Allegati dei volumi Amazon EBS
- indirizzi IP elastici e indirizzo IP privato
- Memoria, CPU e stati di rete

Alcune istanze di dimensioni maggiori potrebbero subire un leggero calo delle prestazioni durante la migrazione.

Dopo la migrazione automatica delle istanze all'host sostitutivo, riceverai notifiche tramite e-mail e Dashboard. AWS Health Le notifiche includono gli ID degli host degradati e sostitutivi, informazioni sulle istanze che sono state migrate automaticamente utilizzando la manutenzione dell'host di migrazione live e informazioni sulle istanze rimanenti.

Reboot-based manutenzione dell'host

Le istanze che richiedono una manutenzione dell'host basata sul riavvio sono pianificate per eventi programmati di riavvio dell'istanza 14 giorni dalla data della notifica. Puoi continuare ad accedere alle istanze sull'host dedicato degradato prima dell'evento programmato.

Puoi riprogrammare gli eventi di riavvio per una data entro 7 giorni dalla data e l'ora dell'evento originale. Per ulteriori informazioni, consulta Ripianifica un evento pianificato per un'istanza EC2.

Amazon EC2 riserva automaticamente la capacità sull'host sostitutivo per queste istanze. Non puoi eseguire istanze in questa capacità riservata.

La console Amazon EC2 mostra la capacità riservata come capacità utilizzata. Potrebbe sembrare che le istanze siano in esecuzione sia sull'host degradato che sull'host sostitutivo. Tuttavia, le istanze continueranno a funzionare solo sull'host degradato fino all'arresto o alla migrazione nella capacità riservata dell'host sostitutivo.

Alla data e all'ora dell'evento programmato, le istanze vengono automaticamente arrestate e riavviate nella capacità riservata sull'host sostitutivo. Le istanze migrate mantengono gli attributi esistenti, fra cui:

- ID istanza
- Metadati delle istanze
- Allegati dei volumi Amazon EBS
- indirizzi IP elastici e indirizzo IP privato

Tuttavia, poiché le istanze vengono arrestate e riavviate durante la migrazione, non mantengono gli stati della memoria, della CPU e della rete.

Puoi anche arrestare e riavviare manualmente queste istanze in qualsiasi momento prima dell'evento programmato per migrarle sull'host sostitutivo o su un altro host. Potresti dover modificare l'affinità host dell'istanza per riavviarla su un host diverso. Se si arresta un'istanza prima dell'evento programmato, la capacità riservata sull'host sostitutivo viene rilasciata e diventa disponibile per l'uso.

Stati di manutenzione degli host

Quando un host diventa degradato, entra nello stato `permanent-failure`. Non è possibile avviare istanze su un host dedicato che è nello stato `permanent-failure`.

Dopo la sua allocazione, l'host sostitutivo rimane nello stato `pending` finché le istanze che supportano la manutenzione degli host con migrazione live vengono migrate automaticamente dall'host degradato, e finché gli eventi pianificati vengono pianificati per le istanze rimanenti. Una volta completate queste attività, l'host sostitutivo entra nello stato `available`.

Dopo che l'host sostitutivo è entrato nello stato `available`, puoi utilizzarlo nello stesso modo in cui usi qualsiasi host nel tuo account. Tuttavia, parte della capacità dell'istanza sull'host sostitutivo è riservata alle istanze che richiedono una migrazione dell'host basata sul riavvio. Non puoi avviare nuove istanze in questa capacità riservata.

Quando l'host degradato non ha più istanze in esecuzione, entra nello stato `released, permanent-failure`, e viene rilasciato definitivamente dal tuo account. L'host e le relative risorse rimangono visibili nella console per un breve periodo di tempo.

Migrazione automatica

Alcune istanze non possono essere migrate automaticamente all'host sostitutivo.

Istanze con volumi EBS-backed root

In questi casi, gli eventi di arresto delle istanze sono programmati per 28 giorni dalla data della notifica. Alla data e all'ora dell'evento programmato, le istanze vengono arrestate. Consigliamo di arrestare manualmente l'istanza al riavvio dell'istanza sull'host sostitutivo o su un host diverso. Potresti dover modificare l'affinità host dell'istanza per riavviarla su un host diverso.

Istanze con un volume root di archivio dell'istanza

In questi casi, gli eventi di ritiro delle istanze sono programmati per 28 giorni dalla data della notifica. Alla data e all'ora dell'evento programmato, le istanze vengono interrotte definitivamente. Consigliamo di avviare manualmente le istanze sostitutive sull'host sostitutivo e quindi di effettuare la migrazione dei dati richiesti sulle istanze sostitutive prima dell'evento programmato.

Le seguenti istanze dispongono di volumi root di archivio dell'istanza: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

Puoi continuare ad accedere alle istanze sull'host dedicato degradato prima dell'evento programmato.

Configura l'impostazione di manutenzione degli host per host dedicati di Amazon EC2

Abilita la manutenzione degli host per garantire che le istanze in esecuzione su un Host dedicato vengano ripristinate automaticamente su un nuovo host dedicato durante un evento di manutenzione programmato.

Se disabiliti la manutenzione dell'host, ricevi una notifica e-mail per espellere l'host danneggiato e migrare manualmente le istanze su un altro host entro 28 giorni. Se hai prenotato un host dedicato, viene assegnato un host sostitutivo. Dopo 28 giorni, le istanze in esecuzione sull'host danneggiato vengono terminate e l'host viene rilasciato automaticamente.

Console

Per abilitare la manutenzione dell'host utilizzato dall'Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Seleziona l'host dedicato > Operazioni > Modifica host.
4. Seleziona attiva nel campo Manutenzione dell'host.

Per disabilitare la manutenzione dell'host utilizzato dall'Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Seleziona l'host dedicato > Operazioni > Modifica host.
4. Seleziona disattiva nel campo Manutenzione dell'host.

AWS CLI

Per abilitare la manutenzione dell'host utilizzato dall'Host dedicato

Utilizza il comando modify-hosts.

```
aws ec2 modify-hosts \
    --host-maintenance on \
    --host-ids h-0d123456bbf78910d
```

Per disabilitare la manutenzione dell'host utilizzato dall'Host dedicato

Utilizza il comando modify-hosts.

```
aws ec2 modify-hosts \
    --host-maintenance off \
    --host-ids h-0d123456bbf78910d
```

PowerShell

Per abilitare la manutenzione dell'host utilizzato dall'Host dedicato

Utilizza il cmdlet Edit-EC2Host.

```
Edit-EC2Host `
    -HostMaintenance on `
    -HostId h-0d123456bbf78910d
```

Per disabilitare la manutenzione dell'host utilizzato dall'Host dedicato

Utilizza il cmdlet Edit-EC2Host.

```
Edit-EC2Host `
    -HostMaintenance off `
    -HostId h-0d123456bbf78910d
```

Monitora lo stato degli host dedicati di Amazon EC2

Amazon EC2 monitora costantemente lo stato degli Host dedicati. Gli aggiornamenti vengono comunicati sulla console Amazon EC2. È possibile visualizzare le informazioni su un Host dedicato utilizzando i seguenti metodi.

Console

Per visualizzare lo stato di un Host dedicato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Host dedicati (Host dedicati).
3. Individuare l'Host dedicato nell'elenco e controllare il relativo valore nella colonna State (Stato).

AWS CLI

Per visualizzare lo stato di un Host dedicato

Usa il comando describe-hosts.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

PowerShell

Per visualizzare lo stato di un Host dedicato

Utilizza il cmdlet Get-EC2Host.

```
Get-EC2Host -HostId h-012a3456b7890cdef
```

Nella seguente tabella sono descritti i possibili stati di un Host dedicato.

Stato	Descrizione
`available`	AWS non ha rilevato alcun problema con l'host dedicato. Non è stata pianificata alcuna manutenzione né correzione. Le istanze possono essere avviate su questo host dedicato.
`released`	L'Host dedicato è stato rilasciato. L'ID host non è più in uso. Gli host rilasciati non possono essere riutilizzati.
`under-assessment`	AWS sta esaminando un possibile problema con l'host dedicato. Se è necessario intraprendere un'azione, riceverai una notifica Console di gestione AWS tramite e-mail. Le istanze non possono essere avviate su occorrenze degli Host dedicato in questo stato.
`pending`	L'Host dedicato non può essere utilizzato per nuovi avvii di istanze. A questo scopo, deve essere modificato per supportare più tipi di istanza o deve essere in corso un ripristino host.
`permanent-failure`	È stato rilevato un errore irreversibile. Riceverai una notifica di espulsion e tramite le istanze o e-mail. È possibile che l'esecuzione delle istanze continui. Se interrompi o interrompi tutte le istanze su un host dedicato con questo stato, l'host viene AWS ritirato. AWS non riavvia le istanze in questo stato. Le istanze non possono essere avviate su occorrenze degli Host dedicati in questo stato.
`released-permanent-failure`	AWS rilascia in modo permanente gli host dedicati che hanno avuto esito negativo e che non contengono più istanze in esecuzione. L'ID dell'Host dedicato non è più disponibile per l'utilizzo.

Tieni traccia delle modifiche alla configurazione degli host dedicati di Amazon EC2 utilizzando AWS Config

È possibile AWS Config utilizzarlo per registrare le modifiche alla configurazione per gli host dedicati e per le istanze avviate, interrotte o terminate su di essi. Puoi quindi utilizzare le informazioni acquisite da AWS Config come origine dati per i report sulle licenze.

AWS Config registra le informazioni di configurazione per gli host dedicati e le istanze singolarmente e associa queste informazioni tramite relazioni. Sono disponibili tre condizioni per la generazione di report:

- AWS Config stato di registrazione: quando è attivo, AWS Config sta registrando uno o più tipi di AWS risorse, che possono includere host dedicati e istanze dedicate. Per acquisire le informazioni richieste per i report sulle licenze, verifica che gli host e le istanze vengano registrate con i seguenti campi.
- Host recording status (Stato registrazione host) — Se questa opzione è impostata su Enabled (Abilitato), vengono registrate le informazioni sulla configurazione delle occorrenze degli Host dedicati.
- Instance recording status (Stato registrazione istanza) — Se questa opzione è impostata su Enabled (Abilitato), vengono registrate le informazioni sulla configurazione delle occorrenze degli Istanze dedicate.

Se una qualsiasi di queste tre condizioni è disabilitata, l'icona del pulsante Edit Config Recording (Modifica la registrazione di Config) è di colore rosso. Per sfruttare tutti i vantaggi di questo strumento assicurati che siano abilitati tutti e tre i metodi di registrazione. Dopo aver abilitato tutti e tre i metodi, l'icona sarà verde. Per modificare le impostazioni, scegli Edit Config Recording (Modifica la registrazione di Config). Verrai indirizzato alla AWS Config pagina di configurazione della AWS Config console, dove puoi configurare AWS Config e avviare la registrazione per gli host, le istanze e gli altri tipi di risorse supportati. Per ulteriori informazioni, consulta Configurazione AWS Config tramite la console nella Guida per gli AWS Config sviluppatori.

> **Note**
>
> AWS Config registra le tue risorse dopo averle scoperte, operazione che potrebbe richiedere diversi minuti.

Dopo aver AWS Config iniziato a registrare le modifiche alla configurazione degli host e delle istanze, è possibile ottenere la cronologia di configurazione di qualsiasi host allocato o rilasciato e di qualsiasi istanza avviata, interrotta o terminata. Ad esempio, in qualsiasi punto della cronologia della configurazione di un Host dedicato, puoi controllare il numero di istanze avviate su tale host, nonché il numero di socket e core sull'host. Per qualsiasi istanza puoi inoltre cercare l'ID della relativa Amazon Machine Image (AMI). Puoi utilizzare queste informazioni per generare report sulle licenze per il software collegato a server con licenza per socket o per core.

Puoi visualizzare la cronologia di configurazione in uno dei seguenti modi:

- Utilizzando la console. AWS Config Per ogni risorsa registrata, puoi visualizzare una pagina della timeline, che fornisce una cronologia dei dettagli di configurazione. Per visualizzare questa pagina, scegli l'icona grigia nella colonna Timeline configurazione della pagina Host dedicati. Per ulteriori informazioni, consulta Visualizzazione dei dettagli di configurazione nella AWS Config console nella Guida per gli AWS Config sviluppatori.
- Eseguendo AWS CLI comandi. Per ottenere un elenco di tutti gli host e di tutte le istanze, innanzitutto puoi utilizzare il comando list-discovered-resources. Puoi quindi utilizzare il comando get-resource-config-history per ottenere i dettagli di configurazione di un host o di un'istanza per un determinato intervallo di tempo.
- Utilizzando l' AWS Config API nelle tue applicazioni. Innanzitutto, puoi utilizzare l'ListDiscoveredResourcesazione per ottenere un elenco di tutti gli host e le istanze. Quindi, puoi utilizzare l'GetResourceConfigHistoryazione per ottenere i dettagli di configurazione di un host o di un'istanza per un intervallo di tempo specifico.

Ad esempio, per ottenere un elenco di tutti i tuoi host dedicati AWS Config, esegui un comando CLI come il seguente.

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Host
```

Per ottenere la cronologia di configurazione di un host dedicato da AWS Config, esegui un comando CLI come il seguente.

```
aws configservice get-resource-config-history \
    --resource-type AWS::EC2::Instance \
    --resource-id i-1234567890abcdef0
```

Da gestire AWS Config impostazioni utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella pagina Host dedicati (Host dedicati) scegliere Edit Config Recording (Modifica la registrazione di Config).
3. Nella AWS Config console, segui i passaggi forniti per attivare la registrazione. Per ulteriori informazioni, consulta Configurazione AWS Config tramite la console.

Per ulteriori informazioni, vedere Visualizzazione dei dettagli di configurazione nella AWS Config console.

Per attivare AWS Config utilizzando la riga di comando o l'API

- AWS CLI: visualizzazione dei dettagli di configurazione (AWS CLI) nella Guida per gli AWS Config sviluppatori.
- API Amazon EC2:. GetResourceConfigHistory

Istanze dedicate Amazon EC2

Per impostazione predefinita, le istanze EC2 vengono eseguite su hardware di tenancy condiviso. Ciò significa che molteplici account AWS potrebbero condividere lo stesso hardware fisico.

Le istanze dedicate sono istanze EC2 che vengono eseguite su hardware dedicato a un singolo account. AWS Ciò significa che le istanze dedicate sono fisicamente isolate a livello di hardware host dalle istanze appartenenti ad altre Account AWS, anche se tali account sono collegati a un unico account pagante. Tuttavia, le istanze dedicate potrebbero condividere l'hardware con altre istanze della stessa Account AWS che non sono istanze dedicate.

Le istanze dedicate non forniscono visibilità o controllo sul posizionamento delle istanze e non supportano l'affinità con gli host. Se si arresta e si avvia un'istanza dedicata, potrebbe non essere eseguita sullo stesso host. Allo stesso modo, non è possibile scegliere come target un host specifico su cui avviare o eseguire un'istanza. Inoltre, le Istanze dedicate forniscono un supporto limitato per l'uso di licenze proprie (BYOL).

Se hai bisogno di visibilità e controllo sul posizionamento delle istanze e di un supporto BYOL più completo, prendi in considerazione l'utilizzo di un host dedicato. Istanze dedicate e host dedicati possono essere entrambi utilizzati per avviare istanze Amazon EC2 su server fisici dedicati. Non ci sono differenze di prestazioni, sicurezza o fisiche tra le Istanze dedicate e le istanze negli Host dedicati. Tuttavia, ci sono alcune differenze chiave tra di loro. La tabella seguente evidenzia alcune differenze chiave tra istanze dedicate e host dedicati:

	Dedicated Host	Dedicated Instance
Server fisico dedicato	Server fisico con capacità di istanza completamente dedicata.	Server fisico dedicato a un singolo account cliente.

	Dedicated Host	Dedicated Instance
Condivisione della capacità di istanza	Possibilità di condividere la capacità di istanza con altri account.	Non supportata
Fatturazione	Per-host fatturazione	Per-instance fatturazione
Visibilità di socket, core e ID host	Fornisce la visibilità del numero di socket e core fisici	Nessuna visibilità
Affinità a livello di host e istanza	Consente di distribuire in modo omogeneo le istanze sullo stesso server fisico nel tempo	Non supportato
Posiziona mento delle istanze interessate	Fornisce ulteriore visibilità e controllo sul posizionamento delle istanze su un server fisico	Non supportato
Ripristino automatico dell'istanza	Supportato. Per ulteriori informazioni, consulta Ripristino host dedicato di Amazon EC2.	Supportata
Modello di licenza Bring Your Own License (BYOL)	Supportata	Supporto parziale*
Prenotazioni della capacità	Non supportata	Supportata

* Le licenze Microsoft SQL Server con mobilità delle licenze tramite Software Assurance e Windows Virtual Desktop Access (VDA) possono essere utilizzate con l'istanza dedicata.

Per ulteriori informazioni, consulta Host dedicati di Amazon EC2.

Indice

- Nozioni di base su Istanza dedicata
- Funzionalità supportate
- Limitazioni di Istanze dedicate
- Prezzi delle Istanze dedicate
- Avvio di Istanze dedicate in un VPC con tenancy predefinita
- Modifica della tenancy di un'istanza EC2
- Modifica della tenancy di un'istanza di un PVC

Nozioni di base su Istanza dedicata

Un VPC può avere una tenancy di `default` o `dedicated`. Per impostazione predefinita, i tuoi VPC hanno una tenancy `default`, mentre le istanze avviate in un VPC di tenancy `default` hanno la tenancy `default`. Per avviare le istanze dedicate, procedi nel modo seguente:

- Crea un VPC con una tenancy di `dedicated` in modo che tutte le istanze del VPC vengano eseguite come istanze dedicate. Per ulteriori informazioni, consulta Avvio di Istanze dedicate in un VPC con tenancy predefinita.
- Crea un VPC con una tenancy di `default` e specifica manualmente una tenancy di `dedicated` per le istanze da eseguire come istanze dedicate. Per ulteriori informazioni, consulta Avvio di Istanze dedicate in un VPC con tenancy predefinita.

Funzionalità supportate

Le istanze dedicate supportano le seguenti funzionalità e integrazioni di AWS servizi:

Funzionalità

- Istanze riservate
- Scalabilità automatica
- Ripristino automatico
- Istanze spot dedicate
- Istanze a prestazioni espandibili

Istanze riservate

Per prenotare capacità per le istanze dedicate, puoi acquistare Istanze riservate dedicate o prenotazioni della capacità. Per ulteriori informazioni, consultare Panoramica delle istanze riservate per Amazon EC2 e Riserva la capacità di calcolo con EC2 On-Demand Capacity Reservations.

Quando acquisti un'istanza riservata dedicata, acquisti anche la capacità di avviare un'istanza dedicata a una tariffa di utilizzo molto ridotta; il costo di utilizzo si applica solo se avvii un'istanza con tenancy dedicata. Quando acquisti un'istanza riservata con una tenancy predefinita, si applica solo a un'istanza in esecuzione con la tenancy `default`; non si applicherà invece a un'istanza in esecuzione con la tenancy `dedicated`.

Non puoi modificare la tenancy di un'Istanza riservata dopo l'acquisto. Puoi tuttavia scambiare un'Istanza riservata modificabile con una nuova Istanza riservata modificabile con una tenancy diversa.

Scalabilità automatica

Per avviare le Istanze dedicate, è possibile utilizzare Amazon EC2 Auto Scaling. Per ulteriori informazioni, consulta Creazione di un modello di avvio con impostazioni avanzate nella Guida per l'utente di Amazon EC2 Auto Scaling.

Ripristino automatico

È possibile configurare il ripristino automatico per un'istanza dedicata se viene compromessa a causa di un guasto hardware sottostante o di un problema che richiede l' AWS intervento di riparazione. Per ulteriori informazioni, consulta Ripristino automatico dell'istanza.

Istanze spot dedicate

Puoi eseguire un'istanza spot dedicata specificando una tenancy `dedicated` quando crei una richiesta di istanza spot. Per ulteriori informazioni, consulta Avvio su hardware con tenant singolo.

Istanze a prestazioni espandibili

È possibile sfruttare i vantaggi dell'esecuzione su hardware istanza dedicata a tenancy singola con the section called "Istanze a prestazioni espandibili". Le istanze dedicate T3 vengono lanciate in modalità illimitata per impostazione predefinita e forniscono un livello di base delle prestazioni della CPU con la possibilità di raggiungere un livello di CPU superiore quando richiesto dal carico di lavoro. Le prestazioni di base T3 e la capacità di ottimizzazione sono governate dai crediti CPU. A causa della natura espandibile dei tipi di istanza T3, si consiglia di monitorare il modo in cui le istanze T3

utilizzano le risorse della CPU dell'hardware dedicato per ottenere prestazioni ottimali. Le istanze dedicate T3 sono destinate a clienti con carichi di lavoro diversi che visualizzano un comportamento casuale della CPU, ma che idealmente hanno un utilizzo medio della CPU pari o inferiore a quello di base. Per ulteriori informazioni, consulta the section called "Concetti chiave".

Amazon EC2 dispone di sistemi per identificare e correggere la variabilità delle prestazioni. Tuttavia, è ancora possibile sperimentare la variabilità a breve termine se si avviano più istanze dedicate T3 con modelli di utilizzo della CPU correlati. Per questi carichi di lavoro più complessi o correlati, si consiglia di utilizzare istanze dedicate M5 o M5a anziché istanze dedicate T3.

Limitazioni di Istanze dedicate

Quando utilizzi le istanze dedicate, tieni presente quanto indicato di seguito:

- Alcuni AWS servizi o le relative funzionalità non sono supportati da un VPC con la tenancy dell'istanza impostata su. `dedicated` Fai riferimento alla documentazione del relativo servizio per verificare se vi sono delle limitazioni.
- Alcuni tipi di istanza non possono essere avviati in un VPC se la tenancy delle istanze è impostata su `dedicated`. Per ulteriori informazioni sui tipi di istanza supportati, consulta Istanze dedicate di Amazon EC2.
- Quando avvii un'Istanza dedicata supportata da Amazon EBS, il volume EBS non viene eseguito sull'hardware con tenant singola.

Prezzi delle Istanze dedicate

I prezzi per le istanze dedicate sono diversi dai prezzi per le istanze. On-Demand Per ulteriori informazioni, consulta le Istanze dedicate di Amazon EC2.

Avvio di Istanze dedicate in un VPC con tenancy predefinita

Quando crei un VPC, puoi specificarne la tenancy delle istanze. Se avvii un'istanza in un VPC che ha una tenancy dell'istanza `dedicated`, verrà eseguita come istanza dedicata su un hardware a tua disposizione.

Per ulteriori informazioni sull'avvio di un'istanza con tenancy `host`, consultare Avvia le istanze Amazon EC2 su un host dedicato Amazon EC2.

Per ulteriori informazioni sulle opzioni di tenancy di un VPC, consulta la sezione Create a VPC nella Guida per l'utente di Amazon VPC.

Requisiti

- Scegli un tipo di istanza supportato. Per ulteriori informazioni, consulta Istanze dedicate di Amazon EC2.

Console

Per avviare un'istanza dedicata in un VPC con tenancy predefinita

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Istanze, Avvia istanza.
3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona un'AMI dall'elenco.
4. Nella sezione Tipo di istanza, seleziona il tipo di istanza da avviare.
5. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da associare all'istanza.
6. Nella sezione Advanced details (Dettagli avanzati), per Tenancy seleziona Dedicated (Dedicata).
7. Configura le opzioni rimanenti dell'istanza in base alla necessità. Per ulteriori informazioni, consulta Riferimento per i parametri di configurazione delle EC2 istanze Amazon.
8. Scegliere Launch Instance (Avvia istanza).

AWS CLI

Per impostare l'opzione della tenancy per un'istanza durante l'avvio

Utilizzare il comando run-instances e includere `Tenancy` con l'opzione `--placement`.

```
--placement Tenancy=dedicated
```

PowerShell

Per impostare l'opzione della tenancy per un'istanza durante l'avvio

Utilizza il New-EC2Instance cmdlet con il parametro. `-Placement_Tenancy`

```
-Placement_Tenancy dedicated
```

Modifica della tenancy di un'istanza EC2

Puoi modificare la tenancy di un'istanza interrotta dopo averla avviata. Le modifiche apportate avranno effetto al successivo avvio dell'istanza.

In alternativa, è possibile modificare la tenancy del cloud privato virtuale (VPC). Per ulteriori informazioni, consulta the section called "Modifica della tenancy di un VPC".

Limitazioni

- Non puoi modificare la tenancy di un'istanza utilizzando la Console di gestione AWS.
- L'istanza deve essere nello stato `stopped`.
- I dettagli del sistema operativo dell'istanza e l'eventuale installazione di SQL Server influiscono sulle conversioni supportate. Per ulteriori informazioni sui percorsi di conversione di tenancy disponibili per la tua istanza, consulta Conversione di tenancy nella Guida per l'utente di License Manager.
- Per le istanze T3, è necessario avviare l'istanza su un host dedicato per utilizzare una tenancy di `host`. Non puoi modificare la tenancy da `host` a `dedicated` o `default`. Se si prova ad apportare una di queste modifiche di tenancy non supportate, verrà visualizzato il codice di errore `InvalidRequest`.

AWS CLI

Per modificare il valore della tenancy di un'istanza

Utilizzare il comando modify-instance-placement.

```
aws ec2 modify-instance-placement \
    --instance-id i-1234567890abcdef0 \
    --tenancy dedicated
```

PowerShell

Per modificare il valore della tenancy di un'istanza

Utilizzare il cmdlet Edit-EC2InstancePlacement

```
Edit-EC2InstancePlacement `
```

```
    -InstanceId i-1234567890abcdef0 `
    -Tenancy Dedicated
```

Modifica della tenancy di un'istanza di un PVC

Puoi modificare la tenancy di un'istanza di un cloud privato virtuale (VPC) da `dedicated` a `default` dopo averla creata. La modifica di una tenancy delle istanze del VPC non influisce sulla tenancy di eventuali istanze esistenti nel VPC. Al successo avvio di un'istanza nel VPC, l'istanza avrà una tenancy `default`, a meno che durante l'avvio dell'istanza non specifichi un valore diverso.

In alternativa, è possibile cambiare la tenancy di istanze specifiche. Per ulteriori informazioni, consulta the section called "Modifica della tenancy di un'istanza".

Limitazioni

- Non è possibile modificare la tenancy di istanza di un VPC da `default` a `dedicated` dopo la sua creazione.
- Non puoi modificare la tenancy dell'istanza di un VPC utilizzando la Console di gestione AWS.

AWS CLI

Per modificare l'attributo della tenancy dell'istanza di un VPC

Utilizza il comando modify-vpc-tenancy. L'unico valore della tenancy supportato è `default`.

```
aws ec2 modify-vpc-tenancy \
    --vpc-id vpc-1234567890abcdef0 \
    --instance-tenancy default
```

PowerShell

Per modificare l'attributo della tenancy dell'istanza di un VPC

Utilizza il cmdlet Edit-EC2VpcTenancy. L'unico valore della tenancy supportato è `Default`.

```
Edit-EC2VpcTenancy `
    -VpcId vpc-1234567890abcdef0 `
    -InstanceTenancy Default
```

On-Demand Prenotazioni di capacità e blocchi di capacità per ML

Prenotazioni della capacità ti permette di prenotare la capacità di elaborazione per le istanze Amazon EC2 in una zona di disponibilità specifica. Esistono due tipi di prenotazioni della capacità per casi d'uso differenti.

Tipi di prenotazioni della capacità

- On-Demand Prenotazioni di capacità
- Blocchi di capacità per ML

Per organizzare le prenotazioni di capacità in raccolte logiche, consulta Gruppi di risorse per le prenotazioni di capacità.

Di seguito sono riportati alcuni casi d'uso comuni per On-Demand Capacity Reservations:

- Scalabilità degli eventi: crea prenotazioni di On-Demand capacità prima degli eventi aziendali critici per assicurarti di poter scalare quando necessario.
- Requisiti normativi e disaster recovery: utilizza On-Demand Capacity Reservations per soddisfare i requisiti normativi in materia di alta disponibilità e riserva la capacità in una zona o regione di disponibilità diversa per il disaster recovery.
- Condivisione della capacità inutilizzata: utilizza le prenotazioni di capacità interrompibile per rendere disponibile la capacità inutilizzata per altri carichi di lavoro all'interno del tuo account, mantenendo il controllo per recuperarla quando necessario.

Di seguito sono elencati alcuni casi d'uso comuni di Blocchi di capacità per ML:

- Addestramento e messa a punto dei modelli di machine learning (ML): ottieni un accesso ininterrotto alle istanze GPU che hai prenotato per completare l'addestramento e la messa a punto dei modelli di ML.
- Esperimenti e prototipi di ML: esegui esperimenti e crea prototipi che richiedono istanze GPU per brevi periodi.

Quando utilizzare Capacity Reservation On-Demand

Utilizza On-Demand Capacity Reservations se hai requisiti di capacità rigorosi e i tuoi carichi di lavoro aziendali critici attuali o futuri richiedono una garanzia della capacità. Con On-Demand

Capacity Reservations, puoi assicurarti di avere sempre accesso alla capacità di Amazon EC2 che hai riservato per tutto il tempo necessario.

Quando utilizzare Blocchi di capacità per ML

Utilizza Blocchi di capacità per ML quando devi assicurarti di avere accesso ininterrotto alle istanze GPU per un periodo di tempo definito a partire da una data futura. I blocchi di capacità sono ideali per addestrare e perfezionare i modelli di ML, per brevi cicli di sperimentazione e per gestire i picchi temporanei della domanda di inferenza in futuro. Con Blocchi di capacità puoi assicurarti di avere accesso alle risorse GPU in una data specifica per eseguire i tuoi carichi di lavoro ML.

Riserva la capacità di calcolo con EC2 On-Demand Capacity Reservations

Le prenotazioni della capacità di Amazon EC2 ti permettono di prenotare la capacità di elaborazione per le istanze Amazon EC2 in una zona di disponibilità specifica per qualsiasi durata. Se hai tuoi requisiti di capacità per carichi di lavoro aziendali critici attuali o futuri che richiedono un certo livello di garanzia della capacità a lungo o breve termine, ti consigliamo di creare una prenotazione della capacità per aiutarti ad avere sempre accesso alla capacità di Amazon EC2 quando ne hai bisogno, per tutto il tempo necessario.

Puoi creare una prenotazione della capacità in qualsiasi momento e scegliere quando avviarla. Puoi richiedere una prenotazione della capacità per uso immediato oppure puoi richiedere una prenotazione della capacità per una data futura.

- Se richiedi una prenotazione della capacità per uso immediato, la prenotazione della capacità diventa immediatamente disponibile per l'uso e non è previsto alcun impegno a termine. È possibile modificare la prenotazione della capacità in qualsiasi momento e annullarla in qualsiasi momento per liberare la capacità riservata e non incorrere in addebiti.
- Se richiedi una prenotazione di capacità con data futura, specifichi quando hai bisogno della capacità e per quanto tempo ti impegni a mantenerla. Alla data futura specificata, la prenotazione della capacità diventa disponibile per l'uso e inizia la fatturazione. Durante la durata dell'impegno, non puoi ridurre il numero di istanze o la durata dell'impegno al di sotto dell'impegno iniziale. Puoi annullare la prenotazione della capacità, ma potrebbe essere applicata una penale a seconda del momento dell'annullamento. Una volta trascorsa la durata dell'impegno, è possibile modificare la prenotazione di capacità in qualsiasi modo o annullarla gratuitamente.

Prenotazioni di capacità può essere utilizzata solo dalle istanze che corrispondono agli attributi. Come impostazione predefinita, Prenotazioni di capacità abbina automaticamente le nuove istanze

e le istanze in esecuzione che hanno attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy). Questo significa che qualsiasi istanza con attributi corrispondenti viene eseguita automaticamente nella Prenotazione della capacità. Tuttavia, puoi anche utilizzare una Prenotazione della capacità per carichi di lavoro specifici. In questo modo puoi controllare in modo esplicito quali istanze possono essere eseguite in quella capacità riservata. Puoi anche specificare che le istanze verranno eseguite solo in un gruppo di risorse Capacity Reservation o Capacity Reservation.

> **Important**
>
> Future-dated Le prenotazioni di capacità servono ad aiutarti ad avviare e coprire istanze incrementali e non a coprire le istanze in esecuzione esistenti. Se hai bisogno di coprire istanze esistenti in esecuzione, utilizza invece prenotazioni della capacità che iniziano immediatamente.

Tutte le istanze Amazon EC2 supportate con attributi corrispondenti, ossia tipo di istanza, piattaforma, zona di disponibilità e tenancy, sono idonee per l'esecuzione in una prenotazione della capacità. L'istanza Amazon EC2 può essere avviata da te (istanze non gestite) o per tuo conto da un AWS servizio (istanze gestite). Ciò vale in particolare per le prenotazioni della capacità aperte, che vengono automaticamente abbinate a qualsiasi istanza in esecuzione con attributi corrispondenti. Ad esempio, le istanze gestite avviate per tuo conto dai seguenti servizi possono essere eseguite nelle prenotazioni della capacità che crei e gestisci.

- Amazon EC2 Auto Scaling
- Amazon ECS
- Amazon EKS
- Amazon EMR
- AWS Batch
- AWS Elastic Beanstalk
- AWS ParallelCluster
- Servizio di calcolo parallelo AWS (AWS PCS)

Indice

- Concetti per le prenotazioni della capacità di Amazon EC2

- Differenze tra Prenotazioni di capacità, Istanze riservate e Savings Plans.
- Piattaforme supportate
- Quote
- Limitazioni
- Prezzi e fatturazione di Prenotazione della capacità
- Creazione di una Prenotazione della capacità
- Visualizza lo stato di una prenotazione della capacità
- Avvio di istanze in una Prenotazione della capacità esistente
- Modifica una prenotazione della capacità attiva
- Modifica le impostazioni di prenotazione della capacità della tua istanza
- Spostare la capacità tra le prenotazioni della capacità
- Suddivisione della capacità da una prenotazione della capacità esistente
- Annullamento di una Prenotazione della capacità
- Utilizza Capacity Reservations con gruppi di collocamento
- Prenotazioni della capacità in zone locali
- Prenotazioni della capacità nelle zone Wavelength
- Prenotazioni di capacità su AWS Outposts
- Prenotazioni della capacità condivise
- Parco istanze prenotazione della capacità
- Monitora l'utilizzo delle prenotazioni di capacità con delle metriche CloudWatch
- Monitorare il sottoutilizzo delle prenotazioni della capacità
- Monitorare le modifiche di stato per le prenotazioni della capacità con data futura
- Prenotazioni di capacità interrompibile

Concetti per le prenotazioni della capacità di Amazon EC2

I seguenti concetti chiave si applicano alle prenotazioni della capacità.

Argomenti

- Data e ora di inizio
- Data e ora di fine
- Durata dell'impegno

- Future-dated Valutazione della prenotazione della capacità
- Attributi della prenotazione della capacità
- Criteri di corrispondenza delle istanze

Data e ora di inizio

La data e l'ora di inizio definiscono quando la prenotazione della capacità diventa disponibile per l'uso. Una prenotazione della capacità può iniziare immediatamente o in una data futura.

- Se scegli di far iniziare immediatamente una prenotazione della capacità, la capacità riservata diventa disponibile per l'uso subito dopo averla creata e la fatturazione inizia non appena la prenotazione della capacità diventa attiva. Non è necessario assumere alcun impegno a termine. Puoi modificare la prenotazione della capacità in base alla necessità in qualsiasi momento e annullarla in qualsiasi momento per liberare la capacità ed evitare di incorrere in addebiti.
- Se scegli di avviare una prenotazione di capacità in una data futura, specifichi quando hai bisogno della capacità e per quanto tempo ti impegni a mantenerla. Alla data futura specificata, la prenotazione della capacità diventa disponibile per l'uso e la fatturazione inizia dopo che la prenotazione di capacità è entrata nello stato attivo. La durata dell'impegno inizia non appena la Capacity Reservation viene accantonata nel tuo account. Durante questo periodo, non puoi ridurre il numero di istanze al di sotto del numero di istanze impegnate o scegliere una data di fine precedente alla durata dell'impegno. Puoi cancellare la Capacity Reservation, ma potrebbe essere applicata una penale a seconda del momento dell'annullamento. Per ulteriori informazioni, consulta Annullamento di una Prenotazione della capacità. Una volta scaduta la durata dell'impegno, puoi modificare la prenotazione di capacità in qualsiasi modo o annullarla per liberare la capacità riservata e non incorrere in addebiti.

Data e ora di fine

La data e l'ora di fine definiscono il momento in cui termina la prenotazione della capacità e la capacità riservata viene liberata dall'account. Puoi configurare una prenotazione della capacità in modo che termini automaticamente in una data e un'ora specifiche oppure in modo che rimanga attiva a tempo indeterminato fino a quando non viene annullata manualmente.

Se configuri una prenotazione della capacità per terminare automaticamente, la prenotazione della capacità scade entro un'ora dall'orario specificato. Ad esempio, se specifichi `5/31/2019, 13:30:55`, è garantito che la prenotazione della capacità termini tra le `13:30:55` e le `14:30:55` del `5/31/2019`.

Dopo il termine della prenotazione, la capacità riservata viene rilasciata dal tuo account e non puoi più puntare istanze alla prenotazione della capacità. Le istanze in esecuzione nella capacità riservata continuano a essere eseguite senza interruzioni. Se le istanze che puntano a una Prenotazione della capacità vengono arrestate, non è possibile riavviarle finché non vengono rimosso le loro preferenze di target della Prenotazione della capacità o configurarle in modo che puntino a una Prenotazione della capacità diversa. Per ulteriori informazioni, consulta Modifica le impostazioni di prenotazione della capacità della tua istanza.

Durata dell'impegno

La durata dell'impegno si applica solo alle prenotazioni della capacità con data futura.

La durata dell'impegno è la durata minima per la quale l'utente si impegna a mantenere attiva la prenotazione della capacità con data futura nel proprio account dopo che è stata fornita. È possibile mantenere una prenotazione della capacità con data futura per un periodo più lungo della durata dell'impegno, ma non per un periodo inferiore. Quanto segue si applica durante la durata dell'impegno:

- È possibile annullare la prenotazione di capacità durante la durata dell'impegno, ma potrebbe essere applicata una penale di cancellazione. Per ulteriori informazioni, consulta Spese di annullamento.
- Non puoi ridurre il numero di istanze al di sotto del numero di istanze impegnate, ma puoi aumentarlo.
- Non puoi configurare una prenotazione della capacità in modo tale che termini automaticamente a una data o a un'ora comprese nella durata dell'impegno. È possibile estendere la data e l'ora di fine durante la durata dell'impegno.

Amazon EC2 utilizza la durata dell'impegno specificata per valutare se la richiesta può essere supportata. La durata minima dell'impegno è di 14 giorni per la maggior parte dei tipi di istanze o di 12 settimane per le istanze U e X. Durante la valutazione di una richiesta, Amazon EC2 potrebbe stabilire che è in grado di supportare un impegno di durata inferiore. In tal caso, Amazon EC2 pianifica la prenotazione della capacità con data futura con una durata di impegno più breve. Ciò significa che ti impegni a mantenere la prenotazione della capacità nel tuo account per un periodo più breve di quello richiesto inizialmente.

Future-dated Valutazione della prenotazione della capacità

Quando richiedi una prenotazione della capacità con data futura, Amazon EC2 valuta la richiesta per determinare se può essere supportata in base alla disponibilità della capacità e alla durata dell'impegno specificata. La valutazione viene completata generalmente entro 5 giorni. Amazon EC2 considera diversi fattori nella valutazione di una richiesta, tra cui:

- Capacità di fornitura prevista
- La durata dell'impegno
- Con quanto anticipo viene richiesta la prenotazione della capacità rispetto alla data di inizio
- La dimensione della richiesta

Puoi richiedere una prenotazione della capacità con data futura con un anticipo compreso tra 5 e 120 giorni. Ti consigliamo di effettuare la richiesta con almeno 56 giorni (8 settimane) di anticipo per consentirci di soddisfarla al meglio. La durata minima dell'impegno è di 14 giorni per la maggior parte dei tipi di istanze o di 12 settimane per le istanze U e X e il numero minimo di istanze è di 32 vCPU.

La prenotazione della capacità rimane nello stato `assessing` durante la valutazione della richiesta.

Se la richiesta può essere supportata, la prenotazione della capacità entra nello stato `scheduled` e la sua consegna è programmata nella data e all'ora richieste. Il numero totale di istanze rimane 0 mentre lo stato di Capacity Reservation è attivo. `scheduled` Una prenotazione della capacità pianificata diventerà `active` e disponibile per l'uso alla data richiesta.

Se una richiesta non può essere supportata, la prenotazione della capacità entra nello stato `unsupported`. Le prenotazioni della capacità non supportate non vengono consegnate.

È possibile annullare una prenotazione di capacità con data futura nello stato`assessing`,`scheduled`, or. `active` Potrebbe essere applicata una penale di cancellazione. Per ulteriori informazioni, consulta Annullamento di una Prenotazione della capacità.

Per creare una prenotazione di capacità con data futura, consulta. Creazione di una prenotazione della capacità con data futura

Attributi della prenotazione della capacità

Quando crei una Prenotazione della capacità, devi specificare i seguenti attributi:

- Zona di disponibilità

- Tipo di istanza
- Piattaforma (tipo di sistema operativo)
- Tenancy (`default` o `dedicated`)

Solo le istanze che corrispondono a questi attributi possono essere avviate o eseguite nella prenotazione della capacità.

Criteri di corrispondenza delle istanze

I criteri di corrispondenza delle istanze, o idoneità dell'istanza, determinano quali istanze possono essere avviate ed eseguite nella prenotazione della capacità. Una prenotazione della capacità può avere uno dei seguenti criteri di corrispondenza:

- Aperta - La prenotazione della capacità corrisponde automaticamente a tutte le istanze che hanno attributi corrispondenti (tipo di istanza, piattaforma e zona di disponibilità). Istanze nuove ed esistenti con attributi corrispondenti vengono automaticamente eseguite nella prenotazione della capacità senza alcuna configurazione aggiuntiva.
- Mirata – La prenotazione della capacità accetta solo le istanze che hanno attributi corrispondenti (tipo di istanza, piattaforma e zona di disponibilità) e che mirano esplicitamente alla prenotazione della capacità. L'istanza deve puntare specificamente alla prenotazione della capacità per l'avvio o l'esecuzione nella sua capacità riservata. In questo modo, puoi controllare in modo esplicito quali istanze possono essere eseguite nella capacità riservata e contribuire a evitare l'utilizzo involontario della capacità riservata.

Quando richiedi una prenotazione della capacità con data futura, puoi specificare solo criteri di corrispondenza mirati. Ciò garantisce che la capacità fornita dalla prenotazione della capacità sia incrementale, o aggiuntiva, a tutte le istanze in esecuzione o alla capacità riservata di cui disponi al momento della consegna. Dopo che la prenotazione della capacità diventa attiva nel tuo account, puoi modificare i criteri di corrispondenza dell'istanza per aprirla, se necessario. Tuttavia, tieni presente che tutte le istanze corrispondenti verranno eseguite automaticamente nella prenotazione della capacità, il che potrebbe portare a un utilizzo involontario della capacità e impedirti di avviare nuove istanze per l'intero numero di istanze richiesto.

Differenze tra Prenotazioni di capacità, Istanze riservate e Savings Plans.

La tabella seguente evidenzia alcune differenze chiave tra Prenotazioni di capacità, Istanze riservate e Savings Plans:

	Prenotazioni di capacità	Istanze riservate zonali	Istanze riservate regionali	Savings Plans
Termine	Non è richiesto alcun impegno per le prenotazioni della capacità ad uso immediato. Possono essere create, modificate e annullate in base alle esigenze. Con le prenotazioni della capacità con data futura, specifichi una durata dell'impegno per la quale ti impegni a mantenere la capacità nel tuo account. Puoi annullare l'abbonamento in qualsiasi momento; durante la durata dell'impegno potrebbe essere applicato un costo di cancellazione.	Richiedono un impegno fisso di uno o tre anni		
Vantaggio capacità	Capacità riservata in una zona di disponibilità specifica.		Nessuna capacità riservata.	
Sconto di	Nessuno sconto di fatturazione. †	Fornisce uno sconto di fatturazione.		

	Prenotazioni di capacità	Istanze riservate zonali	Istanze riservate regionali	Savings Plans
fatturazione				
Limiti di istanze	Si applicano i limiti delle tue On-Demand istanze per regione.	Il valore predefinito è 20 per zona di disponibilità. È possibile richiedere un aumento del limite.	Il valore predefinito è 20 per regione. È possibile richiedere un aumento del limite.	Nessun limite.

† È possibile combinare le prenotazioni di capacità con Savings Plans o le istanze riservate regionali per ricevere uno sconto.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica delle istanze riservate per Amazon EC2
- Guida per l'utente di Savings Plans

Piattaforme supportate

È necessario creare la Prenotazione della capacità con la piattaforma corretta per assicurarsi che corrisponda correttamente alle istanze. Le prenotazioni della capacità supportano i seguenti valori per `platform`:

- Linux/UNIX
- Linux con SQL Server Standard
- Linux con SQL Server Web
- Linux con SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- RHEL con SQL Server Standard
- RHEL con SQL Server Enterprise
- RHEL con SQL Server Web

- RHEL con HA
- RHEL con HA e SQL Server Standard
- RHEL con HA e SQL Server Enterprise
- Ubuntu Pro
- Windows
- Windows con SQL Server
- Windows con SQL Server Web
- Windows con SQL Server Standard
- Windows con SQL Server Enterprise

Per garantire che un'istanza venga eseguita in una specifica prenotazione della capacità, la piattaforma della prenotazione della capacità deve corrispondere alla piattaforma dell'AMI utilizzata per avviare l'istanza. Per le AMI Linux, è importante verificare se la piattaforma AMI utilizza il valore generale Linux/UNIX o un valore più specifico come SUSE Linux.

Console

Per verificare la piattaforma AMI

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Seleziona l'AMI.
4. Nella scheda Dettagli, controlla il valore di Dettagli della piattaforma.

AWS CLI

Per verificare la piattaforma AMI

Utilizza il comando describe-images e controlla il valore di `PlatformDetails`.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[*].PlatformDetails
```

Di seguito è riportato un output di esempio.

```
[
    "Linux/UNIX"
]
```

PowerShell

Per verificare la piattaforma AMI

Usa il Get-EC2Image cmdlet e controlla il valore di. `PlatformDetails`

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).PlatformDetails
```

Di seguito è riportato un output di esempio.

```
Linux/UNIX
```

Quote

Il numero di istanze per le quali è consentito riservare capacità si basa sulla quota di istanze del On-Demand tuo account. È possibile prenotare la capacità per tante istanze quante ne permette tale quota, meno il numero delle istanze in esecuzione.

Le prenotazioni di capacità negli `delayed` stati`assessing`, `scheduled` `pending``active`, e vengono conteggiate ai fini della quota di On-Demand istanze dell'utente.

Limitazioni

Prima di creare le Prenotazioni di capacità, considera le seguenti limitazioni e restrizioni.

- Le prenotazioni di capacità attive e non utilizzate vengono conteggiate ai fini dei limiti dell' On-Demand istanza.
- Le prenotazioni di capacità non sono trasferibili da un AWS account all'altro. Tuttavia, puoi condividere le prenotazioni di capacità con altri AWS account. Per ulteriori informazioni, consulta Prenotazioni della capacità condivise.
- Gli sconti di fatturazione Istanza riservata zonali non si applicano a Prenotazioni di capacità.
- Le Prenotazioni di capacità non possono essere create in gruppi di collocazione cluster. I gruppi di collocazione di partizione non sono supportati.
- Prenotazioni di capacità non può essere utilizzato con Host dedicati. Prenotazioni della capacità non può essere utilizzato con Istanze dedicate.

- [Istanze Windows] Prenotazioni della capacità non può essere impiegato con uso di licenze proprie (BYOL).
- [Istanze Red Hat] Prenotazioni della capacità può essere impiegato con uso di licenze proprie (BYOL).
- Prenotazioni di capacità non assicura che un'istanza ibernata possa riprendere dopo aver tentato di avviarla.
- Puoi richiedere prenotazioni di capacità con data futura per un numero di istanze con un minimo di 32 vCPU. Ad esempio, se richiedi una prenotazione di capacità con data futura per `m5.xlarge` le istanze, devi richiedere almeno 8 istanze (8 * m5.xlarge = 32 vCPU).
- Puoi richiedere prenotazioni di capacità con data futura per i tipi di esempio delle seguenti famiglie: C, G, I, M, R, T, U e X.

Prezzi e fatturazione di Prenotazione della capacità

Gli argomenti di questa sezione forniscono una panoramica dei prezzi e della fatturazione per Prenotazioni della capacità.

Argomenti

- Prezzi
- Fatturazione
- Sconti di fatturazione
- Spese di annullamento nel Rapporto sui costi e sull'utilizzo 2.0
- Visualizzazione di una fattura

Prezzi

Le prenotazioni di capacità vengono addebitate alla On-Demand tariffa equivalente indipendentemente dal fatto che si eseguano istanze con capacità riservata o meno, incluso l'eventuale supplemento regionale applicabile per le istanze dedicate. Se non utilizzi la prenotazione, sarà indicata come prenotazione inutilizzata nella fattura Amazon EC2. Quando esegui un'istanza che corrisponde agli attributi di una prenotazione, paghi solamente per l'istanza e non per la prenotazione. Non sono previsti costi iniziali o costi aggiuntivi.

Ad esempio, se crei una Prenotazione della capacità per 20 istanze Linux `m4.large` e ne esegui 15 `m4.large` nella stessa zona di disponibilità, ti verrà addebitato il costo per 15 istanze attive e per 5 istanze non utilizzate nella prenotazione.

Alle prenotazioni della capacità, si applicano sconti di fatturazione per i Savings Plans e per le istanze riservate regionali. Per ulteriori informazioni, consulta Sconti di fatturazione.

Per ulteriori informazioni, consulta Amazon EC2 Prezzi di .

Fatturazione

La fatturazione viene avviata non appena viene effettuato il provisioning della Prenotazione della capacità nel tuo account e prosegue finché la Prenotazione della capacità rimane effettuata nel tuo account. Per le prenotazioni di capacità con data futura, ciò significa che la fatturazione inizia solo dopo che la prenotazione di capacità è stata accantonata nel tuo account alla data futura richiesta.

Le prenotazioni di capacità vengono fatturate in base alla granularità al secondo, con un minimo di 60 secondi. Questo significa che verrai addebitato per ore parziali Ad esempio, se una Prenotazione della capacità rimane con provisioning nell'account per 24 ore e 15 minuti, saranno fatturate `24.25` ore di prenotazione.

Gli esempi seguenti mostrano come viene fatturata una Prenotazione della capacità. La Capacity Reservation viene creata per un'istanza `m4.large` Linux, con una On-Demand tariffa di 0,10 USD per ora di utilizzo. In questo esempio, la Prenotazione della capacità è con provisioning nell'account per cinque ore. La Capacity Reservation è inutilizzata per la prima ora, quindi viene fatturata per un'ora non utilizzata alla tariffa standard del tipo di `m4.large` istanza. On-Demand Dalle due alle cinque ore, la Prenotazione della capacità è occupata da un'istanza `m4.large`. Durante tale periodo, Prenotazione della capacità non accumula nessun costo e all'account viene addebitata l'istanza `m4.large` che la occupa. Alla sesta ora, la Prenotazione della capacità viene annullata e l'istanza `m4.large` viene eseguita normalmente al di fuori della capacità riservata. Per quell'ora, viene addebitata in base alla On-Demand tariffa del tipo di istanza. `m4.large`

Hour	1	2	3	4	5	6	Total cost
Unused Capacity Reservation	$0.10	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.10**
On-demand Instance Usage	$0.00	$0.10	$0.10	$0.10	$0.10	$0.10	**$0.50**
Hourly cost	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.60**

Sconti di fatturazione

Gli sconti di fatturazione per i piani di risparmio e le istanze riservate regionali si applicano alle prenotazioni di capacità. AWS applica automaticamente questi sconti alle prenotazioni di capacità con attributi corrispondenti. Quando una istanza utilizza una Prenotazione della capacità, lo sconto viene applicato all'istanza. Gli sconti vengono applicati preferibilmente all'utilizzo delle istanze prima di utilizzare le Prenotazioni di capacità inutilizzate.

Gli sconti di fatturazione per le Istanze riservate zonali non si applicano alle Prenotazioni di capacità.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica delle istanze riservate per Amazon EC2
- Guida per l'utente di Savings Plans
- Opzioni di fatturazione e acquisto

Spese di annullamento nel Rapporto sui costi e sull'utilizzo 2.0

Se annulli una prenotazione di capacità con data futura e viene applicata una penale di cancellazione, l'addebito appare nel tuo Rapporto AWS sui costi e l'utilizzo (CUR) 2.0. Per ulteriori informazioni sulle colonne relative alla prenotazione della capacità in CUR 2.0, consulta Colonne relative alla prenotazione della capacità. https://docs.aws.amazon.com/cur/latest/userguide/table-dictionary-cur2-capacity-reservation.html Le tabelle seguenti mostrano come vengono visualizzate le voci relative alla prenotazione della capacità prima e dopo l'annullamento.

Valori CUR 2.0 per una prenotazione attiva

capacity_reservation_capacity_reservation_status	line_item_usage_type	Cosa rappresenta
`Reserved`	Prenotazione	Capacità totale riservata
`Used`	BoxUsage	Istanze avviate
`Unused`	UnusedBox	Capacità inattiva

Valori CUR 2.0 dopo l'annullamento

capacity_reservation_capacity_reservation_status	line_item_usage_type	Cosa rappresenta
`Cancelling`	Prenotazione	Capacità annullata
`Cancelling`	UnusedBox	Spese di annullamento

Visualizzazione di una fattura

È possibile rivedere gli addebiti e le spese relative al proprio account sulla console Gestione costi e fatturazione AWS .

- Il Dashboard (Pannello di controllo) mostra un riepilogo di spesa per l'account.
- Nella pagina Bills (Fatture), sotto Details (Dettagli), espandi la sezione Elastic Compute Cloud e la regione per ottenere le informazioni di fatturazione relative alle Prenotazioni di capacità.

Puoi visualizzare gli addebiti online o scarica un file CSV. Per ulteriori informazioni, consulta Capacity Reservation line items.

Creazione di una Prenotazione della capacità

Puoi creare una prenotazione della capacità in qualsiasi momento per assicurarti di avere capacità di elaborazione disponibile in una zona di disponibilità specifica. Una prenotazione della capacità può iniziare immediatamente o in una data futura. La capacità diventa disponibile per l'uso solo dopo che la prenotazione della capacità è entrata nello `active` stato.

> **Note**
>
> Se crei una prenotazione della capacità con criteri di corrispondenza dell'istanza `open` e disponi di istanze in esecuzione con attributi corrispondenti nel momento in cui la prenotazione della capacità diventa attiva, tali istanze vengono eseguite automaticamente nella capacità riservata. Per evitare ciò, utilizza i criteri di corrispondenza delle istanze `targeted`. Per ulteriori informazioni, consulta Criteri di corrispondenza delle istanze.

La richiesta di creare una Prenotazione della capacità ha esito negativo se una delle seguenti condizioni è true:

- Amazon EC2 non dispone di capacità sufficiente per soddisfare la richiesta. Prova in un momento successivo, prova una zona di disponibilità differente o prova una richiesta inferiore. Se l'applicazione è flessibile su più tipi di istanza e dimensioni, prova con attributi di istanza differenti.
- La quantità richiesta supera il limite di On-Demand istanze per la famiglia di istanze selezionata. Aumenta il limite di On-Demand istanze per la famiglia di istanze e riprova. Per ulteriori informazioni, consulta Quote di istanze on demand.

Argomenti

- Creare una prenotazione della capacità per uso immediato
- Creazione di una prenotazione della capacità con data futura

Creare una prenotazione della capacità per uso immediato

Crea una prenotazione della capacità per uso immediato.

Console

Per creare una prenotazione della capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Prenotazioni della capacità, quindi Crea Prenotazione di capacità.
3. Configurare le seguenti impostazioni nella sezione Dettagli istanza.
   a. Tipo di istanza – Il tipo di istanza per il quale prenotare la capacità.
   b. Piattaforma – Il sistema operativo per le istanze. Per ulteriori informazioni, consulta Piattaforme supportate.
   c. Zona di disponibilità – La zona di disponibilità nella quale prenotare la capacità.
   d. Tenancy – Il tipo di tenancy da utilizzare per la capacità riservata. Scegli Predefinito per prenotare la capacità sull'hardware condiviso o Dedicato per prenotare la capacità sull'hardware dedicato al tuo account.
   e. (Opzionale)Gruppo di posizionamento ARNL'ARN del gruppo di posizionamento cluster in cui creare la prenotazione della capacità. Per ulteriori informazioni, consulta Utilizza Capacity Reservations con gruppi di collocamento.
   f. Numero totale di istanze – Il numero di istanze per cui si desidera prenotare la capacità. Se specifichi una quantità che supera la quota di On-Demand istanze rimanente per il tipo di istanza selezionato, la richiesta ha esito negativo.
4. Configurare le seguenti impostazioni nella sezione Reservation details (Dettagli prenotazione):
   a. Prenotazione della capacità inizia– Scegliere Immediatamente.
   b. Prenotazione della capacità termina – Scegliere una delle seguenti opzioni:
      - Manualmente – Prenotare la capacità fino a quando viene annullata esplicitamente.

- Ora specifica – Annullare la prenotazione della capacità automaticamente alla data e all'ora specificate.

c. Idoneità istanza – Selezionare una delle seguenti opzioni:

- aperta – (Predefinito) La prenotazione della capacità corrisponde a qualsiasi istanza con attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy). Se si avvia un'istanza con gli attributi corrispondenti, viene posizionata nella capacità riservata automaticamente.
- mirata – La prenotazione della capacità accetta solo le istanze che hanno attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy) e che mirano in modo esplicito alla prenotazione.

5. Scegli Crea.

AWS CLI

Per creare una prenotazione della capacità

Utilizza il comando create-capacity-reservation.

```
aws ec2 create-capacity-reservation \
    --availability-zone az_name \
    --instance-type instance_type \
    --instance-count number_of_instances \
    --instance-platform operating_system \
    --instance-match-criteria open|targeted
```

PowerShell

Per creare una prenotazione della capacità

Utilizza il cmdlet Add-EC2CapacityReservation.

```
Add-EC2CapacityReservation `
    -AvailabilityZone az_name `
    -InstanceType instance_type `
    -InstanceCount number_of_instances `
    -InstancePlatform operating_system `
    -InstanceMatchCriterion open|targeted
```

Creazione di una prenotazione della capacità con data futura

Richiedi una prenotazione della capacità con data futura se hai bisogno che la capacità riservata diventi disponibile in una data e ora future.

Dopo aver richiesto una prenotazione della capacità con data futura, la richiesta viene sottoposta a una valutazione per determinare se può essere supportata. Per ulteriori informazioni, consulta Future-dated Valutazione della prenotazione della capacità.

Considerazioni

- Puoi richiedere prenotazioni di capacità con data futura per i tipi di istanza appartenenti alle seguenti famiglie: C, G, I, M, R, T, U e X.
- Puoi richiedere prenotazioni di capacità con data futura per un numero di istanze con un minimo di 32 vCPU. Ad esempio, se richiedi una prenotazione della capacità con data futura per `m5.xlarge` istanze, devi richiedere una capacità di almeno 8 istanze (8 * m5.xlarge = 32 vCPU).
- Puoi richiedere una prenotazione della capacità con data futura con un anticipo compreso tra 5 e 120 giorni. Ti consigliamo di richiederlo con almeno 56 giorni (8 settimane) di anticipo per migliorare la supportabilità.
- La durata minima dell'impegno è di 14 giorni per le istanze C, G, I, M, R e T. Per le istanze U e X, la durata minima dell'impegno è di 12 settimane.

Console

Per creare una prenotazione della capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Prenotazioni della capacità, quindi Crea Prenotazione di capacità.
3. Configurare le seguenti impostazioni nella sezione Dettagli istanza.
    a. Tipo di istanza – Il tipo di istanza per il quale prenotare la capacità.
    b. Piattaforma – Il sistema operativo per le istanze. Per ulteriori informazioni, consulta Piattaforme supportate.
    c. Zona di disponibilità – La zona di disponibilità nella quale prenotare la capacità.
    d. Tenancy – Il tipo di tenancy da utilizzare per la capacità riservata. Scegli Predefinito per prenotare la capacità sull'hardware condiviso o Dedicato per prenotare la capacità sull'hardware dedicato al tuo account.

e. Numero totale di istanze – Il numero di istanze per cui si desidera prenotare la capacità. Se specifichi una quantità che supera la quota di On-Demand istanze rimanente per il tipo di istanza selezionato, la richiesta non va a buon fine.

4. Configurare le seguenti impostazioni nella sezione Reservation details (Dettagli prenotazione):

   a. La prenotazione della capacità inizia – Scegli In un momento specifico.

   b. Data di inizio – Specifica la data e l'ora in cui la prenotazione della capacità deve essere disponibile per l'uso. Per ulteriori informazioni, consulta Data e ora di inizio.

   c. Durata dell'impegno – Specifica la durata minima per la quale ti impegni a mantenere la prenotazione della capacità dopo che è stata consegnata. Per ulteriori informazioni, consulta Durata dell'impegno.

   d. Prenotazione della capacità termina – Scegliere una delle seguenti opzioni:

      - Quando la annullo – Prenota la capacità fino a quando viene annullata esplicitamente.
      - Ora specifica – Annullare la prenotazione della capacità automaticamente alla data e all'ora specificate.

5. Scegli Crea.

AWS CLI

Per creare una prenotazione della capacità

Utilizza il comando create-capacity-reservation.

```
aws ec2 create-capacity-reservation \
    --availability-zone az_name \
    --instance-type instance_type \
    --instance-count number_of_instances \
    --instance-platform operating_system \
    --instance-match-criteria targeted \
    --delivery-preference incremental \
    --commitment-duration commitment_in_seconds \
    --start-date YYYY-MMDDThh:mm:ss.sssZ
```

PowerShell

Per creare una prenotazione della capacità

Utilizza il cmdlet Add-EC2CapacityReservation.

```
Add-EC2CapacityReservation `
    -AvailabilityZone az_name `
    -InstanceType instance_type `
    -InstanceCount number_of_instances `
    -InstancePlatform operating_system `
    -InstanceMatchCriterion targeted `
    -DeliveryPreference incremental `
    -CommitmentDuration commitment_in_seconds `
    -StartDate  YYYY-MMDDThh:mm:ss.sssZ
```

Visualizza lo stato di una prenotazione della capacità

Amazon EC2 monitora costantemente lo stato delle prenotazioni della capacità.

A cautilizza del modello di consistenza eventuale seguito dall'API Amazon EC2, dopo aver creato una prenotazione della capacità, possono essere necessari fino a 5 minuti prima che lo stato della prenotazione della capacità rifletta che è `active`. Durante questo periodo, la prenotazione della capacità potrebbe rimanere nello stato `pending`. Tuttavia, potrebbe essere già disponibile per l'uso, nel qual caso i tentativi di avviare istanze nella prenotazione della capacità avrebbero esito positivo.

Console

Come visualizzare le prenotazioni della capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Seleziona la prenotazione della capacità.

AWS CLI

Per descrivere le prenotazioni della capacità

Utilizza il comando describe-capacity-reservations:

Ad esempio, il comando seguente descrive tutte le Prenotazioni di capacità.

```
aws ec2 describe-capacity-reservations
```

Di seguito è riportato un output di esempio.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1234abcd56EXAMPLE",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-16T09:03:18.000Z",
            "AvailableInstanceCount": 1,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 1,
            "State": "active",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "a1.medium",
            "PlacementGroupArn": "arn:aws:ec2:us-east-1:123456789012:placement-
group/MyPG"
        },
        {
            "CapacityReservationId": "cr-abcdEXAMPLE9876ef",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-07T11:34:19.000Z",
            "AvailableInstanceCount": 3,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 3,
            "State": "cancelled",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "m5.large"
        }
    ]
}
```

PowerShell

Per descrivere una prenotazione della capacità

Utilizza il cmdlet Get-EC2CapacityReservation.

```
Get-EC2CapacityReservation `
    -CapacityReservationId cr-1234abcd56EXAMPLE
```

Stato della prenotazione della capacità

Le prenotazioni della capacità possono trovarsi nei possibili stati elencati di seguito.

Stato	Description
`active`	– La capacità è disponibile per l'uso.
`expired`	La prenotazione della capacità è scaduta automaticamente alla data e ora specificate nella richiesta di prenotazione. La capacità riservata non è più disponibile per l'utilizzo.
`cancelled`	La Prenotazione della capacità è stata annullata. La capacità riservata non è più disponibile per l'utilizzo.
`pending`	La richiesta Prenotazione della capacità è stata completata, ma il provisioning della capacità è ancora in corso.
`failed`	La richiesta Prenotazione della capacità ha avuto esito negativo. Una richiesta potrebbe non riuscire a causa di parametri della richiesta non validi, limitazioni di capacità o vincoli al limite di istanze. È possibile visualizzare una richiesta non riuscita per 60 minuti.
`scheduled`	(Solo prenotazioni Future-dated di capacità) La richiesta di prenotazi one della capacità con data futura è stata approvata e la consegna della prenotazione della capacità è prevista per la data di inizio richiesta.
`assessing`	(Solo prenotazioni Future-dated di capacità) Amazon EC2 sta valutando la tua richiesta di prenotazione di capacità con data futura. Per ulteriori

Stato	Description
	informazioni, consulta Future-dated Valutazione della prenotazione della capacità.
`delayed`	(Solo prenotazioni Future-dated di capacità) Amazon EC2 ha riscontra to un ritardo nel provisioning della prenotazione di capacità richiesta con data futura. Amazon EC2 non è in grado di fornire la capacità richiesta entro la data e l'ora di inizio richieste.
`unsupported`	(Solo prenotazioni Future-dated di capacità) Amazon EC2 non è in grado di supportare la richiesta di prenotazione della capacità con data futura a causa di vincoli di capacità. Puoi visualizzare le richieste non supportate per 30 giorni. La prenotazione della capacità non verrà fornita.
`cancelling`	(Solo prenotazioni Future-dated di capacità) La prenotazione di capacità è stata annullata. La capacità è stata liberata, ma gli addebiti continuer anno fino alla fine del periodo di impegno ridotto. La prenotazione della capacità passa alla `cancelled` data di scadenza dell'impegno. Per ulteriori informazioni, consulta Spese di annullamento.

Avvio di istanze in una Prenotazione della capacità esistente

Puoi solo avviare un'istanza in una prenotazione della capacità che:

- Ha attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy)
- Ha una capacità disponibile sufficiente
- È nello stato `active`

Quando si avvia un'istanza, è possibile specificare se avviare l'istanza in qualsiasi Prenotazione della capacità `open`, in una specifica Prenotazione della capacità o in un gruppo di Prenotazioni di capacità.

In alternativa, è possibile configurare l'istanza in modo da evitare l'esecuzione in una Prenotazione della capacità, anche se si dispone di un Prenotazione della capacità `open` che ha attributi corrispondenti e capacità disponibile.

L'avvio di un'istanza in una Prenotazione della capacità ne riduce la capacità disponibile per il numero di istanze avviate. Ad esempio, se avvii tre istanze, la capacità disponibile della Prenotazione della capacità è ridotta di tre.

Console

Per avviare istanze in una prenotazione della capacità esistente

1. Segui la procedura per l'avvio di un'istanza, ma non avviare l'istanza finché non avrai completato i seguenti passaggi per specificare le impostazioni per il gruppo di posizionamento e la prenotazione della capacità.
2. Espandere Impostazioni avanzate ed eseguire le operazioni descritte di seguito:

   a. Per Gruppo di posizionamento, seleziona il gruppo di posizionamento cluster in cui avviare l'istanza.

   b. Per Capacity Reservation (Prenotazione della capacità), scegliere una delle seguenti opzioni a seconda della configurazione della prenotazione della capacità:

      - Nessuno – Impedisce l'avvio delle istanze in una Prenotazione della capacità. Le istanze sono esaurite. On-Demand
      - Apri – Avvia l'istanza in una qualsiasi Prenotazione della capacità che abbia attributi corrispondenti e capacità sufficiente per il numero di istanze selezionate. Se non esiste una prenotazione di capacità corrispondente a una capacità sufficiente, l'istanza utilizza la On-Demand capacità.
      - Specifica prenotazione della capacità – Avvia le istanze nella Prenotazione della capacità selezionata. Se questa Prenotazione della capacità non dispone di capacità sufficiente per il numero di istanze selezionate, l'avvio dell'istanza non riesce.
      - Specifica il gruppo di risorse per la prenotazione della capacità: avvia le istanze in qualsiasi prenotazione di capacità con attributi corrispondenti e capacità disponibile nel gruppo di prenotazione della capacità selezionato. Se il gruppo selezionato non dispone di una Capacity Reservation con attributi corrispondenti e capacità disponibile, le istanze vengono avviate al massimo della capacità. On-Demand
      - Specifica solo prenotazione della capacità – Avvia le istanze in una Prenotazione della capacità. Se non viene specificato un ID di prenotazione della capacità, le istanze si avviano in una prenotazione della capacità aperta. Se la capacità non è disponibile, le istanze non vengono avviate.

- Specifica solo il gruppo di risorse per la prenotazione della capacità: avvia le istanze in una prenotazione di capacità in un gruppo di risorse per la prenotazione della capacità. Se non viene specificato un ARN del Capacity Reservation Reservation Reservation Group, le istanze vengono avviate in un Capacity Reservation aperto. Se la capacità non è disponibile, le istanze non vengono avviate.

3. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza).

AWS CLI

Per avviare un'istanza in una prenotazione della capacità esistente

Utilizza il comando run-instances e specifica l'opzione `--capacity-reservation-specification`.

L'esempio seguente avvia un'istanza in qualsiasi prenotazione della capacità aperta che abbia attributi corrispondenti e capacità disponibile:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification CapacityReservationPreference=open
```

L'esempio seguente avvia un'istanza in una prenotazione della capacità `targeted`:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \
        CapacityReservationTarget={CapacityReservationId=cr-1234abcd56EXAMPLE}
```

L'esempio seguente avvia un'istanza nel gruppo prenotazione della capacità specificato:

```
aws ec2 run-instances \
```

```
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \

 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-2:123456789012:group/my-cr-group}
```

L'esempio seguente avvia un'istanza solo in una prenotazione della capacità. Poiché non specifica un ID di prenotazione della capacità, l'istanza viene avviata in qualsiasi prenotazione della capacità aperta con attributi corrispondenti e capacità disponibile:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \
        CapacityReservationPreference=capacity-reservations-only
```

L'esempio seguente avvia un'istanza solo in una prenotazione della capacità specifica. Se la capacità non è disponibile nella prenotazione della capacità specificata, l'istanza non viene avviata.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \
        CapacityReservationPreference=capacity-reservations-only \
        CapacityReservationTarget={CapacityReservationId=cr-1234abcd56EXAMPLE}
```

PowerShell

Per avviare un'istanza in una prenotazione della capacità esistente

Utilizza il cmdlet New-EC2Instance.

L'esempio seguente avvia un'istanza in qualsiasi prenotazione della capacità aperta che abbia attributi corrispondenti e capacità disponibile:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationSpecification_CapacityReservationPreference "open"
```

L'esempio seguente avvia un'istanza in una prenotazione della capacità `targeted`:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationTarget_CapacityReservationId cr-1234abcd56EXAMPLE
```

L'esempio seguente avvia un'istanza nel gruppo prenotazione della capacità specificato:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationTarget_CapacityReservationResourceGroupArn `
        "arn:aws:resource-groups:us-west-2:123456789012:group/my-cr-group"
```

L'esempio seguente avvia un'istanza solo in una prenotazione della capacità. Poiché non specifica un ID di prenotazione della capacità, l'istanza viene avviata in qualsiasi prenotazione della capacità aperta con attributi corrispondenti e capacità disponibile:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservations-only"
```

L'esempio seguente avvia un'istanza solo in una prenotazione della capacità specifica. Se la capacità non è disponibile nella prenotazione della capacità specificata, l'istanza non viene avviata.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservations-only" `
    -CapacityReservationTarget_CapacityReservationId cr-1234abcd56EXAMPLE
```

Modifica una prenotazione della capacità attiva

Se disponi di una prenotazione della capacità esistente che non è adatta al carico di lavoro che richiede tale capacità, puoi modificare la quantità, l'idoneità dell'istanza (`open` o `targeted`) e l'ora di fine (`At specific time` o `Manually`). Se specifichi una nuova quantità di istanze che supera il limite di On-Demand istanze rimanente per il tipo di istanza selezionato, l'aggiornamento non riesce.

Le modifiche consentite dipendono dallo stato della prenotazione della capacità:

- Stato `assessing` o `scheduled` – Puoi modificare solo i tag.
- Stato `pending`– Non puoi modificare in alcun modo la prenotazione della capacità.
- Stato `active` ma comunque entro la durata dell'impegno – Non puoi ridurre il numero di istanze al di sotto del conteggio delle istanze impegnate o impostare una data di fine precedente alla durata dell'impegno. Tutte le altre modifiche sono consentite.
- Stato `active` senza durata dell'impegno o durata dell'impegno trascorsa – Sono consentite tutte le modifiche.
- Stato `expired`, `cancelled`, `unsupported`, o `failed` – Non puoi modificare in alcun modo la prenotazione della capacità.

Considerazioni

- Non puoi modificare il tipo di istanza, la piattaforma, la zona di disponibilità o la tenancy dopo la creazione. Se devi modificare uno di questi attributi, ti consigliamo di annullare la prenotazione, quindi crearne una nuova con gli attributi richiesti.

- Se modifichi una prenotazione della capacità esistente modificando l'idoneità dell'istanza da `targeted` a `open`, tutte le istanze in esecuzione che corrispondono agli attributi della prenotazione della capacità, hanno il parametro `CapacityReservationPreference` impostato su `open` e non sono ancora in esecuzione in una prenotazione della capacità, utilizzeranno automaticamente la prenotazione della capacità modificata.
- Per modificare l'idoneità dell'istanza, la prenotazione della capacità deve essere completamente inattiva (utilizzo zero) perché Amazon EC2 non può modificare l'idoneità dell'istanza quando le istanze sono in esecuzione all'interno della prenotazione.

Console

Per modificare una prenotazione della capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Prenotazioni di capacità, selezionare la Prenotazione della capacità da modificare e selezionare Edit (Modifica).
3. Modifica le opzioni di Capacità totale, La prenotazione della capacità termina, o Idoneità dell'istanza secondo necessità e scegli Salva.

AWS CLI

Per modificare una prenotazione della capacità

Utilizza il comando modify-capacity-reservation. L'esempio seguente modifica la prenotazione della capacità specificata per riservare la capacità per otto istanze.

```
aws ec2 modify-capacity-reservation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --instance-count 8
```

PowerShell

Per modificare una prenotazione della capacità

Utilizza il cmdlet Edit-EC2CapacityReservation. L'esempio seguente modifica la prenotazione della capacità specificata per riservare la capacità per otto istanze.

```
Edit-EC2CapacityReservation `
    -CapacityReservationId cr-1234567890abcdef0 `
```

```
    -InstanceCount 8
```

Modifica le impostazioni di prenotazione della capacità della tua istanza

Puoi modificare le impostazioni Prenotazione della capacità seguenti per un'istanza arrestata in qualsiasi momento:

- Avviare su qualsiasi prenotazione della capacità che abbia attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy) e capacità disponibile.
- Avviare l'istanza in una Prenotazione della capacità specifica.
- Avviare in qualsiasi prenotazione della capacità che abbia attributi corrispondenti e capacità disponibile in un gruppo di prenotazione della capacità
- Impedire l'avvio dell'istanza in una Prenotazione della capacità.

Console

Per modificare le impostazioni della Prenotazione della capacità dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Instances (Istanze) e selezionare l'istanza da modificare. Arrestare l'istanza in errore, se non è già stata arrestata.
3. Scegliere Operazioni, Impostazioni istanza, Modifica impostazioni prenotazione della capacità.
4. Per Prenotazione della capacità, scegliere una delle seguenti opzioni:
   - Apri – Avvia l'istanza in una qualsiasi Prenotazione della capacità che abbia attributi corrispondenti e capacità sufficiente per il numero di istanze selezionate. Se non esiste una prenotazione di capacità corrispondente con una capacità sufficiente, l'istanza utilizza la On-Demand capacità.
   - Nessuno – Impedisce l'avvio delle istanze in una Prenotazione della capacità. La On-Demand capacità delle istanze è esaurita.
   - Specifica prenotazione della capacità – Avvia le istanze nella Prenotazione della capacità selezionata. Se questa Prenotazione della capacità non dispone di capacità sufficiente per il numero di istanze selezionate, l'avvio dell'istanza non riesce.
   - Specifica gruppo Prenotazione capacità – Avvia le istanze in qualsiasi Prenotazione della capacità con attributi corrispondenti e capacità disponibile nel gruppo di — selezionato.

Se il gruppo selezionato non dispone di una prenotazione di capacità con attributi corrispondenti e capacità disponibile, le istanze vengono On-Demand avviate al massimo della capacità.

- Specifica solo prenotazione della capacità – Avvia le istanze in una Prenotazione della capacità. Se non viene specificato un ID di prenotazione della capacità, le istanze si avviano in una prenotazione della capacità aperta. Se la capacità non è disponibile, le istanze non vengono avviate.
- Specifica solo il gruppo di risorse per la prenotazione della capacità: avvia le istanze in una prenotazione di capacità in un gruppo di risorse per la prenotazione della capacità. Se non viene specificato un ARN del Capacity Reservation Reservation Reservation Group, le istanze vengono avviate in un Capacity Reservation aperto. Se la capacità non è disponibile, le istanze non vengono avviate.

AWS CLI

Per modificare le impostazioni della Prenotazione della capacità dell'istanza

Utilizza il comando modify-instance-capacity-reservation-attributes:

L'esempio seguente modifica la preferenza di prenotazione della capacità in none.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification CapacityReservationPreference=none
```

L'esempio seguente indica l'obiettivo di una prenotazione della capacità specifica.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification \
    CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

L'esempio seguente modifica la destinazione in un gruppo di prenotazione della capacità specifico.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification \
```

```
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-2:123456789012:group/my-cr-group}
```

L'esempio seguente modifica la preferenza di prenotazione della capacità in `capacity-reservation-only`. Poiché non specifica una prenotazione della capacità, le istanze vengono avviate in qualsiasi prenotazione della capacità aperta con attributi corrispondenti e capacità disponibile.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification CapacityReservationPreference=capacity-
reservation-only
```

Il seguente esempio modifica l'impostazione delle preferenze relative alla prenotazione della capacità impostandola su `capacity-reservation-only`. Se la capacità non è disponibile nella prenotazione della capacità specificata, le istanze non verranno avviate.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification \
        CapacityReservationPreference=capacity-reservation-only \
        CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

PowerShell

Per modificare le impostazioni della Prenotazione della capacità dell'istanza

Utilizza il cmdlet Edit-EC2InstanceCapacityReservationAttribute.

L'esempio seguente modifica la preferenza di prenotazione della capacità in `none`.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationSpecification_CapacityReservationPreference "none"
```

L'esempio seguente indica l'obiettivo di una prenotazione della capacità specifica.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
```

```
    -CapacityReservationTarget_CapacityReservationId cr-1234567890abcdef0
```

L'esempio seguente modifica la destinazione in un gruppo di prenotazione della capacità specifico.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationTarget_CapacityReservationResourceGroupArn `
        "arn:aws:resource-groups:us-west-2:123456789012:group/my-cr-group"
```

L'esempio seguente modifica la preferenza di prenotazione della capacità in `capacity-reservation-only`. Poiché non specifica una prenotazione della capacità, le istanze vengono avviate in qualsiasi prenotazione della capacità aperta con attributi corrispondenti e capacità disponibile.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservation-only"
```

Il seguente esempio modifica l'impostazione delle preferenze relative alla prenotazione della capacità impostandola su `capacity-reservation-only`. Se la capacità non è disponibile nella prenotazione della capacità specificata, le istanze non verranno avviate.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservation-only" `
    -CapacityReservationTarget_CapacityReservationId cr-1234567890abcdef0
```

Spostare la capacità tra le prenotazioni della capacità

Puoi spostare la capacità da una prenotazione della capacità all'altra per ridistribuire le risorse di elaborazione prenotate in base alle esigenze. Ad esempio, se hai bisogno di capacità aggiuntiva in una prenotazione con un utilizzo crescente e hai capacità disponibile in un'altra prenotazione, puoi ridistribuire tale capacità tra le due prenotazioni.

Prerequisiti per spostare la capacità

Come prerequisito, le due prenotazioni della capacità devono soddisfare i seguenti requisiti:

- Entrambe le prenotazioni devono essere nello stato attivo.
- Entrambe le prenotazioni devono essere di proprietà del tuo. Account AWS Non puoi spostare la capacità tra prenotazioni della proprietà di Account AWS diversi.
- Entrambe le prenotazioni devono condividere le seguenti informazioni:
  - Tipo di istanza
  - Platform (Piattaforma)
  - Zona di disponibilità
  - Tenancy
  - Gruppo di posizionamento
  - Ora di fine

L'idoneità (`open` o `targeted`) dell'istanza di prenotazione della capacità di destinazione e i tag non devono necessariamente corrispondere alla prenotazione di origine. La configurazione di entrambe le prenotazioni rimane la stessa, tranne per il fatto che la prenotazione di origine ha una capacità ridotta e la prenotazione di destinazione ha una capacità maggiore.

Quando specifichi la quantità di istanze da spostare, per impostazione predefinita, viene spostata per prima qualsiasi capacità disponibile, seguita da tutte le istanze idonee in esecuzione (la capacità utilizzata nella prenotazione). Ad esempio, se sposti 4 istanze da una prenotazione con 5 istanze usate e 3 istanze disponibili, verranno spostate le 3 istanze disponibili e 1 istanza usata.

> **Note**
>
> Quando sposti la capacità usata dalla prenotazione specificando una Quantità da spostare superiore alla capacità disponibile, verranno spostate solo le istanze avviate con la relativa Specifica di prenotazione della capacità come `open`.

Considerazioni

Le seguenti considerazioni si applicano quando si sposta la capacità da una prenotazione a un'altra:

- La capacità utilizzata può essere spostata solo tra le prenotazioni della capacità con idoneità dell'istanza `open` che sono condivise con lo stesso insieme di account.
- Quando sposti la capacità utilizzata, le istanze idonee vengono selezionate casualmente. Non puoi specificare quali istanze in esecuzione vengono spostate. Se non si trova un numero sufficiente

di istanze idonee per soddisfare la quantità da spostare, l'operazione di spostamento avrà esito negativo.

- Se sposti tutta la capacità dalla prenotazione di origine, la prenotazione della capacità verrà annullata automaticamente.
- Future-dated Prenotazioni di capacità: non è possibile spostare la capacità per una prenotazione di capacità con data futura durante il periodo dell'impegno.

> **Note**
>
> Lo spostamento della capacità da un blocco di capacità non è supportato.

Spostare la capacità

Puoi spostare la capacità da una prenotazione della capacità di origine a una prenotazione della capacità di destinazione.

Console

Per spostare la capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione sinistro, seleziona Prenotazioni della capacità.
3. Seleziona un ID On-Demand di prenotazione della capacità con capacità di spostamento.
4. In Operazioni, Gestisci capacità, scegli Sposta.
5. Nella pagina Sposta capacità, in Prenotazione della capacità di destinazione, seleziona una prenotazione dall'elenco.
6. In Quantità da spostare, utilizza il cursore o digita il numero di istanze da spostare dalla prenotazione della capacità di origine alla prenotazione della capacità di destinazione.
7. Controlla il riepilogo e, quando sei pronto, scegli Sposta.

AWS CLI

Per spostare la capacità

Utilizza il comando move-capacity-reservation-instances. L'esempio seguente sposta 10 istanze dalla prenotazione della capacità di origine specificata alla prenotazione della capacità di destinazione specificata.

```
aws ec2 move-capacity-reservation-instances \
    --source-capacity-reservation-id cr-1234567890abcdef0 \
    --destination-capacity-reservation-id cr-021345abcdef56789 \
    --instance-count 10
```

PowerShell

Per spostare la capacità

Utilizza il cmdlet Move-EC2CapacityReservationInstance. L'esempio seguente sposta 10 istanze dalla prenotazione della capacità di origine specificata alla prenotazione della capacità di destinazione specificata.

```
Move-EC2CapacityReservationInstance `
    -SourceCapacityReservationId cr-1234567890abcdef0 `
    -DestinationCapacityReservationId cr-021345abcdef56789 `
    -InstanceCount 10
```

Suddivisione della capacità da una prenotazione della capacità esistente

Puoi suddividere la capacità da una prenotazione della capacità esistente e creare una nuova prenotazione. Suddividendo la capacità, si assegna una parte della prenotazione originale a un carico di lavoro specifico o la si condivide con un altro Account AWS. Ad esempio, per condividere parzialmente una prenotazione della capacità con un altro account, puoi suddividere parte della capacità per creare una prenotazione della capacità di dimensioni minori. La prenotazione della capacità di dimensioni minori può quindi essere condivisa con gli altri account usando AWS Resource Access Manager.

Quando si suddivide la capacità da una prenotazione della capacità esistente, viene creata automaticamente una nuova prenotazione della capacità. La prenotazione esistente rimarrà invariata, tranne che per la capacità totale ridotta rispetto al numero di istanze suddivise. Le istanze in esecuzione nella prenotazione della capacità esistente non sono interessate. Puoi suddividere la prenotazione esistente in una sola nuova prenotazione della capacità.

La nuova prenotazione della capacità avrà la stessa configurazione della prenotazione della capacità esistente, ad eccezione dei tag. Per impostazione predefinita, la nuova prenotazione della

capacità non ha alcun tag. Puoi specificare nuovi tag durante l'operazione di suddivisione. La nuova prenotazione della capacità può essere modificata anche dopo la creazione, se necessario.

Quando specifichi la quantità di istanze da suddividere, per impostazione predefinita, viene suddivisa per prima qualsiasi capacità disponibile, seguita da tutte le istanze idonee in esecuzione (la capacità utilizzata nella prenotazione). Ad esempio, se suddividi 4 istanze da una prenotazione della capacità con 5 istanze usate e 3 istanze disponibili, le 3 istanze disponibili e 1 istanza usata verranno suddivise in una nuova prenotazione.

Prerequisiti per suddividere la capacità

Come prerequisito, la prenotazione della capacità deve soddisfare i seguenti requisiti:

- La prenotazione di origine deve essere nello stato attivo.
- La prenotazione di origine deve essere di proprietà del tuo Account AWS.

> **Note**
>
> Quando suddividi la capacità usata dalla prenotazione specificando una Quantità da suddividere superiore alla capacità disponibile, verranno suddivise solo le istanze avviate con la relativa Specifica di prenotazione della capacità come `open`.

Considerazioni

Le seguenti considerazioni si applicano quando si suddivide la capacità da una prenotazione a una nuova prenotazione:

- La capacità utilizzata può essere suddivisa solo per le prenotazioni di capacità con idoneità all'istanza «aperta» e non condivise con nessun account.
- Quando suddividi la capacità utilizzata, le istanze idonee vengono selezionate casualmente. Non puoi specificare quali istanze in esecuzione vengono suddivise. Se non si trova un numero sufficiente di istanze idonee per soddisfare la quantità da suddividere, l'operazione di suddivisione avrà esito negativo.
- La quantità massima di istanze da suddividere da una prenotazione esistente corrisponde alla dimensione della prenotazione meno una. Ad esempio, se la capacità totale della tua prenotazione è di 5 istanze, puoi suddividere un massimo di 4 istanze in una nuova prenotazione.

- Future-dated Prenotazioni di capacità: non è possibile suddividere la capacità per una prenotazione di capacità con data futura durante il periodo di impegno.
- Gruppi di risorse per la prenotazione della capacità: se la prenotazione di capacità esistente appartiene a un gruppo di risorse per la prenotazione della capacità, la nuova prenotazione di capacità non verrà aggiunta automaticamente al gruppo di risorse per la prenotazione della capacità. È possibile aggiungere il nuovo Capacity Reservation a un gruppo di risorse di Capacity Reservation dopo la sua creazione, se necessario.
- Condivisione – Se la prenotazione della capacità esistente viene condivisa con un account consumatore, la nuova prenotazione della capacità non verrà condivisa automaticamente con l'account consumatore. Se necessario, puoi condividere la nuova prenotazione della capacità dopo la sua creazione.
- Gruppo di posizionamento cluster – Se la prenotazione della capacità esistente fa parte di un gruppo di posizionamento cluster, la nuova prenotazione della capacità verrà creata nello stesso gruppo di posizionamento cluster.

> **Note**
>
> La suddivisione della capacità da un blocco di capacità non è supportato.

Controlla l'accesso per suddividere le prenotazioni della capacità utilizzando i tag

Puoi utilizzare i tag per controllare l'accesso alle risorse Amazon EC2, inclusa la suddivisione della capacità da una prenotazione della capacità esistente per creare una nuova prenotazione della capacità. Per ulteriori informazioni, consulta Controllare l'accesso alle AWS risorse tramite tag nella IAM User Guide.

Per controllare l'accesso alla suddivisione di una prenotazione della capacità utilizzando i tag, assicurati di specificare sia i tag di risorsa che quelli di richiesta nella dichiarazione di policy, perché le policy IAM vengono valutate sia rispetto alla prenotazione della capacità di origine che alla prenotazione della capacità appena creata. La seguente policy di esempio include la chiave di condizione `ec2:ResourceTag` con il tag `Owner=ExampleDepartment1` per la prenotazione della capacità di origine e la chiave di condizione `ec2:RequestTag` con il tag `stack=production` per la prenotazione della capacità appena creata.

```
{
```

```
  "Statement": [
    {
      "Sid": "AllowSourceCapacityReservation",
      "Effect": "Allow",
      "Action": "ec2:CreateCapacityReservationBySplitting",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:capacity-reservation/
cr-1234567890abcdef0",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Owner": "ExampleDepartment1"
        }
      }
    },
    {
      "Sid": "AllowNewlyCreatedCapacityReservation",
      "Effect": "Allow",
      "Action": ["ec2:CreateCapacityReservationBySplitting", "ec2:CreateTags"],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:capacity-reservation/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/stack": "production"
        }
      }
    }
  ]
}
```

Suddivisione della capacità

Puoi suddividere la capacità da una prenotazione della capacità esistente e creare una nuova prenotazione della capacità.

Console

Per suddividere la capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione sinistro, seleziona Prenotazioni della capacità.
3. Seleziona un On-Demand Capacity Reservation ID con capacità di frazionamento.
4. In Operazioni, Gestisci capacità, scegli Suddividi.

5. Nella pagina Suddividi prenotazione della capacità, in Quantità da suddividere, usa il cursore o digita il numero di istanze da suddividere dalla prenotazione attuale.
6. (Opzionale) Aggiungi dei tag per la nuova prenotazione della capacità.
7. Controlla il riepilogo e, quando sei pronto, scegli Suddividi.

AWS CLI

Per suddividere la capacità

Utilizza il comando `create-capacity-reservation-by-splitting`. L'esempio seguente crea una nuova prenotazione della capacità suddividendo 10 istanze dalla prenotazione della capacità specificata.

```
aws ec2 create-capacity-reservation-by-splitting \
    --source-capacity-reservation-id cr-1234567890abdef0 \
    --instance-count 10
```

PowerShell

Per suddividere la capacità

Utilizza il cmdlet New-EC2CapacityReservationBySplitting. L'esempio seguente crea una nuova prenotazione della capacità suddividendo 10 istanze dalla prenotazione della capacità specificata.

```
New-EC2CapacityReservationBySplitting `
    -SourceCapacityReservationId cr-1234567890abdef0 `
    -InstanceCount 10
```

Annullamento di una Prenotazione della capacità

Puoi annullare una prenotazione della capacità che è in uno dei seguenti stati:

- `assessing`
- `scheduled`
- `active`
- `delayed`

> **Note**
>
> Non puoi annullare o modificare un blocco di capacità. Per ulteriori informazioni, consulta Blocchi di capacità per ML.

Se la Capacity Reservation è `active` priva di impegno o ha una durata di impegno scaduta, la cancellazione è gratuita.

Se la prenotazione della capacità è `assessing` o `delayed`, la cancellazione è gratuita.

Se la Capacity Reservation è valida `scheduled` o `active` prevede la durata residua dell'impegno, potrebbe essere applicata una penale di cancellazione. Per ulteriori informazioni, consulta Spese di annullamento.

Se annulli una Capacity Reservation con istanze in esecuzione, le istanze continuano a funzionare normalmente al di fuori della Capacity Reservation alle tariffe standard o a una tariffa scontata se disponi di un piano di risparmio o di un' On-Demand istanza riservata regionale corrispondenti.

Dopo l'annullamento di una Prenotazione della capacità, le istanze che la puntano non possono più avviare. Modifica queste istanze in modo che puntino a una Prenotazione della capacità diversa, vengano avviate in una qualsiasi Prenotazione della capacità aperta con attributi corrispondenti e capacità sufficiente oppure evita di avviare in una Prenotazione della capacità. Per ulteriori informazioni, consulta Modifica le impostazioni di prenotazione della capacità della tua istanza.

Argomenti

- Spese di annullamento
- Preventivo di cancellazione
- Annullamento di una Prenotazione della capacità

Spese di annullamento

Se annulli una prenotazione di capacità con data futura entro 8 settimane dalla data di inizio o durante la durata dell'impegno dopo la consegna, ti verrà addebitata una percentuale della durata dell'impegno. La capacità viene liberata non appena effettui l'annullamento, ma la prenotazione continua a essere fatturata alla On-Demand tariffa prevista fino alla fine del periodo di impegno ridotto. Se disponi di un piano di risparmio o di un'istanza riservata regionale corrispondente, la tariffa scontata si applica automaticamente.

Per calcolare l'addebito, Amazon EC2 moltiplica la durata dell'impegno per un tasso di annullamento. Quanto prima si effettua l'annullamento rispetto alla data di inizio, tanto più bassa è la tariffa. La tabella seguente mostra le percentuali di cancellazione.

Tariffe di cancellazione

Quando si annulla	Percentuale minima di cancellazione
8 o più settimane prima della data di inizio originale	Nessun addebito
da 2 a 8 settimane prima della data di inizio originale	25% dell'impegno totale
Entro 2 settimane dalla data di inizio originale	50% dell'impegno totale
Dopo la consegna, durante la durata dell'impegno	50% dell'impegno residuo

Questa tabella fornisce indicazioni generali sulle spese di annullamento. Il preventivo di cancellazione determina la durata esatta delle spese di annullamento.

Ad esempio, se disponi di una prenotazione di `c8g.xlarge` capacità di 70 istanze con un impegno della durata di 14 giorni e effettui la cancellazione entro 2 settimane dalla data di inizio originale (percentuale di annullamento del 50%), ti verranno addebitati 7 giorni di impegno. Durante questi 7 giorni, paghi 70 istanze alla stessa tariffa. On-Demand

Quando ti viene addebitato il costo della cancellazione:

- La Capacity Reservation entra nello `cancelling` stato.
- La prenotazione della capacità non può essere modificata, spostata, condivisa o divisa.
- La prenotazione della capacità rimane visibile nella console e nelle `DescribeCapacityReservations` risposte.
- La prenotazione della capacità passa a `cancelled` quando termina l'impegno.

Per sapere quando scadono le spese di annullamento, usa il comando describe-capacity-reservations e controlla il campo nella risposta. `CommitmentInfo.CommitmentEndDate` Gli addebiti si interrompono quando l'impegno termina e la prenotazione della capacità passa a.

`cancelled` Per informazioni su come vengono visualizzate le spese di annullamento nel Rapporto AWS sui costi e l'utilizzo 2.0, vedereSpese di annullamento nel Rapporto sui costi e sull'utilizzo 2.0.

Se la Capacity Reservation ha una durata residua dell'impegno, non puoi annullarla mentre le istanze sono ancora in corso. Devi prima interrompere o terminare le istanze in esecuzione, in modo da evitare di incorrere contemporaneamente in costi di annullamento e addebiti per le On-Demand istanze.

Per cancellare una Capacity Reservation con una penale di cancellazione, devi prima generare un preventivo di cancellazione e accettarne i termini. Per ulteriori informazioni, consulta Preventivo di cancellazione.

Preventivo di cancellazione

Quando una cancellazione richiede un addebito, è necessario rivedere e accettare un preventivo di cancellazione prima di procedere. Il preventivo fornisce i termini di cancellazione esatti, inclusi i seguenti dettagli:

- L'attuale configurazione della prenotazione della capacità
- Lo stato a cui passa la Capacity Reservation dopo l'annullamento () `cancelling`
- Il conteggio delle istanze confermate a cui si applica l'addebito
- La durata dell'addebito
- La data di scadenza dell'addebito (quando l'impegno termina e la prenotazione della capacità passa `acancelled`)

Dopo aver esaminato i termini, confermi l'annullamento accettando il preventivo.

Nella console Amazon EC2, il preventivo viene generato automaticamente quando si avvia un annullamento. Puoi rivedere i termini e confermare direttamente la tua accettazione. Con l'API AWS CLI o, utilizzalo `CreateCapacityReservationCancellationQuote` per generare il preventivo, quindi passa l'ID del preventivo a`CancelCapacityReservation`.

Il preventivo di cancellazione è valido per 24 ore. Dopo 24 ore, è necessario generare un nuovo preventivo. Per visualizzare i preventivi di annullamento esistenti, utilizza`DescribeCapacityReservationCancellationQuotes`.

> **Important**
>
> L'annullamento è irreversibile. Dopo aver accettato un preventivo di cancellazione e annullato una prenotazione di capacità, non è possibile annullare la cancellazione.

Annullamento di una Prenotazione della capacità

Utilizza le seguenti procedure per annullare una prenotazione di capacità.

Console

Per annullare una prenotazione della capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Prenotazioni di capacità e selezionare Prenotazione della capacità per annullare.
3. Scegli Annulla prenotazione.
4. Se è richiesto un preventivo di cancellazione, consulta i termini di cancellazione, inclusa la durata dell'addebito e la data di fine dell'addebito. Inserisci **`confirm`** per accettare i termini.
5. Scegli Annulla prenotazione.

AWS CLI

Per annullare una prenotazione della capacità

Utilizza il comando cancel-capacity-reservation.

```
aws ec2 cancel-capacity-reservation \
    --capacity-reservation-id cr-1234567890abcdef0
```

Se è richiesto un preventivo di annullamento, genera prima il preventivo utilizzando create-capacity-reservation-cancellation-quote, quindi passa l'ID del preventivo al comando di annullamento.

```
aws ec2 create-capacity-reservation-cancellation-quote \
    --capacity-reservation-id cr-1234567890abcdef0
```

`CancellationTermsChargeCommitmentDurationHoursChargeEndDate`Rivedi nella risposta, inclusi e. Quindi annulla con l'ID del preventivo:

```
aws ec2 cancel-capacity-reservation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --quote-id crcq-1a2b3c4d5e6f7g8h9 \
    --apply-cancellation-charges commitment-wind-down
```

PowerShell

Per annullare una prenotazione della capacità

Utilizza il cmdlet Remove-EC2CapacityReservation.

```
Remove-EC2CapacityReservation `
    -CapacityReservationId cr-1234567890abcdef0
```

Se è richiesto un preventivo di annullamento, genera prima il preventivo utilizzando New-EC2CapacityReservationCancellationQuote, quindi passa l'ID del preventivo al cmdlet cancel.

```
New-EC2CapacityReservationCancellationQuote `
    -CapacityReservationId cr-1234567890abcdef0
```

Rivedi i termini di annullamento nella risposta. Quindi annulla con l'ID del preventivo:

```
Remove-EC2CapacityReservation `
    -CapacityReservationId cr-1234567890abcdef0 `
    -QuoteId crcq-1a2b3c4d5e6f7g8h9 `
    -ApplyCancellationCharge "commitment-wind-down"
```

Utilizza Capacity Reservations con gruppi di collocamento

Puoi creare prenotazioni di capacità in un gruppo di collocamento per riservare la capacità di calcolo di Amazon EC2 per i tuoi carichi di lavoro.

La creazione di una prenotazione di capacità in un gruppo di collocamento garantisce l'accesso alla capacità di calcolo dei gruppi di collocamento quando ne hai bisogno, per tutto il tempo necessario. Ciò consente di ridimensionare la capacità assicurando al contempo che la capacità rimanga disponibile per l'uso, in modo da poterla ridimensionare quando necessario.

Dopo aver creato una prenotazione di capacità in un gruppo di collocamento, puoi condividerla con altri AWS account. Per ulteriori informazioni, consulta Condivisione delle prenotazioni di capacità nei gruppi di collocamento.

Strategie di posizionamento supportate

È possibile creare prenotazioni di capacità in gruppi di collocamento che utilizzano le seguenti strategie:

- Cluster
- Tempo di precisione

> **Note**
>
> I gruppi di collocamento Spread e Partition non supportano le prenotazioni di capacità. I Capacity Blocks non supportano i gruppi di collocamento.

Per informazioni sui tipi di istanze supportati, sulle regioni disponibili e sulle strategie di posizionamento, consultaGruppi di collocamento per le tue istanze Amazon EC2.

Argomenti

- Limitazioni
- Lavora con Capacity Reservations nei gruppi di collocamento
- Condivisione delle prenotazioni di capacità nei gruppi di collocamento

Limitazioni

Quando crei le prenotazioni di capacità nei gruppi di collocamento, tieni presente quanto segue:

- Se una prenotazione della capacità esistente non si trova in un gruppo di posizionamento, non puoi modificare la prenotazione della capacità per prenotare capacità in un gruppo di posizionamento. Per prenotare la capacità in un gruppo di collocazione, è necessario creare la Prenotazione della capacità nel gruppo di collocazione.
- Dopo aver creato una prenotazione della capacità in un gruppo di collocazione, non è possibile modificarla per prenotare la capacità al di fuori del gruppo di collocazione.
- È possibile aumentare la capacità riservata in un gruppo di collocazione modificando una prenotazione della capacità esistente nel gruppo di collocazione o creando prenotazioni della capacità aggiuntive nel gruppo di collocazione. Tuttavia, si aumentano le possibilità di ottenere un errore di capacità insufficiente.

- Puoi condividere le prenotazioni di capacità solo dal gruppo di collocamento di cui sei proprietario. Non puoi condividere le prenotazioni di capacità di un gruppo di collocamento di cui non sei proprietario.
- Non puoi eliminare un gruppo di collocamento con `active` Capacity Reservations. È necessario annullare tutte le prenotazioni di capacità presenti nel gruppo di collocamento prima di poterle eliminare.

Lavora con Capacity Reservations nei gruppi di collocamento

Per iniziare a utilizzare Capacity Reservations con i gruppi di collocamento, procedi nel seguente modo.

> **Note**
>
> Se desideri creare una prenotazione di capacità in un gruppo di collocamento esistente, salta il passaggio 1. Quindi, per i passaggi 2 e 3, specifica l'ARN del gruppo di collocamento esistente.

Processi

- Fase 1: (CondizionaleCrea un gruppo di collocamento da utilizzare con una prenotazione di capacità
- Fase 2: Creare una prenotazione di capacità in un gruppo di collocamento
- Fase 3: Avvia le istanze in Capacity Reservations in un gruppo di collocamento

Fase 1: (CondizionaleCrea un gruppo di collocamento da utilizzare con una prenotazione di capacità

Eseguite questo passaggio solo se avete bisogno di creare un nuovo gruppo di collocamento. Per utilizzare un gruppo di collocamento esistente, salta questo passaggio e poi, per i passaggi 2 e 3, utilizza l'ARN di quel gruppo di collocamento.

Console

Come creare un gruppo di posizionamento

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, scegliere Placement Groups (Gruppi di collocazione), quindi Create Placement Group (Crea gruppo di collocazione).
3. Per Name (Nome), specificare un nome descrittivo per il gruppo di collocazione.
4. Per Strategia di collocamento, scegli la strategia di posizionamento.
5. Seleziona Crea gruppo.
6. Nella tabella Gruppi di collocamento, nella colonna ARN del gruppo, annota l'ARN del gruppo di collocamento che hai creato. Servirà per la fase successiva.

AWS CLI

Come creare un gruppo di posizionamento

Utilizzare il comando create-placement-group.

```
aws ec2 create-placement-group \
    --group-name MyPG \
    --strategy strategy
```

Prendi nota del gruppo di posizionamento ARN restituito nell'output, perché ti servirà per il passaggio successivo.

PowerShell

Come creare un gruppo di posizionamento

Utilizza il cmdlet New-EC2PlacementGroup.

```
New-EC2PlacementGroup `
    -GroupName my-placement-group `
    -Strategy strategy
```

Prendi nota del gruppo di posizionamento ARN restituito nell'output, perché ti servirà per il passaggio successivo.

Fase 2: Creare una prenotazione di capacità in un gruppo di collocamento

Crei una prenotazione di capacità in un gruppo di collocamento nello stesso modo in cui crei qualsiasi prenotazione di capacità. Tuttavia, è necessario specificare anche l'ARN del gruppo di collocamento in cui creare la prenotazione di capacità.

Considerazioni

- Il gruppo di collocamento specificato deve trovarsi nello `available` stato. Se il gruppo di collocamento è nello `deleted` stato `pendingdeleting`, o, la richiesta ha esito negativo.
- La prenotazione della capacità e il gruppo di collocamento devono trovarsi nella stessa zona di disponibilità. Se la richiesta di creazione della prenotazione di capacità specifica una zona di disponibilità diversa da quella del gruppo di collocamento, la richiesta ha esito negativo.
- È possibile creare prenotazioni di capacità solo per i tipi di istanza supportati dai gruppi di collocamento. Se si specifica un tipo di istanza non supportato, la richiesta avrà un esito negativo.
- Se si crea una `open` Capacity Reservation in un gruppo di collocamento e sono presenti istanze in esecuzione con attributi corrispondenti (ARN del gruppo di collocamento, tipo di istanza, zona di disponibilità, piattaforma e tenancy), tali istanze vengono eseguite automaticamente nella Capacity Reservation.
- La richiesta di creare una Prenotazione della capacità ha esito negativo se una delle seguenti condizioni è true:
  - Amazon EC2 non dispone di capacità sufficiente per soddisfare la richiesta. Provare in un momento successivo, provare una zona di disponibilità differente o provare una capacità inferiore. Se l'applicazione è flessibile su più tipi di istanza e dimensioni, provare con attributi di istanza differenti.
  - La quantità richiesta supera il limite di istanze per la famiglia di On-Demand istanze selezionata. Aumenta il limite di On-Demand istanze per la famiglia di istanze e riprova. Per ulteriori informazioni, consulta Quote di istanze on demand.

Console

Per creare una prenotazione della capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Prenotazioni della capacità, quindi Crea Prenotazione di capacità.
3. Nella pagina Crea una prenotazione della capacità, specifica il tipo di istanza, la piattaforma, la zona di disponibilità, la tenancy, la quantità e la data di fine in base alle tue esigenze.
4. Per il gruppo di collocamento, seleziona l'ARN del gruppo di collocamento in cui creare la prenotazione di capacità.
5. Scegli Create (Crea).

Per ulteriori informazioni, consulta Creazione di una Prenotazione della capacità.

AWS CLI

Per creare una prenotazione della capacità

Utilizza il comando create-capacity-reservation. Per `--placement-group-arn`, specificate l'ARN del gruppo di collocamento in cui creare la Capacity Reservation.

```
aws ec2 create-capacity-reservation \
    --instance-type instance_type \
    --instance-platform platform \
    --availability-zone-id az_id \
    --instance-count quantity \
    --placement-group-arn "placement_group_arn"
```

PowerShell

Per creare una prenotazione della capacità

Utilizza il cmdlet Add-EC2CapacityReservation. Per `-PlacementGroupArn`, specifica l'ARN del gruppo di collocamento in cui creare la prenotazione di capacità.

```
Add-EC2CapacityReservation `
    -InstanceType instance_type `
    -InstancePlatform platform `
    -AvailabilityZoneId az_id `
    -InstanceCount quantity `
    -PlacementGroupArn "placement_group_arn"
```

Fase 3: Avvia le istanze in Capacity Reservations in un gruppo di collocamento

Puoi avviare un'istanza in una Capacity Reservation che si trova in un gruppo di collocamento con una delle seguenti opzioni:

- Specificare l'ARN del gruppo di collocamento in cui avviare l'istanza: quando fornisci l'ARN di un gruppo di collocamento, Amazon EC2 avvia l'istanza in quel gruppo di collocamento. È possibile utilizzare uno dei seguenti metodi:
  - Specificare *open*: non è necessario specificare la prenotazione della capacità nella richiesta di avvio istanza. Se l'istanza ha attributi (gruppo di collocazione ARN, tipo di istanza, zona di disponibilità, piattaforma e tenancy) che corrispondono a un prenotazione della capacità in un

specifico gruppo di collocazione, l'istanza viene eseguita automaticamente nella prenotazione della capacità.

- Specificazione di una prenotazione di capacità: se la prenotazione della capacità accetta solo lanci di istanze mirati, è necessario specificare la prenotazione di capacità di destinazione in aggiunta al gruppo di collocamento nella richiesta.
- Specificazione di un gruppo di prenotazione di capacità: per ulteriori informazioni, vedere Utilizzo di Capacity Reservation in gruppi di collocamento con un gruppo di prenotazione di capacità.

- Specificare solo un gruppo di prenotazione di capacità: per ulteriori informazioni, vedere Utilizzo di Capacity Reservation nei gruppi di collocamento con un gruppo di prenotazione di capacità.
- Specificare solo una prenotazione di capacità: è possibile avviare le istanze in una prenotazione di capacità in un gruppo di collocamento.

> **Note**
>
> Quando si avviano le istanze specificando solo una Capacity Reservation o solo un gruppo Capacity Reservation, le istanze vengono avviate nelle Capacity Reservations create nel gruppo di collocamento, ma le istanze non sono direttamente collegate al gruppo di collocamento.

Console

Per avviare istanze in una prenotazione della capacità esistente

1. Segui la procedura per l'avvio di un'istanza, ma non avviare l'istanza finché non avrai completato i seguenti passaggi per specificare le impostazioni per il gruppo di posizionamento e la prenotazione della capacità.
2. Espandere Impostazioni avanzate ed eseguire le operazioni descritte di seguito:
   a. Per il gruppo di collocamento, selezionate il gruppo di collocamento in cui avviare l'istanza.
   b. Per Capacity Reservation (Prenotazione della capacità), scegliere una delle seguenti opzioni a seconda della configurazione della prenotazione della capacità:
      - Apri: per avviare le istanze in qualsiasi riserva open di capacità del gruppo di collocamento con attributi corrispondenti e capacità sufficiente.

- Destinazione con ID – Per avviare le istanze in una prenotazione della capacità che accetta solo avvii di istanze con destinazione.
- Destinazione con gruppo – Per avviare le istanze in qualsiasi prenotazione della capacità con attributi corrispondenti e capacità disponibile nel gruppo della prenotazione della capacità selezionato.

3. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

AWS CLI

Per avviare istanze in una prenotazione della capacità esistente

Utilizzare il comando run-instances. Se è necessario indirizzare una prenotazione della capacità specifica o un gruppo di prenotazione della capacità specifico, specificare il parametro `--capacity-reservation-specification`. Per `--placement`, specificare il parametro `GroupName` e quindi specificare il nome del gruppo di collocazione creato nelle fasi precedenti.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count quantity \
    --instance-type instance_type \
    --key-name key_pair_name \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_reservation_id} \
    --placement "GroupName=placement_group_name"
```

PowerShell

Per avviare istanze in una prenotazione della capacità esistente

Utilizza il cmdlet New-EC2Instance. Per `-Placement`, specificare il parametro `GroupName` e quindi specificare il nome del gruppo di collocazione creato nelle fasi precedenti.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType instance_type `
    -KeyName key_pair_name `
    -SubnetId subnet-0abcdef1234567890 `
```

```
    -CapacityReservationTarget_CapacityReservationId capacity_reservation_id `
    -Placement_GroupName placement_group_name
```

Condivisione delle prenotazioni di capacità nei gruppi di collocamento

Puoi condividere le prenotazioni di capacità nei gruppi di collocamento condividendo solo le prenotazioni di capacità o condividendo sia le prenotazioni di capacità che il gruppo di collocamento in cui sono state create.

Condividendo solo la prenotazione della capacità, concedi agli account consumatore l'accesso solo a tale prenotazione della capacità. Gli account dei consumatori non hanno visibilità o accesso al gruppo di collocamento in cui viene creata la Capacity Reservation. Questo ti offre un controllo dettagliato sull'accesso all'account consumatore. Gli account consumer non possono visualizzare alcuna informazione sul gruppo di collocamento, incluso il relativo ARN.

Quando condividi il gruppo di collocamento e la Capacity Reservation, il gruppo di collocamento è visibile e accessibile agli account dei consumatori. Possono avviare istanze e creare al loro interno le proprie prenotazioni della capacità.

Per ulteriori informazioni, consulta le risorse seguenti.

- Avvia le istanze in Capacity Reservations in un gruppo di collocamento
- Prenotazioni della capacità condivise
- Gruppi di posizionamento condivisi

Prenotazioni della capacità in zone locali

Una zona locale è un'estensione di una AWS regione geograficamente vicina ai tuoi utenti. Le risorse create in una Local Zone possono servire gli utenti locali con comunicazioni a latenza molto bassa. Per ulteriori informazioni, consulta AWS Local Zones.

Puoi estendere un VPC dalla sua AWS regione principale a una zona locale creando una nuova sottorete in quella zona locale. Quando si crea una sottorete in una Local Zone, il VPC viene esteso anche a tale Local Zone. La sottorete nella Local Zone funziona allo stesso modo delle altre sottoreti nel VPC.

Utilizzando le Local Zones, è possibile collocare Prenotazioni di capacità in più posizioni più vicine agli utenti. È possibile creare e utilizzare Prenotazioni di capacità in Local Zones nello stesso modo in cui si crea e si utilizza Prenotazioni di capacità nelle normali zone di disponibilità. Si applicano le

stesse caratteristiche e il comportamento di corrispondenza delle istanze. Per ulteriori informazioni sui modelli di determinazione dei prezzi supportati nelle Local Zones, consultare Domande frequenti sulle Local Zones AWS.

Considerazioni

Non è possibile utilizzare gruppi Prenotazione della capacità in una zona locale.

Per utilizzare una prenotazione della capacità in una zona locale

1. Abilita la zona locale per utilizzarla nel tuo AWS account. Per ulteriori informazioni, consulta la Guida introduttiva alle zone AWS locali nella Guida per l'utente delle zone AWS locali.
2. Creare una prenotazione della capacità nella zona locale. Per Availability Zone (Zona di disponibilità), scegli la Local Zone. La zona locale è rappresentata da un codice regione AWS seguito da un identificatore che indica la posizione, ad esempio `us-west-2-lax-1a`. Per ulteriori informazioni, consulta Creazione di una Prenotazione della capacità.
3. Creare una sottorete nella Local Zone. Per Availability Zone (Zona di disponibilità), scegli la Local Zone. Per ulteriori informazioni, consulta Creazione di una sottorete nel VPC nella Guida per l'utente di Amazon VPC.
4. Avvia un'istanza. Per Subnet (Sottorete), scegliere la sottorete nella Local Zone (ad esempio `subnet-123abc | us-west-2-lax-1a`), e per Capacity Reservation (Prenotazione della capacità), scegliere la specifica (`open` o la destinazione per ID) necessaria per la Prenotazione della capacità creata nella Local Zone. Per ulteriori informazioni, consulta Avvio di istanze in una Prenotazione della capacità esistente.

Prenotazioni della capacità nelle zone Wavelength

AWS Wavelength consente agli sviluppatori di creare applicazioni che offrono latenze molto basse a dispositivi mobili e utenti finali. Wavelength distribuisce servizi di calcolo e storage standard di AWS all'edge delle reti 5G dei provider all'avanguardia nei servizi di telecomunicazione. Puoi estendere un Amazon Virtual Private Cloud (VPC) a una o più zone Wavelength. Puoi quindi utilizzare AWS risorse come le istanze Amazon EC2 per eseguire applicazioni che richiedono una latenza estremamente bassa e una connessione ai AWS servizi nella regione. Per maggiori informazioni, consultare Zone AWS Wavelength.

Quando crei le prenotazioni On-Demand di capacità, puoi scegliere la zona di lunghezza d'onda e avviare le istanze in una riserva di capacità in una zona di lunghezza d'onda specificando la sottorete associata alla zona di lunghezza d'onda. Una zona di lunghezza d'onda è rappresentata da un codice

AWS regionale seguito da un identificatore che indica la posizione, ad esempio. `us-east-1-wl1-bos-wlz-1`

Le zone Wavelength non sono disponibili in tutte le regioni. Per informazioni sulle regioni che supportano le zone Wavelength, consulta Zone Wavelength disponibili nella Guida per gli sviluppatori di AWS Wavelength .

Considerazioni

Non è possibile utilizzare gruppi Prenotazione della capacità in una zona Wavelength.

Utilizzo di una Prenotazione della capacità in una zona Wavelength

1. Abilita la Wavelength Zone per utilizzarla nel tuo account. AWS Per ulteriori informazioni, consulta Nozioni di base su AWS Wavelength nella Guida per gli sviluppatori di AWS Wavelength .
2. Creare una Prenotazione della capacità nella zona Wavelength. Per Zona di disponibilità, scegli Wavelength. La Wavelength è rappresentata da un codice regione AWS seguito da un identificatore che indica la posizione, ad esempio `us-east-1-wl1-bos-wlz-1`. Per ulteriori informazioni, consulta Creazione di una Prenotazione della capacità.
3. Crea una sottorete nella zona Wavelength. Per Zona di disponibilità, scegli la zona Wavelength. Per ulteriori informazioni, consulta Creazione di una sottorete nel VPC nella Guida per l'utente di Amazon VPC.
4. Avvia un'istanza. Per Subnet (Sottorete), scegliere la sottorete nella zona Wavelength (ad esempio `subnet-123abc | us-east-1-wl1-bos-wlz-1`), e per Prenotazione della capacità, scegliere la specifica (`open` o la destinazione per ID) necessaria per la Prenotazione della capacità creata nella Wavelength. Per ulteriori informazioni, consulta Avvio di istanze in una Prenotazione della capacità esistente.

Prenotazioni di capacità su AWS Outposts

AWS Outposts è un servizio completamente gestito che estende l' AWS infrastruttura, i servizi, le API e gli strumenti alla sede del cliente. Fornendo l'accesso locale all'infrastruttura AWS gestita, AWS Outposts consente ai clienti di creare ed eseguire applicazioni in locale utilizzando le stesse interfacce di programmazione AWS delle regioni, utilizzando al contempo risorse di elaborazione e archiviazione locali per esigenze di latenza inferiore e di elaborazione locale dei dati.

Un Outpost è un pool di capacità di AWS elaborazione e archiviazione distribuito presso la sede del cliente. AWS opera, monitora e gestisce questa capacità come parte di una regione. AWS

È possibile creare Prenotazioni di capacità sugli Outpost creati nel tuo account. Questo ti permette di riservare capacità di calcolo su un Outpost presso il tuo sito. È possibile creare e utilizzare Prenotazioni di capacità negli Outpost nello stesso modo in cui si crea e si utilizzano le Prenotazioni di capacità nelle normali zone di disponibilità. Si applicano le stesse caratteristiche e il comportamento di corrispondenza delle istanze.

Puoi anche condividere le prenotazioni di capacità su Outposts con altri AWS account all'interno della tua organizzazione utilizzando AWS Resource Access Manager. Per informazioni sulla condivisione delle prenotazioni di capacità, consulta Prenotazioni della capacità condivise.

Prerequisito

Devi avere un Outpost installato presso il tuo sito. Per ulteriori informazioni, consulta Creazione di un Outpost e ordinazione della capacità Outpost nella Guida per l'utente di AWS Outposts .

Considerazioni

- Non è possibile utilizzare gruppi Prenotazione della capacità in un Outpost.

Per utilizzare una Prenotazione della capacità in un Outpost

1. Creare una sottorete nell'Outpost. Per ulteriori informazioni, consulta Creazione di una sottorete nella Guida per l'utente di AWS Outposts .
2. Creare una prenotazione della capacità nell'Outpost.
   a. Apri la AWS Outposts console all'indirizzo. https://console.aws.amazon.com/outposts/
   b. Nel pannello di navigazione, selezionare Outposts e quindi Operazioni, Crea prenotazione della capacità.
   c. Configurare la Prenotazione della capacità in base alle esigenze, quindi scegliere Create (Crea). Per ulteriori informazioni, consulta Creazione di una Prenotazione della capacità.

> **Note**
>
> Il menu a discesa Instance Type (Tipo di istanza) elenca solo i tipi di istanza supportati dall'Outpost selezionato, mentre Availability zone (Zona di disponibilità) elenca solo la zona di disponibilità a cui è associato l'Outpost selezionato.

3. Avviare un'istanza in una Prenotazione della capacità. Per Subnet (Sottorete), selezionare la sottorete creata alla fase 1 e per Capacity Reservation (Prenotazione della capacità) selezionare la Prenotazione della capacità creata alla fase 2. Per ulteriori informazioni, consulta Avvio di un'istanza sull'Outpost nella Guida per l'utente di AWS Outposts .

Prenotazioni della capacità condivise

La condivisione di Capacity Reservation consente ai proprietari di Capacity Reservation di condividere la capacità riservata con altri AWS account o all'interno di un' AWS organizzazione. Ciò consente di creare e gestire centralmente le prenotazioni di capacità e condividere la capacità riservata tra più AWS account o all'interno AWS dell'organizzazione.

In questo modello, l' AWS account proprietario della Capacity Reservation (proprietario) la condivide con altri AWS account (consumatori). I consumatori possono avviare le istanze in Prenotazioni di capacità condivise con loro nello steso modo in cui le avvierebbero in Prenotazioni di capacità di cui sono proprietari nel proprio account. Il proprietario Prenotazione della capacità è responsabile della gestione di Prenotazione della capacità e delle istanze avviate in esso. I proprietari non possono modificare le istanze che i consumatori avviano in Prenotazioni di capacità che hanno condiviso. I consumatori sono responsabili della gestione delle istanze che avviano in Prenotazioni di capacità condivisi con loro. I consumatori non possono visualizzare o modificare le istanze di proprietà di altri consumatori o del proprietario Prenotazione della capacità.

Un proprietario Prenotazione della capacità può condividere Prenotazione della capacità con:

- AWS Account specifici all'interno o all'esterno della sua AWS organizzazione
- Un'unità organizzativa all'interno della sua AWS organizzazione
- La sua intera AWS organizzazione

Prerequisiti per la condivisione di Prenotazioni di capacità

- Per condividere una prenotazione di capacità, devi possederla nel tuo AWS account. Non è possibile condividere una Prenotazione della capacità che è stato condiviso con te.
- È possibile condividere solo Prenotazioni di capacità per istanze con tenancy condivise. Non è possibile condividere Prenotazioni di capacità per istanze dedicate a tenancy singola.
- La condivisione di Capacity Reservation non è disponibile per AWS i nuovi AWS account o per gli account con una cronologia di fatturazione limitata.

- Per condividere una Capacity Reservation con la tua AWS organizzazione o un'unità organizzativa AWS della tua organizzazione, devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta Abilitare la condivisione con AWS Organizations nella Guida per l'utente AWS RAM .
- Puoi condividere una prenotazione di capacità nel `active` nostro `scheduled` stato. Non è possibile condividere la prenotazione di capacità in altri stati, come `assessing` o `unsupported`.

Servizi correlati

La condivisione di Capacity Reservation si integra con AWS Resource Access Manager (AWS RAM). AWS RAM è un servizio che ti consente di condividere AWS le tue risorse con qualsiasi AWS account o tramite AWS Organizations. Con AWS RAM, condividi le risorse di cui sei proprietario creando una condivisione delle risorse. Una condivisione delle risorse specifica le risorse da condividere e gli utenti con cui condividerle. I consumatori possono essere singoli AWS account, unità organizzative o un'intera organizzazione di AWS Organizations.

Per ulteriori informazioni AWS RAM, consulta la Guida AWS RAM per l'utente .

Condivisione tra zone di disponibilità

Per garantire che le risorse vengano distribuite tra le zone di disponibilità di una regione, mappiamo in modo indipendente le zone di disponibilità ai nomi per ciascun account. Questo potrebbe comportare una diversa denominazione delle zone di disponibilità tra i diversi account. Ad esempio, la zona `us-east-1a` di disponibilità del tuo AWS account potrebbe non avere la stessa posizione `us-east-1a` di un altro AWS account.

Per individuare la posizione di Prenotazioni di capacità relativamente ai tuoi account, devi utilizzare l'ID della zona di disponibilità (ISD AZ). L'ID AZ è un identificatore univoco e coerente per una zona di disponibilità in tutti gli AWS account. Ad esempio, `use1-az1` è un ID AZ per la `us-east-1` regione ed è la stessa posizione in tutti gli AWS account.

Quando condividi una prenotazione di capacità con un altro account, la prenotazione di capacità viene associata a una sede specifica identificata dal relativo ID AZ. L'account consumatore può utilizzare la prenotazione di capacità condivisa solo nella zona di disponibilità associata allo stesso ID AZ del proprio account. Ad esempio, se si crea una prenotazione di capacità in `us-east-1a` (ID AZ`use1-az1`), il consumatore deve avviare le istanze nella zona di disponibilità associata al `use1-az1` proprio account. Tale zona di disponibilità potrebbe avere un nome diverso, ad esempio`us-east-1b`.

Per visualizzare gli ID AZ per le zone di disponibilità nell'account

1. Apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram/home.
2. Gli ID AZ per la regione attuale vengono visualizzati nel pannello Il tuo ID AZ sul lato destro dello schermo.

Condivisione di una Prenotazione della capacità

Quando condividi una prenotazione di capacità che possiedi con altri Account AWS, consenti loro di avviare istanze che sfruttano la tua capacità riservata. Se condividi una Prenotazione della capacità aperta, tieni a mente quanto segue, poiché potrebbe portare a un utilizzo indesiderato di Prenotazione della capacità:

- Se i consumatori hanno istanze in esecuzione che corrispondono agli attributi di Prenotazione della capacità, il parametro `CapacityReservationPreference` impostato su `open` e non sono ancora in esecuzione nella capacità riservata, utilizzano automaticamente la Prenotazione della capacità condivisa.
- Se i consumatori avviano le istanze con attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy) e hanno il parametro `CapacityReservationPreference` impostato su `open`, automaticamente si avviano nella prenotazione della capacità condivisa.

Per condividere Prenotazione della capacità, devi aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una AWS RAM risorsa che ti consente di condividere le tue risorse tra più AWS account. Una condivisione di risorse specifica le risorse da condividere e i consumatori con cui sono condivise. Quando condividi Prenotazione della capacità tramite la console Amazon EC2, l'aggiungi a una condivisione risorse esistente. Per aggiungere la Prenotazione della capacità a una nuova condivisione di risorse, devi creare la condivisione di risorse utilizzando la console AWS RAM.

Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno della tua organizzazione è abilitata, ai consumatori dell'organizzazione viene concesso l'accesso alla riserva di capacità condivisa se i prerequisiti per la condivisione sono soddisfatti. Se la Prenotazione della capacità è condivisa con account esterni, i consumatori ricevono un invito a unirsi alla condivisione di risorse e viene loro concesso l'accesso alla Prenotazione della capacità condivisa una volta accettato l'invito.

> **Important**
>
> Prima di avviare le istanze in una Capacity Reservation condivisa con te, verifica di avere accesso alla Capacity Reservation condivisa visualizzandola nella console o descrivendola utilizzando il comando describe-capacity-reservations. https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-capacity-reservations.html AWS CLI Se riesci a visualizzare la Reservation di capacità condivisa nella console o a descriverla utilizzando il AWS CLI, è disponibile per l'uso e puoi avviare istanze al suo interno. Se tenti di avviare le istanze nella Capacity Reservation e questa non è accessibile a causa di un errore di condivisione, la capacità delle istanze verrà avviata. On-Demand

Console

Per condividere Prenotazione della capacità di cui sei proprietario utilizzando la console Amazon EC2.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Scegliere Prenotazione della capacità per condividere e scegliere Azioni, Condividi prenotazione.
4. Selezionare la condivisione di risorse a cui aggiungere Prenotazione della capacità e scegliere Condividi Prenotazione della capacità.

   Prima dell'accesso a Prenotazione della capacità condiviso possono essere necessari alcuni minuti.

Per condividere una Capacity Reservation di tua proprietà utilizzando il AWS RAM console

Consulta Creating a resource share in Guida per l'utente di AWS RAM .

AWS CLI

Come condividere una prenotazione della capacità che possiedi

Utilizza il comando create-resource-share.

```
aws ram create-resource-share \
    --name my-resource-share \
```

```
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE
```

PowerShell

Come condividere una prenotazione della capacità che possiedi

Utilizza il cmdlet New-RAMResourceShare.

```
New-RAMResourceShare `
    -Name my-resource-share `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE"
```

Interrompere la condivisione di una Prenotazione della capacità

Il proprietario Prenotazione della capacità può interrompere la condivisione di una Prenotazione della capacità in qualsiasi momento. Si applicano le regole seguenti:

- Le istanze di proprietà dei consumatori che erano in esecuzione con capacità condivisa al momento dell'interruzione della condivisione continuano a funzionare nella capacità riservata. La capacità viene ripristinata nella Capacity Reservation quando i consumatori chiudono le istanze.
- I consumatori con cui è stato condiviso Prenotazione della capacità non possono più avviare nuove istanze nella capacità riservata.

Per interrompere la condivisione di una Prenotazione della capacità di un utente, è necessario rimuoverla dalla condivisione risorse.

Console

Per interrompere la condivisione di una Prenotazione della capacità di un utente tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Selezionare la Prenotazione della capacità e scegliere la scheda Condivisione.

4. La scheda Condivisione elenca le condivisioni di risorse a cui Prenotazione della capacità è stato aggiunto. Selezionare la condivisione di risorse da cui eliminare Prenotazione della capacità e selezionare Elimina dalla condivisione di risorse.

Per interrompere la condivisione di una prenotazione di capacità di tua proprietà, utilizza AWS RAM console

Consulta Aggiornamento di una condivisione di risorse in Guida per l'utente di AWS RAM .

AWS CLI

Come arrestare la condivisione di una prenotazione della capacità che possiedi

Utilizza il comando disassociate-resource-share.

```
aws ram disassociate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
 --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE
```

PowerShell

Come arrestare la condivisione di una prenotazione della capacità che possiedi

Utilizza il cmdlet Disconnect-RAMResourceShare.

```
Disconnect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE"
```

Assegnazione di fatturazione per prenotazioni della capacità di Amazon EC2 condivise

Per impostazione predefinita, quando una prenotazione della capacità viene condivisa, al proprietario vengono fatturate le istanze eseguite nella prenotazione della capacità e l'eventuale capacità disponibile, detta anche capacità inutilizzata, nella prenotazione della capacità; mentre ai consumatori vengono fatturate solo le istanze eseguite nella prenotazione della capacità condivisa.

Se necessario, il proprietario della prenotazione della capacità può assegnare la fatturazione di qualsiasi capacità disponibile nella prenotazione della capacità a uno qualsiasi degli account con cui è condivisa la prenotazione della capacità. Dopo l'assegnazione della fatturazione a un altro account, tale account diventa il proprietario della fatturazione di qualsiasi capacità disponibile nella prenotazione della capacità. Qualsiasi addebito per la capacità disponibile nella Prenotazione della capacità, da quel momento in poi, viene fatturato sull'account assegnato anziché sull'account del proprietario. Il proprietario della prenotazione della capacità e gli account con cui è condivisa la prenotazione della capacità continuano a essere fatturati per le istanze eseguite nella prenotazione della capacità.

> **Important**
>
> Il proprietario della prenotazione della capacità rimane il proprietario della risorsa e rimane responsabile della gestione di Prenotazione della capacità. L'account a cui è assegnata la fatturazione non ottiene alcun privilegio aggiuntivo; non può annullare, modificare o condividere in alcun modo la prenotazione della capacità.

Argomenti

- Come funziona
- Considerazioni
- Assegna la fatturazione di una prenotazione della capacità EC2 condivisa a un altro account
- Visualizza l'assegnazione della fatturazione per prenotazioni della capacità di EC2 condivise
- Accetta o rifiuta la fatturazione di una prenotazione della capacità EC2 condivisa
- Cancella o revoca l'assegnazione della fatturazione per prenotazioni della capacità di EC2 condivise
- Monitora l'assegnazione della fatturazione per prenotazioni della capacità condivise

Come funziona

Solo il proprietario della prenotazione della capacità può assegnare la fatturazione di una prenotazione della capacità condivisa a un altro account. La fatturazione può essere assegnata solo a un account con cui la Capacity Reservation è condivisa e che è consolidato nello stesso account AWS Organizations pagante del titolare della Capacity Reservation.

Per assegnare la fatturazione della capacità disponibile di una prenotazione della capacità a un altro account, il proprietario della prenotazione della capacità deve inviare una richiesta all'account richiesto. L'account specificato riceve la richiesta e deve accettarla o rifiutarla entro 12 ore.

- Se accetta, diventa proprietario della fatturazione di qualsiasi capacità disponibile, detta anche capacità inutilizzata, inclusa nella prenotazione della capacità. Da quel momento in poi, qualsiasi addebito per la capacità disponibile nella prenotazione della capacità viene fatturato sul suo account anziché sull'account del proprietario. Dopo l'accettazione, solo il proprietario della prenotazione della capacità può revocare la fatturazione dall'account assegnato.
- Se rifiuta, il proprietario della prenotazione della capacità rimane il responsabile della fatturazione della capacità disponibile nella prenotazione della capacità. I costi per qualsiasi capacità disponibile nella prenotazione della capacità continuano a essere fatturati sull'account del proprietario.
- Se non accetta o rifiuta la richiesta entro 12 ore, la richiesta scade e i costi per l'eventuale capacità disponibile nella prenotazione della capacità continuano ad essere addebitati sull'account del proprietario.

Per il periodo in cui la fatturazione è assegnata a un altro account, le voci `Reservation` e `UnusedBox` appaiono nel report di costi e utilizzo (CUR) dell'account assegnato anziché nel CUR del proprietario.

La tabella seguente mostra quali voci appaiono nel CUR per gli account proprietario e consumatore della prenotazione della capacità prima che la fatturazione venga assegnata a un altro account.

Account	Voci CUR prima dell'assegnazione della fatturazione
Proprietario della prenotazione della capacità	• `Reservation` • `BoxUsage *` • `UnusedBox`
Account consumatore con cui è condivisa la prenotazione della capacità	• `BoxUsage *`

Account	Voci CUR prima dell'assegnazione della fatturazione

La tabella seguente mostra quali voci appaiono nel CUR per gli account proprietario e consumatore della prenotazione della capacità dopo che la fatturazione venga assegnata a un altro account.

Account	Voci CUR dopo l'assegnazione della fatturazione
Proprietario della prenotazione della capacità	• `BoxUsage *`
Account consumatore a cui è assegnata la fatturazione	• `Reservation` • `BoxUsage *` • `UnusedBox`
Altri account consumatore con cui è condivisa la prenotazione della capacità	• `BoxUsage *`

Note

- * La voce `BoxUsage` appare nel CUR di un account solo se ci sono istanze in esecuzione nella prenotazione della capacità. Per ulteriori informazioni sulle voci del CUR, consulta Monitoraggio delle prenotazioni della capacità.
- Utilizza l'ARN di prenotazione della capacità nel CUR per determinare a chi appartiene la prenotazione della capacità. Se l'ARN include l'ID del tuo AWS account, sei il proprietario di Capacity Reservation. In caso contrario, la prenotazione della capacità è di proprietà di un altro account, ma la fatturazione viene assegnata all'utente.

- I tag di allocazione dei costi assegnati alla prenotazione della capacità dal proprietario non appariranno nel CUR dell'account consumatore. I tag di allocazione dei costi appaiono solo nel CUR del proprietario della prenotazione della capacità.

Considerazioni

Quando assegni la fatturazione di una prenotazione della capacità condivisa, tieni presente quanto segue:

- Non puoi realizzare assegnazioni di fatturazione parziali o suddivise. La fatturazione di tutta la capacità disponibile di una prenotazione della capacità può essere assegnata a un account alla volta.
- La capacità disponibile di una prenotazione della capacità può cambiare nel corso del tempo. Ciò influirà sulla fatturazione dell'account assegnato. Ad esempio, la capacità disponibile può aumentare se il proprietario della prenotazione della capacità aumenta le dimensioni della prenotazione della capacità o se altri account consumer interrompono o arrestano le relative istanze in esecuzione nella prenotazione della capacità.
- La fatturazione può essere assegnata solo a un account consumatore consolidato con lo stesso AWS Organizations account pagante. La fatturazione viene revocata automaticamente dall'account consumatore se l'utente lascia l'organizzazione o se la prenotazione della capacità non è più condivisa con lui.
- Solo il proprietario della prenotazione della capacità può annullare una richiesta di assegnazione di fatturazione in sospeso e revocare la fatturazione da un account assegnato dopo che la richiesta è stata accettata.
- Se il titolare annulla una prenotazione di capacità con data futura con fatturazione assegnata a un altro account, il titolare della fatturazione assegnato paga le spese di annullamento.

Assegna la fatturazione di una prenotazione della capacità EC2 condivisa a un altro account

Per assegnare la fatturazione della capacità disponibile di una prenotazione della capacità condivisa a un altro account, il proprietario della prenotazione della capacità deve inviare una richiesta all'account richiesto. Nella console Amazon EC2, questa richiesta viene chiamata richiesta di trasferimento.

Un proprietario della prenotazione della capacità può assegnare la fatturazione della capacità disponibile di una prenotazione della capacità a un account se:

- La prenotazione della capacità è già condivisa con quell'account.
- L'account è consolidato sotto lo stesso conto AWS Organizations pagante del titolare di Capacity Reservation.

La fatturazione viene assegnata all'account specificato solo dopo l'accettazione della richiesta.

Quando il titolare di Capacity Reservation avvia una richiesta, un EventBridge evento Amazon viene inviato all'account richiesto. Per ulteriori informazioni, consulta Monitora l'assegnazione della fatturazione per prenotazioni della capacità condivise.

Console

Per assegnare la fatturazione di una prenotazione della capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Prenotazioni della capacità e poi chiudi la prenotazione della capacità condivisa.
3. Nella sezione Fatturazione della capacità disponibile, scegli Assegna fatturazione.
4. Nella schermata Assegna fatturazione, seleziona l'account consumatore a cui assegnare la fatturazione, poi scegli Richiedi.

AWS CLI

Per assegnare la fatturazione di una prenotazione della capacità

Utilizza il comando associate-capacity-reservation-billing-owner. Per `--capacity-reservation-id`, specifica l'ID della prenotazione della capacità. Per`--unused-reservation-billing-owner-id`, specifica l'ID dell' AWS account a cui assegnare la fatturazione.

```
aws ec2 associate-capacity-reservation-billing-owner \
    --capacity-reservation-id cr-01234567890abcdef \
    --unused-reservation-billing-owner-id 123456789012
```

PowerShell

Per assegnare la fatturazione di una prenotazione della capacità

Utilizza il cmdlet Register-EC2CapacityReservationBillingOwner. Per `-CapacityReservationId`, specifica l'ID della prenotazione della capacità. Per `-UnusedReservationBillingOwnerId`, specifica l'ID dell' AWS account a cui assegnare la fatturazione.

```
Register-EC2CapacityReservationBillingOwner `
    -CapacityReservationId cr-01234567890abcdef `
    -UnusedReservationBillingOwnerId 123456789012
```

Visualizza l'assegnazione della fatturazione per prenotazioni della capacità di EC2 condivise

Un proprietario di prenotazione della capacità può visualizzare solo la richiesta di assegnazione di fatturazione più recente che ha avviato. Inoltre, gli account consumatore possono visualizzare solo le richieste di assegnazione di fatturazione più recenti a loro inviate.

Le richieste possono essere visualizzate per 24 ore dopo che sono entrate nello stato `cancelled`, `expired` o `revoked`. Dopo 24 ore, non possono più essere visualizzate.

Console

(Proprietario di prenotazione della capacità) Per visualizzare le richieste avviate

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Prenotazioni della capacità e poi scegli la prenotazione della capacità condivisa per cui visualizzare le richieste.
3. La sezione Fatturazione della capacità disponibile mostra la richiesta più recente e il suo stato attuale.

(Account consumatore) Alle richieste inviate a te

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Prenotazioni della capacità.
3. Se hai richieste in sospeso, nella parte superiore dello schermo viene visualizzato il banner Richieste di assegnazione della fatturazione in sospeso. Se il banner non viene visualizzato, non vi sono richieste in sospeso.

   Per visualizzare le richieste, scegli Rivedi le richieste nel banner.

AWS CLI

(Proprietario di prenotazione della capacità) Per visualizzare le richieste avviate

Utilizza il comando describe-capacity-reservation-billing-requests.

```
aws ec2 describe-capacity-reservation-billing-requests \
    --role odcr-owner
```

(Account consumatore) Per visualizzare le richieste inviate a te

Utilizza il comando describe-capacity-reservation-billing-requests.

```
aws ec2 describe-capacity-reservation-billing-requests \
    --role unused-reservation-billing-owner
```

PowerShell

(Proprietario di prenotazione della capacità) Per visualizzare le richieste avviate

Utilizza il cmdlet Get-EC2CapacityReservationBillingRequest.

```
Get-EC2CapacityReservationBillingRequest `
    -Role odcr-owner
```

(Account consumatore) Per visualizzare le richieste inviate a te

Utilizza il cmdlet Get-EC2CapacityReservationBillingRequest.

```
Get-EC2CapacityReservationBillingRequest `
    -Role unused-reservation-billing-owner
```

Una richiesta può avere uno dei seguenti stati.

Stato	Description			
`pending`	La richiesta non è stata accettata o rifiutata, ma non è ancora scaduta.			

Stato	Description
`accepted`	La richiesta è stata accettata dall'account specificato. La fatturazione della capacità disponibile della prenotazione della capacità è assegnata all'account consumatore.
`rejected`	La richiesta è stata rifiutata dall'account consumatore.
`cancelled`	La richiesta è stata annullata dal proprietario della prenotazione della capacità mentre si trovava nello stato `pending`.
`revoked`	La fatturazione è stata revocata dall'account consumatore per uno dei seguenti motivi: • È stato revocata esplicitamente dal proprietario della prenotazione della capacità. • La prenotazione della capacità non è più condivisa con l'account consumatore. • L'account consumatore non fa più parte dell'organizzazione AWS .

Stato	Description			
`expired`	La richiesta è scaduta perché l'account consumatore non l'ha accettata o rifiutata entro 12 ore.			

Accetta o rifiuta la fatturazione di una prenotazione della capacità EC2 condivisa

Se ricevi una richiesta di assegnazione della fatturazione per una prenotazione della capacità condivisa con te, puoi accettarla o rifiutarla. La richiesta rimane nello stato `pending` finché non viene accettata o rifiutata.

Se l'utente accetta la richiesta, questa entra nello stato `accepted` e la fatturazione di qualsiasi capacità disponibile o inutilizzata di tale prenotazione della capacità viene assegnata al suo account da quel momento in poi. Dopo aver accettato una richiesta, solo il proprietario della prenotazione della capacità può revocare la fatturazione dal tuo account.

Se rifiuti la richiesta, questa entra nello stato `rejected` e la fatturazione della capacità disponibile della prenotazione della capacità rimane assegnata al proprietario della prenotazione della capacità.

Le richieste scadono se non vengono accettate o rifiutate entro 12 ore. Se una richiesta scade, la fatturazione dell'eventuale capacità inutilizzata della prenotazione della capacità rimane assegnata al proprietario della prenotazione della capacità.

Quando una richiesta viene accettata o rifiutata, un EventBridge evento Amazon viene inviato all'account del proprietario di Capacity Reservation. Quando una richiesta scade, viene inviato un EventBridge evento Amazon al proprietario di Capacity Reservation e all'account del consumatore. Per ulteriori informazioni, consulta Monitora l'assegnazione della fatturazione per prenotazioni della capacità condivise.

Console

Per accettare o rifiutare una richiesta

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Prenotazioni della capacità.

3. Se hai richieste in sospeso, nella parte superiore dello schermo viene visualizzato il banner Richieste di assegnazione della fatturazione in sospeso. Se il banner non viene visualizzato, non vi sono richieste in sospeso.

   Per visualizzare le richieste, scegli Rivedi le richieste nel banner.

4. Seleziona la richiesta da accettare o rifiutare, poi scegli Accetta o Rifiuta.

AWS CLI

Per accettare una richiesta

Utilizza il comando accept-capacity-reservation-billing-ownership. Per `--capacity-reservation-id`, specifica l'ID della prenotazione della capacità per cui accettare la richiesta.

```
aws ec2 accept-capacity-reservation-billing-ownership \
    --capacity-reservation-id cr-01234567890abcdef
```

Per rifiutare una richiesta

Utilizza il comando reject-capacity-reservation-billing-ownership. Per `--capacity-reservation-id`, specifica l'ID della prenotazione della capacità per cui rifiutare la richiesta.

```
aws ec2 reject-capacity-reservation-billing-ownership \
    --capacity-reservation-id cr-01234567890abcdef
```

PowerShell

Per accettare una richiesta

Utilizza il cmdlet Approve-EC2CapacityReservationBillingOwnership.

```
Approve-EC2CapacityReservationBillingOwnership `
    -CapacityReservationId cr-01234567890abcdef
```

Per rifiutare una richiesta

Utilizza il cmdlet Deny-EC2CapacityReservationBillingOwnership.

```
Deny-EC2CapacityReservationBillingOwnership `
```

```
    -CapacityReservationId cr-01234567890abcdef
```

Cancella o revoca l'assegnazione della fatturazione per prenotazioni della capacità di EC2 condivise

Solo il proprietario della prenotazione della capacità può annullare una richiesta di assegnazione di fatturazione `pending`. Se una richiesta in sospeso viene annullata, questa entra nello stato `cancelled` e la fatturazione della capacità disponibile, o inutilizzata della prenotazione della capacità rimane assegnata al proprietario della prenotazione della capacità.

Una volta che una richiesta è `accepted`, solo il proprietario della prenotazione della capacità può revocare la fatturazione dall'account assegnato. Se la fatturazione viene revocata, la richiesta entra nello stato `revoked` e la fatturazione della capacità disponibile della prenotazione della capacità viene riassegnata al proprietario della prenotazione della capacità.

Quando una richiesta viene annullata o revocata, EventBridge gli eventi Amazon vengono inviati al proprietario di Capacity Reservation e all'account consumatore specificato. Per ulteriori informazioni, consulta Monitora l'assegnazione della fatturazione per prenotazioni della capacità condivise.

Console

Per annullare o revocare una richiesta

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Prenotazioni della capacità e poi scegli la prenotazione della capacità per cui annullare o revocare la richiesta.
3. Nella sezione Fatturazione della capacità disponibile, scegli Annulla trasferimento o Revoca trasferimento, a seconda dello stato attuale della richiesta.

AWS CLI

Per annullare o revocare una richiesta

Utilizza il comando disassociate-capacity-reservation-billing-owner. Per `--unused-reservation-billing-owner-id`, specifica l'ID dell' AWS account a cui è stata inviata la richiesta.

```
aws ec2 disassociate-capacity-reservation-billing-owner \
    --capacity-reservation-id cr-01234567890abcdef \
    --unused-reservation-billing-owner-id 123456789012
```

PowerShell

Per annullare o revocare una richiesta

Utilizza il cmdlet Unregister-EC2CapacityReservationBillingOwner. Per-UnusedReservationBillingOwnerId, specificare l'ID dell' AWS account a cui è stata inviata la richiesta.

```
Unregister-EC2CapacityReservationBillingOwner `
    -CapacityReservationId cr-01234567890abcdef `
    -UnusedReservationBillingOwnerId 123456789012
```

Monitora l'assegnazione della fatturazione per prenotazioni della capacità condivise

Amazon EC2 invia EventBridge eventi Amazon quando lo stato di una richiesta di assegnazione di fatturazione cambia.

- Gli eventi vengono inviati al proprietario della prenotazione della capacità quando una richiesta entra nei seguenti stati: `accepted` | `rejected` | `expired` | `revoked`.
- Gli eventi vengono inviati all'account consumatore richiesto quando una richiesta entra nei seguenti stati: `pending` | `expired` | `cancelled` | `revoked`.

Per ulteriori informazioni su Amazon EventBridge, consulta la Amazon EventBridge User Guide.

Di seguito è riportato lo schema EventBridge degli eventi Amazon.

```
{
   "version":"0",
   "id":"12345678-1234-1234-1234-123456789012",
   "detail-type":"On-Demand Capacity Reservation Billing Ownership Request pending|
accepted|rejected|cancelled|revoked|expired",
   "source":"aws.ec2",
   "account":"account_id",
   "time":"state_change_timestamp",
   "region":"region",
   "resources":[
      "arn:aws:ec2:region:cr_owner_account_id:capacity-reservation/cr_id"
   ],
   "detail":{
      "capacity-reservation-id":"cr_id",
```

```
      "updateTime":timestamp,
      "ownerAccountId":"cr_owner_account_id",
      "unusedReservationChargesOwnerID":"consumer_account_id",
      "status":"pending|accepted|rejected|cancelled|revoked|expired",
      "statusMessage":"message
   }
}
```

Di seguito è riportato un esempio di evento inviato al proprietario della prenotazione della capacità (222222222222) quando un account consumatore (111111111111) accetta una richiesta di assegnazione della fatturazione per una prenotazione della capacità (`cr-01234567890abcdef`) condivisa.

```
{
   "version":"0",
   "id":"12345678-1234-1234-1234-123456789012",
   "detail-type":"On-Demand Capacity Reservation Billing Ownership Request accepted",
   "source":"aws.ec2",
   "account":"222222222222",
   "time":"2024-09-01Thh:59:59Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:222222222222:capacity-reservation/cr-01234567890abcdef"
   ],
   "detail":{
      "capacity-reservation-id":"cr-01234567890abcdef",
      "updateTime":"2024-08-01Thh:59:59Z",
      "ownerAccountId":"222222222222",
      "unusedReservationChargesOwnerID":"111111111111",
      "status":"accepted",
      "statusMessage":"billing transfer status message"
   }
}
```

Autorizzazioni di Prenotazione della capacità condivise

Autorizzazioni per i proprietari

I proprietari sono responsabili della gestione e dell'annullamento dei loro Prenotazioni di capacità condivisi. I proprietari non possono modificare le istanze in esecuzione nel Prenotazione della capacità condiviso di proprietà di altri account. I proprietari sono comunque responsabili della gestione delle istanze che avviano nel Prenotazione della capacità condiviso.

Autorizzazioni per i consumatori

I consumatori sono responsabili della gestione delle istanze in esecuzione nell'Prenotazione della capacità condiviso. I consumatori non possono modificare l'Prenotazione della capacità condiviso in nessun modo e non possono visualizzare o modificare le istanze di proprietà di altri consumatori o del proprietario di Prenotazione della capacità. I consumatori possono visualizzare solo la capacità totale e la capacità disponibile nella prenotazione condivisa.

Fatturazione e misurazione

Non sono previsti costi aggiuntivi per la condivisione di Prenotazioni di capacità.

Per impostazione predefinita, il proprietario della prenotazione della capacità riceve la fatturazione per istanze in esecuzione all'interno della prenotazione della capacità e per la capacità riservata inutilizzata, mentre ai consumatori vengono fatturate solo le istanze in esecuzione nella prenotazione della capacità condivisa. Tuttavia, puoi assegnare la fatturazione della capacità disponibile di una prenotazione della capacità condivisa a un altro account consumatore specifico. Per ulteriori informazioni, consulta Assegnazione di fatturazione per prenotazioni della capacità di Amazon EC2 condivise.

Se il titolare della prenotazione della capacità appartiene a un account pagante diverso e la prenotazione della capacità è coperta da un'istanza riservata regionale o da un Savings Plan, al proprietario della prenotazione della capacità continuerà a essere fatturata l'istanza riservata regionale o il Savings Plan. In questi casi, il proprietario della prenotazione della capacità paga l'istanza regionale riservata o il Savings Plan e ai consumer vengono fatturati i costi delle istanze eseguite nella prenotazione della capacità condivisa.

Limiti di istanze

L'intero utilizzo di Capacity Reservation viene conteggiato ai fini dei limiti di On-Demand istanza del proprietario di Capacity Reser di ripetizione che riesce:

- Capacità prenotata non utilizzata
- Utilizzo da parte delle istanze possedute dal proprietario Prenotazione della capacità
- Utilizzo da parte delle istanze possedute dai consumatori

Le istanze avviate nella capacità condivisa dai consumatori vengono conteggiate ai fini del limite di On-Demand istanze del proprietario di Capacity Reservation. I limiti di istanze dei consumatori sono

la somma dei propri limiti di On-Demand istanze e della capacità disponibile nelle prenotazioni di capacità condivise a cui hanno accesso.

Parco istanze prenotazione della capacità

Una flotta On-Demand di prenotazioni di capacità è un gruppo di prenotazioni di capacità.

Una richiesta di parco istanze di prenotazione della capacità contiene tutte le informazioni di configurazione necessarie per avviare un parco istanze di prenotazione della capacità. Utilizzando una singola richiesta, puoi prenotare grandi quantità di capacità Amazon EC2 per il tuo carico di lavoro su più tipi di istanze, fino a una capacità di destinazione specificata.

Dopo aver creato un parco istanze di prenotazione della capacità, potrai gestire collettivamente le prenotazione della capacità nel parco istanze, modificandolo o annullandolo.

Argomenti

- Come funzionano i parchi istanze di prenotazione della capacità
- Considerazioni
- Prezzi
- Concetti sui parchi istanze di prenotazione della capacità e pianificazione
- Creazione di un parco istanze di prenotazione della capacità
- Modifica di un parco istanze di prenotazione della capacità
- Annullamento di un parco istanze di prenotazione della capacità
- Esempio di configurazione di un parco istanze di prenotazione della capacità
- Utilizzo di ruoli collegati ai servizi per il parco istanze di prenotazione della capacità

Come funzionano i parchi istanze di prenotazione della capacità

Quando crei un parco istanze di prenotazione della capacità, questo tenta di creare prenotazioni della capacità individuali per soddisfare la capacità target totale specificata nella richiesta del parco istanze.

Il numero di istanze per cui il parco istanze prenota la capacità dipende dalla capacità target totale e dai pesi del tipo di istanza specificati. Il tipo di istanza per il quale prenota la capacità dipende dalla strategia di allocazione e dalla priorità del tipo di istanza utilizzate.

Se non c'è capacità sufficiente al momento della creazione del parco istanze e questo non è in grado di soddisfare immediatamente la capacità target totale, il parco istanze tenta di creare

asincronicamente le prenotazioni della capacità, finché non avrà prenotato la quantità di capacità richiesta.

Quando il parco istanze avrà raggiunto la sua capacità target totale, tenterà di mantenerla. Se una prenotazione della capacità nel parco istanze viene annullata, questo creerà automaticamente una o più prenotazioni della capacità, a seconda della configurazione del parco istanze, per sostituire la capacità persa e mantenere la capacità target totale.

Le prenotazioni della capacità nel parco istanze non possono essere gestite individualmente. Devono essere gestite collettivamente, modificando il parco istanze. Quando modifichi un parco istanze, le prenotazioni della capacità in esso contenute vengono automaticamente aggiornate per riflettere le modifiche.

Attualmente, i parchi istanze di prenotazione della capacità supportano i criteri `open` di corrispondenza delle istanze e tutte le prenotazioni della capacità avviate da un parco istanze utilizzano automaticamente questi criteri di corrispondenza. Con questi criteri, le nuove istanze e le istanze esistenti che hanno attributi corrispondenti di (tipo di istanza, piattaforma, zona di disponibilità e tenancy) vengono automaticamente eseguite nelle prenotazioni della capacità create da un parco istanze. I parchi istanze di prenotazione della capacità non supportano i criteri di corrispondenza delle istanze specifici.

Considerazioni

Quando utilizzi i parchi istanze di prenotazione della capacità, tieni presente quanto segue:

- Una flotta di prenotazioni di capacità può essere creata, modificata, visualizzata e annullata utilizzando l' AWS API AWS CLI and.
- Le prenotazioni della capacità in un parco istanze non possono essere gestite individualmente. Devono essere gestite collettivamente, modificando o annullando il parco istanze.
- Un parco istanze di prenotazione della capacità non può estendersi in tutte le Regioni.
- Un parco istanze di prenotazione della capacità non può estendersi su più zone di disponibilità.
- Le prenotazioni della capacità create da un parco istanze vengono automaticamente contrassegnate con il seguente tag AWS generato:
  - Chiave - `aws:ec2-capacity-reservation-fleet`
  - Valore - *`fleet_id`*

  È possibile utilizzare questo tag per identificare le prenotazioni della capacità create da un parco istanze di prenotazione della capacità.

Prezzi

Non sono previsti costi aggiuntivi, per l'utilizzo di parchi istanze di prenotazione della capacità. Ti verranno fatturate le singole prenotazioni della capacità create dai parchi istanze di prenotazioni della capacità. Per ulteriori informazioni sulla fatturazione delle prenotazioni della capacità, consulta Prezzi e fatturazione di Prenotazione della capacità.

Concetti sui parchi istanze di prenotazione della capacità e pianificazione

Le seguenti informazioni descrivono come pianificare un parco istanze di prenotazione della capacità e descrivono i concetti del parco istanze di prenotazione della capacità, tra cui la capacità target totale, la strategia di allocazione, il peso del tipo di istanza e la priorità del tipo di istanza.

Argomenti

- Pianificare un parco istanze di prenotazione della capacità
- Capacità target totale
- Strategia di allocazione
- Peso del tipo di istanza
- Priorità del tipo di istanza

Pianificare un parco istanze di prenotazione della capacità

Nella pianificazione del proprio parco istanze di prenotazione della capacità, consigliamo di procedere come segue:

1. Determina la quantità di capacità di calcolo necessaria per il carico di lavoro.
2. Decidi i tipi di istanza e le zone di disponibilità che desideri utilizzare.
3. Assegna a ciascun tipo di istanza una priorità in base alle tue esigenze e preferenze. Per ulteriori informazioni, consulta Priorità del tipo di istanza.
4. Crea un sistema di ponderazione della capacità che abbia senso per il tuo carico di lavoro. Assegna un peso a ciascun tipo di istanza e determina la capacità target totale. Per ulteriori informazioni, consulta Peso del tipo di istanza e Capacità target totale.
5. Stabilisci se hai bisogno della prenotazione della capacità a tempo indeterminato o solo per uno specifico periodo di tempo.

Capacità target totale

LaCapacità target totale definisce la quantità totale della capacità di calcolo prenotata dal parco istanze di prenotazione della capacità. Specifichi la capacità target totale quando crei il parco istanze di prenotazione della capacità. Dopo la creazione del parco istanze, Amazon EC2 crea automaticamente le prenotazioni della capacità per prenotare la capacità fino al target totale.

Il numero di istanze per cui il parco istanze di prenotazione della capacità prenota la capacità è determinato dalla capacità target totale e dal peso del tipo di istanza specificato per ciascun tipo di istanza nel parco di prenotazione della capacità (`total target capacity/instance type weight=number of instances`).

È possibile assegnare una capacità target totale in base alle unità significative per il carico di lavoro. Ad esempio, se il carico di lavoro richiede un certo numero di vCPU, puoi assegnare la capacità target totale in base al numero di vCPU richieste. Se il carico di lavoro richiede vCPU `2048`, specifica una capacità target totale di `2048` e quindi assegna i pesi del tipo di istanza in base al numero di vCPU fornite dai tipi di istanza nel parco istanze. Per un esempio, consulta Peso del tipo di istanza.

Strategia di allocazione

La strategia di allocazione del parco istanze di prenotazione della capacità stabilisce il modo in cui questo soddisfa la richiesta di capacità riservata dalle specifiche del tipo di istanza nella configurazione del parco istanze di prenotazione della capacità.

Attualmente, è supportata solo la strategia di allocazione `prioritized`. Con questa strategia, il parco istanze di prenotazione della capacità crea prenotazioni utilizzando le priorità assegnate a ciascuna delle specifiche del tipo di istanza nella configurazione sua configurazione. I valori di priorità inferiori indicano una priorità più elevata per l'uso. Ad esempio, supponiamo di creare un parco istanze di prenotazione della capacità che utilizza i seguenti tipi e priorità di istanza:

- `m4.16xlarge`: priorità = 1
- `m5.16xlarge`: priorità = 3
- `m5.24xlarge`: priorità = 2

Come prima cosa, il parco istanze tenta di creare prenotazioni di capacità per `m4.16xlarge`. Se Amazon EC2 non ha sufficiente capacità `m4.16xlarge`, il parco istanze tenta di creare prenotazioni di capacità per `m5.24xlarge`. Se Amazon EC2 non ha sufficiente capacità `m5.24xlarge`, il parco istanze tenta di creare prenotazioni di capacità per `m5.16xlarge`.

Peso del tipo di istanza

Il peso del tipo di istanza è un peso assegnato a ciascun tipo di istanza nel parco istanze di prenotazione della capacità. Il peso determina quante unità di capacità ciascuna istanza di quel tipo specifico conta verso la capacità target totale del parco istanze.

È possibile assegnare pesi in base a unità significative per il carico di lavoro. Ad esempio, se il carico di lavoro richiede un certo numero di vCPU, è possibile assegnare pesi in base al numero di vCPU fornite da ciascun tipo di istanza nel parco istanze di prenotazione della capacità. In questo caso, se crei un parco istanze di capacità utilizzando `m4.16xlarge` e `m5.24xlarge`, assegnerai pesi corrispondenti al numero di vCPU per ciascuna istanza come segue:

- `m4.16xlarge` — 64 vCPU, peso = 64 unità
- `m5.24xlarge` — 96 vCPU, peso = 96 unità

Il peso del tipo di istanza determina il numero di istanze per cui il parco istanze di prenotazione della capacità prenota quest'ultima. Ad esempio, se una flotta di prenotazioni di capacità con una capacità target totale di `384` unità utilizza i tipi e i pesi delle istanze dell'esempio precedente, la flotta potrebbe riservare la capacità per 6 `m4.16xlarge` le istanze (384 pesi totali del tipo di istanza di destinazione = 6 capacity/64 istanze) o `4` `m5.24xlarge` per le istanze (384/96 = 4).

Se non assegni i pesi del tipo di istanza o se assegni un peso del tipo di istanza di `1`, la capacità target totale si baserà esclusivamente sul conteggio delle istanze. Ad esempio, se un parco istanze di prenotazione della capacità con una capacità target totale di `384`unità utilizza i tipi di istanza nell'esempio precedente, ma omette i pesi o specifica un peso di `1` per entrambi i tipi di istanza, il parco istanze potrebbe prenotare capacità per `384` istanze `m4.16xlarge` o per `384` istanze `m5.24xlarge`.

Priorità del tipo di istanza

La priorità del tipo di istanza è un valore che assegni ai tipi di istanza nel parco istanze. Le priorità vengono utilizzate per determinare quali tipi di istanza specificati per il parco istanze devono essere assegnati per l'uso.

I valori di priorità inferiori indicano una priorità più elevata per l'uso.

Creazione di un parco istanze di prenotazione della capacità

Quando crei un parco istanze di prenotazione della capacità, questo crea automaticamente le prenotazioni di capacità per i tipi di istanza specificati nella richiesta del parco istanze, fino a

raggiungere la capacità target totale specificata. Il numero di istanze per le quali il parco istanze di prenotazione della capacità prenota quest'ultima dipende dalla capacità target totale e dai pesi del tipo di istanza specificati nella richiesta. Per ulteriori informazioni, consulta Peso del tipo di istanza e Capacità target totale.

Quando crei il parco istanze, devi specificare i tipi di istanza da utilizzare e una priorità per ciascuno di questi tipi di istanza. Per ulteriori informazioni, consulta Strategia di allocazione e Priorità del tipo di istanza.

> **Note**
>
> Il ruolo AWSServiceRoleForEC2CapacityReservationFleet collegato al servizio viene creato automaticamente nel tuo account la prima volta che crei un Capacity Reservation Fleet. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per il parco istanze di prenotazione della capacità.

Attualmente, i parchi istanze di prenotazione della capacità supportano solo i criteri `open` di corrispondenza delle istanze.

AWS CLI

Creazione di un parco istanze di prenotazione della capacità

Utilizza il comando create-capacity-reservation-fleet.

```
aws ec2 create-capacity-reservation-fleet \
    --total-target-capacity 24 \
    --allocation-strategy prioritized \
    --instance-match-criteria open \
    --tenancy default \
    --end-date 2021-12-31T23:59:59.000Z \
    --instance-type-specifications file://instanceTypeSpecification.json
```

Di seguito sono riportati i contenuti di `instanceTypeSpecification.json`.

```
[
  {
    "InstanceType": "m5.xlarge",
    "InstancePlatform": "Linux/UNIX",
```

```
    "Weight": 3.0,
    "AvailabilityZone":"us-east-1a",
    "EbsOptimized": true,
    "Priority" : 1
  }
]
```

Di seguito è riportato un output di esempio.

```
{
    "Status": "submitted",
    "TotalFulfilledCapacity": 0.0,
    "CapacityReservationFleetId": "crf-abcdef01234567890",
    "TotalTargetCapacity": 24
}
```

PowerShell

Come creare un parco di prenotazione della capacità

Utilizza il cmdlet New-EC2CapacityReservationFleet.

```
New-EC2CapacityReservationFleet `
    -TotalTargetCapacity 24 `
    -AllocationStrategy "prioritized" `
    -InstanceMatchCriterion "open" `
    -Tenancy "default" `
    -EndDate 2021-12-31T23:59:59.000Z `
    -InstanceTypeSpecification $specification
```

La specifica è definita come indicato di seguito.

```
$specification = New-Object Amazon.EC2.Model.ReservationFleetInstanceSpecification
$specification.InstanceType = "m5.xlarge"
$specification.InstancePlatform = "Linux/UNIX"
$specification.Weight = 3.0
$specification.AvailabilityZone = "us-east-1a"
$specification.EbsOptimized = $true
$specification.Priority = 1
```

Modifica di un parco istanze di prenotazione della capacità

È possibile modificare la capacità target totale e la data di un parco istanze di prenotazione della capacità in qualsiasi momento. Quando modifichi la capacità target totale di un parco istanze di prenotazione della capacità, questo crea automaticamente nuove prenotazioni di capacità o modifica o annulla le prenotazioni di capacità esistenti nel parco istanze per soddisfare la nuova capacità target totale. Quando modifichi la data di fine del parco istanze, le date di fine per tutte le singole prenotazioni di capacità vengono aggiornate di conseguenza.

Considerazioni

- Dopo aver modificato un parco istanze, il suo stato passa a `modifying`. Non è possibile tentare ulteriori modifiche a un parco istanze mentre si trova nello stato `modifying`.
- Non è possibile modificare la tenancy, la zona di disponibilità, i tipi di istanza, le piattaforme di istanza, le priorità o i pesi utilizzati da un parco istanze di prenotazione della capacità. Se devi modificare uno di questi parametri, potrebbe essere necessario che tu annulli il parco istanze esistente e crearne uno nuovo con i parametri richiesti.
- Non è possibile specificare `--end-date` e `--remove-end-date` nello stesso comando.

AWS CLI

Come modificare un parco istanze di prenotazione delle capacità

Utilizza il comando modify-capacity-reservation-fleet.

Esempio 1: modifica della capacità target totale

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --total-target-capacity 160
```

Esempio 2: modifica della data di fine

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --end-date 2021-07-04T23:59:59.000Z
```

Esempio 3: rimozione della data di fine

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --remove-end-date
```

PowerShell

Come modificare un parco istanze di prenotazione delle capacità

Utilizza il cmdlet Edit-EC2CapacityReservationFleet.

Esempio 1: modifica della capacità target totale

```
Edit-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-01234567890abcedf `
    -TotalTargetCapacity 160
```

Esempio 2: modifica della data di fine

```
Edit-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-01234567890abcedf `
    -EndDate 2021-07-04T23:59:59.000Z
```

Esempio 3: rimozione della data di fine

```
Edit-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-01234567890abcedf `
    -RemoveEndDate
```

Annullamento di un parco istanze di prenotazione della capacità

Quando non hai più bisogno di un parco istanze di prenotazione della capacità e della capacità questa prenota, puoi annullarla. Quando annulli un parco istanze, il suo stato cambia in `cancelled` e non può più creare nuove prenotazioni di capacità. Inoltre, tutte le singole prenotazioni della capacità nel parco istanze vengono annullate. Le istanze precedentemente in esecuzione nella capacità riservata continuano a essere eseguite normalmente nella capacità condivisa.

AWS CLI

Come annullare un parco di prenotazione della capacità

Utilizza il comando cancel-capacity-reservation-fleets.

```
aws ec2 cancel-capacity-reservation-fleets \
    --capacity-reservation-fleet-ids crf-abcdef01234567890
```

Di seguito è riportato un output di esempio.

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "cancelling",
            "PreviousFleetState": "active",
            "CapacityReservationFleetId": "crf-abcdef01234567890"
        }
    ],
    "FailedFleetCancellations": []
}
```

PowerShell

Come annullare un parco di prenotazione della capacità

Utilizza il cmdlet Stop-EC2CapacityReservationFleet.

```
Stop-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-abcdef01234567890
```

Esempio di configurazione di un parco istanze di prenotazione della capacità

Nell'esempio seguente viene creata un parco istanze di prenotazione della capacità che utilizza due tipi di istanza: `m5.4xlarge` e `m5.12xlarge`.

Utilizza un sistema di ponderazione basato sul numero di vCPU fornito dai tipi di istanza specificati. La capacità target totale è di `480` vCPU. `m5.4xlarge` fornisce 16 vCPU e ottiene un peso di 16, mentre `m5.12xlarge` fornisce 48 vCPU e ottiene un peso di 48. Questo sistema di ponderazione configura il Capacity Reservation Fleet in modo da riservare la capacità per 30 `m5.4xlarge` istanze (480/16=30) o 10 istanze (=10). `m5.12xlarge` 480/48

Il parco istanze è configurato per dare priorità alla capacità `m5.12xlarge` e ottiene la priorità di `1`, mentre `m5.4xlarge`ottiene una priorità inferiore di 2. Ciò significa che la flotta cercherà di riservare

prima la capacità `m5.12xlarge` e farà il tentativo di prenotare `m5.4xlarge` solo se Amazon EC2 non disporrà di sufficiente capacità `m5.12xlarge`.

Il parco istanze prenota la capacità per `Windows` istanze e la prenotazione scade automaticamente il `October 31, 2021` alle `23:59:59` UTC.

```
aws ec2 create-capacity-reservation-fleet \
    --total-target-capacity 480 \
    --allocation-strategy prioritized \
    --instance-match-criteria open \
    --tenancy default \
    --end-date 2021-10-31T23:59:59.000Z \
    --instance-type-specifications file://instanceTypeSpecification.json
```

Di seguito sono riportati i contenuti di `instanceTypeSpecification.json`.

```
[
    {
        "InstanceType": "m5.4xlarge",
        "InstancePlatform":"Windows",
        "Weight": 16,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 2
    },
    {
        "InstanceType": "m5.12xlarge",
        "InstancePlatform":"Windows",
        "Weight": 48,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 1
    }
]
```

Utilizzo di ruoli collegati ai servizi per il parco istanze di prenotazione della capacità

On-Demand Capacity Reservation Fleet utilizza AWS Identity and Access Management ruoli collegati ai servizi (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Capacity Reservation Fleet. Service-linked i ruoli sono predefiniti da Capacity Reservation Fleet e includono tutte le autorizzazioni necessarie al servizio per chiamare altri AWS servizi per conto dell'utente.

Un ruolo collegato al servizio semplifica la configurazione di Capacity Reservation Fleet perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Il parco istanze di prenotazione della capacità definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, solo il parco istanze di prenotazione della capacità potrà assumere i suoi ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato al servizio solo dopo avere eliminato le risorse correlate. Questa procedura protegge le risorse del parco istanze di prenotazione della capacità, poiché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Service-linked autorizzazioni di ruolo per Capacity Reservation Fleet

Capacity Reservation Fleet utilizza il ruolo collegato AWSServiceRoleForEC2CapacityReservationFleet al servizio denominato per creare, descrivere, modificare e annullare le prenotazioni di capacità in una flotta di prenotazioni di capacità per conto dell'utente.

Il ruolo AWSServiceRoleForEC2CapacityReservationFleet collegato al servizio prevede che la seguente entità assuma il ruolo:

- `capacity-reservation-fleet.amazonaws.com`

Il ruolo utilizza la policy gestita. `AWSEC2CapacityReservationFleetRolePolicy` AWS Per ulteriori informazioni, consulta AWS politica gestita: AWSEC2CapacityReservationFleetRolePolicy.

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 il parco istanze di prenotazione della capacità

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un Capacity Reservation Fleet utilizzando il `create-capacity-reservation-fleet` AWS CLI comando o l'`CreateCapacityReservationFleet`API, il ruolo collegato al servizio viene creato automaticamente per te.

Se si elimina questo ruolo collegato ai servizi e quindi deve essere creato di nuovo, è possibile utilizzare lo stesso processo per ricreare il ruolo nell'account. Quando crei un parco istanze di prenotazione della capacità, questo crea nuovamente il ruolo collegato ai servizi per tuo conto.

Modifica di un ruolo collegato ai servizi per il parco istanze di prenotazione della capacità

Capacity Reservation Fleet non consente di modificare il ruolo collegato al AWSServiceRoleForEC2CapacityReservationFleet servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Edit a service-linked role description nella Guida per l'utente IAM.

Eliminazione di un ruolo collegato ai servizi per il parco istanze di prenotazione della capacità

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, consigliamo di eliminare il ruolo. 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 parco istanze di prenotazione della capacità utilizza tale ruolo quando provi a eliminare le risorse, è possibile che l'eliminazione abbia esito negativo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare il ruolo collegato al servizio AWSServiceRoleForEC2CapacityReservationFleet

1. Usa il `delete-capacity-reservation-fleet` AWS CLI comando o l'`DeleteCapacityReservationFleet`API per eliminare le flotte di prenotazioni di capacità nel tuo account.
2. Usa la console IAM AWS CLI, l'API o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForEC2CapacityReservationFleet servizio. Per ulteriori dettagli, consulta Delete a service-linked role nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi del parco istanze di prenotazione della capacità

Il parco istanze di prenotazione della capacità supporta l'utilizzo di ruoli collegati ai servizi in tutte le Regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint di AWS.

Monitora l'utilizzo delle prenotazioni di capacità con delle metriche CloudWatch

Grazie alle CloudWatch metriche, puoi monitorare in modo efficiente le prenotazioni di capacità e identificare la capacità inutilizzata impostando CloudWatch allarmi per notificarti quando vengono

raggiunte le soglie di utilizzo. Questo può aiutare a mantenere un volume Prenotazione della capacità costante e ottenere un livello di utilizzo più elevato.

Le prenotazioni sulla capacità inviano dati metrici ogni cinque minuti. CloudWatch I parametri non sono supportati per Prenotazioni di capacità che sono attivi per meno di cinque minuti.

Per ulteriori informazioni sulla visualizzazione delle metriche nella CloudWatch console, consulta Utilizzo di Amazon CloudWatch Metrics. Per ulteriori informazioni sulla creazione di allarmi, consulta Creazione di allarmi Amazon. CloudWatch

Indice

- Parametri di utilizzo Prenotazione della capacità
- Dimensioni dei parametri Prenotazione della capacità
- Visualizza le CloudWatch metriche relative alle prenotazioni di capacità

Parametri di utilizzo Prenotazione della capacità

Il namespace `AWS/EC2CapacityReservations` include le seguenti metriche di utilizzo che è possibile utilizzare per monitorare e mantenere la capacità su richiesta entro le soglie specificate per la prenotazione.

Parametro	Descrizione
`UsedInstanceCount`	Numero di istanze attualmente in uso. Unità: numero
`AvailableInstanceCount`	Numero di istanze disponibili. Unità: numero
`TotalInstanceCount`	Numero totale di istanze riservate. Unità: numero
`InstanceUtilization`	Percentuale di istanze di capacità riservata attualmente in uso.

Parametro	Descrizione
	Unità: percentuale

Dimensioni dei parametri Prenotazione della capacità

È possibile utilizzare le seguenti dimensioni per perfezionare i parametri elencati nella tabella precedente nella regione e nell'account selezionati.

Dimensione	Description
(Nessuna dimensione)	Questa dimensione filtra il parametro specificato per tutte le prenotazioni della capacità.
`CapacityReservationId`	Questa dimensione filtra il parametro specificato per la prenotazione della capacità identificata.
`InstanceType`	Questa dimensione filtra il parametro specificato per il tipo di istanza identificato.
`AvailabilityZone`	Questa dimensione filtra il parametro specificato per la zona di disponibilità identificata.
`InstanceMatchCriteria`	Questa dimensione filtra il parametro specificato per i criteri di corrispondenza dell'istanza identificati (`open` o `targeted`).
`InstancePlatform`	Questa dimensione filtra i dati di parametro specificati per la piattaforma identificata.
`Tenancy`	Questa dimensione filtra il parametro specificato per la tenancy identificata.

Visualizza le CloudWatch metriche relative alle prenotazioni di capacità

I parametri sono raggruppati in primo luogo in base al namespace del servizio e in secondo luogo in base alle dimensioni supportate. È possibile utilizzare le procedure seguenti per visualizzare i parametri per Prenotazioni di capacità.

Per visualizzare le metriche relative alle prenotazioni di capacità utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo. https://console.aws.amazon.com/cloudwatch/
2. Se necessario, modificare la regione. Dalla barra di navigazione, selezionare la regione dove si trova Prenotazione della capacità. Per ulteriori informazioni, consulta Regioni ed endpoint.
3. Nel riquadro di navigazione, seleziona Parametri.
4. Per Tutti i parametri, scegliere Prenotazione capacità EC2.
5. Scegli tra le precedenti dimensioni dei parametri In tutte le prenotazioni della capacità, Per prenotazione della capacità, Per tipo di istanza, Per zona di disponibilità, Per piattaforma, Per criteri di corrispondenza dell'istanza o Per tenancy e i parametri verranno raggruppati rispettivamente per Nessuna dimensione, `CapacityReservationId`, `InstanceType`, `AvailabilityZone`, `Platform`, `InstanceMatchCriteria` e `Tenancy`.
6. Per ordinare i parametri, utilizza l'intestazione della colonna. Per creare il grafico di un parametro, seleziona la casella di spunta accanto al parametro.

Per visualizzare le metriche relative alla prenotazione della capacità utilizzando il AWS CLI

Utilizza il comando list-metrics seguente:

```
aws cloudwatch list-metrics --namespace "AWS/EC2CapacityReservations"
```

Monitorare il sottoutilizzo delle prenotazioni della capacità

Puoi monitorare il sottoutilizzo della prenotazione della capacità sfruttando i metodi riportati di seguito:

Argomenti

- Eventi Amazon EventBridge
- E-mail e AWS Health Notifiche sulla dashboard

Eventi Amazon EventBridge

AWS Health invia eventi ad Amazon EventBridge quando una prenotazione di capacità nel tuo account è inferiore al 20% di utilizzo in determinati periodi. Con EventBridge, puoi stabilire regole che attivano azioni programmatiche in risposta a tali eventi. Ad esempio, è possibile creare una regola che annulla automaticamente una prenotazione della capacità quando il suo utilizzo è inferiore al 20% in un periodo di 7 giorni.

Gli eventi in EventBridge sono rappresentati come oggetti JSON. I campi univoci per l'evento sono contenuti nella sezione "detail" dell'oggetto JSON. Il campo "event" contiene il nome dell'evento. Il campo "result" contiene lo stato completato dell'operazione che ha attivato l'evento. Per ulteriori informazioni, consulta i modelli di EventBridge eventi di Amazon nella Amazon EventBridge User Guide.

Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

Questa funzionalità non è supportata in AWS GovCloud (US).

Eventi

AWS Health invia i seguenti eventi quando l'utilizzo della capacità per una prenotazione di capacità è inferiore al 20%.

- `AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION`

  Di seguito è riportato un esempio di evento generato quando l'utilizzo della capacità di una prenotazione della capacità appena creata è inferiore al 20% in un periodo di 24 ore.

```
{
    "version": "0",
    "id": "b3e00086-f271-12a1-a36c-55e8ddaa130a",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-10T12:03:38Z",
    "region": "ap-south-1",
    "resources": [
        "cr-01234567890abcdef"
    ],
    "detail": {
```

```
        "eventArn": "arn:aws:health:ap-south-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_cr-01234567890abcdef-6211-4d50-9286-0c9fbc243f04",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION",
        "eventTypeCategory": "accountNotification",
        "startTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "endTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef"
            }
        ]
    }
    }
```

- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

  Di seguito è riportato un esempio di evento generato quando l'utilizzo della capacità di una o più prenotazioni di capacità è inferiore al 20% in un periodo di 7 giorni.

```
{
    "version": "0", "id":"7439d42b-3c7f-ad50-6a88-25e2a70977e2",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-07T06:06:01Z",
    "region": "us-east-1",
    "resources": [
        "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/UNIX | 0.0%",
        "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/UNIX | 0.0%"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/
EC2/AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY/
```

```
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY_726c1732-d6f6-4037-b9b8-
bec3c2d3ba65",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY",
        "eventTypeCategory": "accountNotification",
        "startTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "endTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef | us-east-1b | t3.medium |
 Linux/UNIX | 0.0%"
            },
            {
                "entityValue": "cr-09876543210fedcba | us-east-1a | t3.medium |
 Linux/UNIX | 0.0%"
            }
        ]
    }
}
```

Crea una EventBridge regola

Per ricevere notifiche e-mail quando l'utilizzo di Capacity Reservation scende al di sotto del 20%, crea un argomento Amazon SNS e quindi crea una EventBridge regola per l'`AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATIO`Nevento.

Creazione dell'argomento Amazon SNS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nel riquadro di navigazione scegliere Argomenti, quindi Crea nuovo argomento.
3. Per Tipo, scegliere Standard.
4. Per Nome argomento, inserisci un nome per il nuovo argomento.
5. Scegli Create topic (Crea argomento).

6. Scegli Crea iscrizione.
7. Per Protocollo scegli E-mail, mentre per Endpoint inserisci l'indirizzo e-mail che deve ricevere le notifiche.
8. Scegli Crea iscrizione.
9. L'indirizzo e-mail inserito sopra riceverà un messaggio e-mail con l'oggetto seguente: `AWS Notification - Subscription Confirmation`. Segui le istruzioni per confermare la tu sottoscrizione.

Per creare la regola EventBridge

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Nel riquadro di navigazione scegli Rules (Regole), quindi Create rule (Crea regola).
3. Per Nome, inserisci un nome per la nuova regola.
4. Per Tipo di regola, scegli Regola con un modello di eventi.
5. Scegli Avanti.
6. Per Modello di eventi, procedi come segue:
   a. Per Origine evento, scegli Servizi AWS .
   b. Per Servizio AWS , scegli AWS Health.
   c. Per Tipo di evento, scegli Notifica di sottoutilizzo prenotazione della capacità on demand EC2.
7. Scegli Avanti.
8. Per Destinazione 1, esegui queste operazioni:
   a. Per Tipi di destinazione, scegli servizio AWS .
   b. Per Seleziona una destinazione, scegli Argomento SNS.
   c. Per Argomento, scegli l'argomento che hai creato in precedenza.
9. Scegli Avanti, quindi scegli di nuovo Avanti.
10. Scegli Crea regola.

E-mail e AWS Health Notifiche sulla dashboard

AWS Health invia le seguenti e-mail e Health Dashboard notifiche quando l'utilizzo della capacità per le prenotazioni di capacità nel tuo account scende al di sotto del 20 percento.

- Notifiche individuali per ogni prenotazione della capacità appena creata il cui utilizzo è stato inferiore al 20% nelle ultime 24 ore.
- Una notifica riepilogativa per tutte le prenotazioni di capacità il cui utilizzo è stato inferiore al 20% negli ultimi 7 giorni.

Le notifiche e le Health Dashboard notifiche e-mail vengono inviate all'indirizzo e-mail associato all' AWS account proprietario di Capacity Reservations. Le notifiche includono le seguenti informazioni:

- ID della prenotazione della capacità.
- La zona di disponibilità della prenotazione della capacità.
- Il tasso medio di utilizzo della prenotazione della capacità.
- Il tipo di istanza e la piattaforma (sistema operativo) della prenotazione della capacità.

Inoltre, quando l'utilizzo della capacità per una prenotazione di capacità nel tuo account scende al di sotto del 20 percento in un periodo di 24 ore e 7 giorni, AWS Health invia eventi a. EventBridge ConEventBridge, puoi creare regole che attivano azioni automatiche, come l'invio di notifiche e-mail o l'attivazione di AWS Lambda funzioni, in risposta a tali eventi. Per ulteriori informazioni, consulta Monitorare il sottoutilizzo delle prenotazioni della capacità.

Monitorare le modifiche di stato per le prenotazioni della capacità con data futura

Amazon EC2 invia un evento ad Amazon EventBridge quando lo stato di una prenotazione di capacità con data futura cambia.

Di seguito è illustrato un esempio di questo evento. In questo esempio, la prenotazione della capacità con data futura è entrata nello stato `scheduled`. Nota lo stato evidenziato nel campo `detail-type`.

```
{
   "version":"0",
   "id":"12345678-1234-1234-1234-123456789012",
   "detail-type":"EC2 Capacity Reservation Scheduled",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"yyyy-mm-ddThh:mm:ssZ",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdefg"
   ],
   "detail":{
```

```
      "capacity-reservation-id":"cr-1234567890abcdefg",
      "state":"scheduled"
   }
}
```

I valori possibili per il campo `detail-type` sono:

- `Scheduled`
- `Active`
- `Delayed`
- `Unsupported`
- `Failed`
- `Expired`

Per ulteriori informazioni su questi stati, consulta Visualizza lo stato di una prenotazione della capacità.

Puoi creare EventBridge eventi Amazon che monitorano questi eventi e quindi attivano azioni specifiche quando si verificano. Per ulteriori informazioni, consulta Creazione di regole che reagiscono agli eventi in Amazon EventBridge.

Per creare una regola che monitori tutti gli eventi di modifica dello stato, puoi utilizzare il seguente modello di evento.

```
{
  "source": ["aws.ec2"],
  "detail-type": [{
    "prefix": "EC2 Capacity Reservation"
  }]
}
```

Per creare una regola che monitori solo specifici cambiamenti di stato, puoi utilizzare il seguente modello di evento.

```
{
  "source": ["aws.ec2"],
  "detail-type": [{
    "prefix": "EC2 Capacity Reservation state"
  }]
```

```
}
```

Ad esempio, il seguente modello di evento monitora gli eventi inviati quando una prenotazione della capacità con data futura entra nello stato `active`.

```
{
  "source": ["aws.ec2"],
  "detail-type": [{
    "prefix": "EC2 Capacity Reservation Active"
  }]
}
```

Prenotazioni di capacità interrompibile

Le prenotazioni della capacità interrompibile ti aiutano a rendere temporaneamente disponibile la capacità inutilizzata per altri carichi di lavoro all'interno del tuo account. In questo modo hai il controllo necessario per recuperare la capacità quando necessario. Quando recuperi la capacità, tutte le istanze in esecuzione all'interno della prenotazione interrompibile vengono interrotte. Dopo aver creato una prenotazione interrompibile, puoi condividerla con altri AWS account o con la tua AWS organizzazione utilizzando AWS Resource Access Manager (RAM).

Utilizza le prenotazioni di capacità interrompibili quando hai una capacità riservata inutilizzata durante i periodi non di punta, tra le implementazioni o quando i carichi di lavoro si riducono. Se conosci un altro team che potrebbe utilizzare questa capacità, puoi renderla disponibile creando una prenotazione di capacità interrompibile. Quando è necessario ripristinare la capacità del carico di lavoro critico, è possibile recuperarla.

Puoi utilizzare le prenotazioni di capacità interrompibili come una delle seguenti opzioni:

- Proprietario della capacità: possiedi la Capacity Reservation di origine e crei la Capacity Reservation interrompibile per condividere la capacità inutilizzata con altri team mantenendo il controllo per recuperarla quando necessario.
- Consumatore di capacità: avvii le istanze in prenotazioni interrompibili condivise, con la consapevolezza che le istanze possono essere chiuse quando il proprietario recupera la capacità.

Argomenti

- Come funziona
- Fatturazione

- Considerazioni
- Prenotazioni di capacità interrompibile per i proprietari di capacità
- Prenotazioni di capacità interrompibile per i consumatori di capacità
- Monitora le prenotazioni di capacità interrompibile con e EventBridge CloudTrail

Come funziona

Per rendere disponibile la capacità inutilizzata ad altri team, crea una prenotazione interrompibile specificando il numero di istanze inutilizzate che desideri condividere dalla tua prenotazione di origine. Quando crei la prenotazione interrompibile, trasferiamo queste istanze dalla tua prenotazione di origine alla nuova prenotazione interrompibile all'interno del tuo account.

Manteniamo l'associazione tra la prenotazione alla fonte e la prenotazione della capacità interrompibile. Di conseguenza, quando si recupera la capacità, tutte le istanze consumer in esecuzione vengono interrotte e la capacità viene ripristinata alla prenotazione di origine originale.

Caratteristiche principali:

- Rendi temporaneamente disponibile la capacità inutilizzata mantenendo il controllo per recuperarla
- Recupera la capacità in qualsiasi momento. Per ulteriori informazioni, consulta Processo di recupero e tracciamento
- Condividi con altri account o con la tua AWS organizzazione utilizzando AWS Resource Access Manager (RAM)

Fatturazione

Quando crei una prenotazione interrompibile, ti viene fatturata come nuova prenotazione indipendente. Questo suddivide la fatturazione:

- Prenotazione alla fonte: ti viene addebitata la capacità totale meno la capacità allocata
- Prenotazione interrompibile: ti viene addebitata la capacità allocata

Per ulteriori informazioni sulla fatturazione di On-Demand Capacity Reservation, vedi Prezzi e fatturazione di Capacity Reservation.

Considerazioni

Prima di utilizzare le prenotazioni di capacità interrompibili, consulta le seguenti limitazioni e requisiti che si applicano ai proprietari di capacità e ai consumatori.

Proprietari di capacità

- Non è possibile modificare o annullare direttamente una prenotazione di capacità interrompibile. Per modificarla, aggiorna la capacità allocata dall'origine Capacity Reservation.
- Puoi visualizzare, avviare, taggare, condividere e assegnare la fatturazione solo per le prenotazioni interrompibili.
- È possibile creare una sola allocazione interrompibile per ogni Capacity Reservation di origine.

Consumatori di capacità

- Le prenotazioni di capacità interrompibile sono prenotazioni di capacità mirate per impostazione predefinita, quindi è necessario impostarle come target al momento del lancio dell'istanza.
- Non è possibile aggiungere prenotazioni di capacità interrompibili ai gruppi di prenotazione di capacità.
- Ti consigliamo di utilizzare le prenotazioni di capacità interrompibili solo per le applicazioni che possono essere interrotte.
- Le tue istanze verranno chiuse quando il proprietario recupererà la capacità, senza possibilità di ricorrere a Spot. On-Demand Per ulteriori informazioni, consulta Esperienza di interruzione.

Prenotazioni di capacità interrompibile per i proprietari di capacità

Il proprietario della capacità è l'account proprietario della prenotazione della capacità di origine e crea la prenotazione della capacità interrompibile per condividere la capacità inutilizzata con altri team mantenendo il controllo per recuperarla quando necessario.

Questa sezione spiega come tu (il proprietario della capacità) puoi creare, modificare, recuperare e tenere traccia di una prenotazione di capacità interrompibile.

Argomenti

- Creazione di una prenotazione di capacità interrompibile
- Visualizza la tua prenotazione di capacità interrompibile
- Modifica della prenotazione della capacità interrompibile

- Mantenimento della riserva di capacità interrompibile a capacità zero
- Processo di recupero e tracciamento
- Condivisione delle prenotazioni interrompibili

Creazione di una prenotazione di capacità interrompibile

Crea una prenotazione di capacità interrompibile per rendere disponibile la capacità inutilizzata della prenotazione di origine per altri carichi di lavoro mantenendo il controllo per recuperarla quando necessario.

Prerequisiti

Prima di creare un'allocazione interrompibile, assicurati che la tua prenotazione di capacità di origine soddisfi questi requisiti: On-Demand

- La prenotazione della capacità deve essere attiva senza una data di fine impostata. Non è possibile creare allocazioni da prenotazioni in sospeso, scadute, annullate o con date di fine programmate.
- La tua prenotazione di capacità deve avere una capacità disponibile per l'allocazione. È possibile allocare solo le istanze disponibili (denominate anche capacità inutilizzata).
- È possibile creare una sola allocazione interrompibile per Capacity Reservation di origine. Se esiste già un'allocazione, è necessario modificarla o annullarla prima di crearne una nuova.
- È possibile allocare un massimo di 1000 istanze contemporaneamente a una prenotazione di capacità interrompibile.

È possibile utilizzare la console o la AWS CLI per creare una prenotazione di capacità interrompibile.

Console

Per creare una prenotazione di capacità interrompibile

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegli Prenotazioni di capacità.
3. Seleziona la tua prenotazione di capacità.
4. Scegli Azioni, Crea una prenotazione interrompibile.
5. Per Quantità, inserisci il numero di istanze da allocare.
6. Per la preferenza di allocazione quando viene recuperata tutta la capacità, scegli Predefinito o Conserva.

7. (Facoltativo) Aggiungi tag.
8. Scegli Crea prenotazione interrompibile.

AWS CLI

Per creare una prenotazione di capacità interrompibile

Usa il comando https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/create-interruptible-capacity-reservation-allocation.html create-interruptible-capacity-reservation-allocation:

```
aws ec2 create-interruptible-capacity-reservation-allocation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --instance-count 10
```

Visualizza la tua prenotazione di capacità interrompibile

Dopo aver creato una prenotazione di capacità interrompibile, puoi visualizzarla nel tuo account o da una risorsa specifica.

Visualizza tutte le prenotazioni di capacità interrompibile nel tuo account

Utilizza la seguente procedura per visualizzare le prenotazioni di capacità interrompibile nel tuo account.

Console

Per visualizzare le prenotazioni di capacità interrompibile nel tuo account

1. Vai alla pagina Prenotazioni di capacità nella console.
2. Nella colonna Interrompibile, cerca le prenotazioni contrassegnate con Sì.
3. Seleziona la prenotazione interrompibile per visualizzare i dettagli.

AWS CLI

Per visualizzare le prenotazioni di capacità interrompibile nel tuo account

```
aws ec2 describe-capacity-reservations \
    --capacity-reservation-id cr-interruptible-id \
```

```
    --filters Name=interruptible,Values=true
```

Visualizza la prenotazione di capacità interrompibile da una fonte specifica

Utilizzare la procedura seguente per visualizzare la prenotazione di capacità interrompibile creata da una fonte specifica.

```
aws ec2 describe-capacity-reservations \
    --capacity-reservation-id cr-source-id
```

Nella risposta, troverai un `interruptibleCapacityAllocation` oggetto che contiene il Capacity Reservation ID interrompibile e i dettagli dell'allocazione. Per informazioni sulla struttura della risposta, consulta l'API InterruptibleCapacityAllocation Reference di Amazon EC2.

Modifica della prenotazione della capacità interrompibile

Utilizza le seguenti procedure per modificare o cancellare la tua prenotazione di capacità interrompibile.

> **Note**
>
> - Quando riduci l'allocazione, recuperiamo prima le istanze disponibili, quindi le istanze in esecuzione, fino a raggiungere il numero richiesto. Se riusciamo a soddisfare il conteggio interamente con le istanze disponibili, non si verifica alcuna chiusura. Tutte le modifiche al numero di istanze allocate vengono apportate tramite la Capacity Reservation di origine, non direttamente sulla Capacity Reservation interrompibile.
> - È possibile modificare una prenotazione di capacità interrompibile solo di un massimo di 1000 istanze contemporaneamente (aumento o diminuzione).

Modifica la tua prenotazione di capacità interrompibile

Utilizza la seguente procedura per modificare la tua prenotazione di capacità interrompibile.

Console

1. Dalla pagina dei dettagli della prenotazione della capacità di origine, scegli il link Modifica allocazione interrompibile.

2. Per Quantità, inserisci il nuovo numero:
   - Aggiungi più capacità da condividere
   - Recupera la capacità dalla tua prenotazione di capacità di origine
3. Scegliere Aggiorna.

AWS CLI

```
aws ec2 update-interruptible-capacity-reservation-allocation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --target-instance-count 80
```

Annulla la tua prenotazione di capacità interrompibile

Utilizza la seguente procedura per rimuovere definitivamente l'allocazione e restituire tutta la capacità.

Console

1. Dalla pagina dei dettagli della prenotazione della capacità di origine, accedi ai dettagli sull'allocazione della capacità interrompibile.
2. Scegli Modifica allocazione interrompibile.
3. Per Quantità, inserisci. `0`
4. Scegliere Aggiorna.

AWS CLI

```
aws ec2 update-interruptible-capacity-reservation-allocation \
--capacity-reservation-id cr-1234567890abcdef0 \
--target-instance-count 0
```

Mantieni la preferenza di dimensione zero

Se hai configurato `retain` la preferenza di dimensione zero, la prenotazione della capacità interrompibile rimane attiva a zero istanze. Per annullarla, aggiorna la preferenza relativa

alla `default` dimensione zero e quindi riduci l'allocazione a zero. Per ulteriori informazioni, consulta Mantenimento della riserva di capacità interrompibile a capacità zero.

Mantenimento della riserva di capacità interrompibile a capacità zero

Per impostazione predefinita, Amazon EC2 annulla la prenotazione interrompibile quando ne riduci l'allocazione a zero istanze. La capacità recuperata ritorna alla Capacity Reservation di origine.

Se prevedi di condividere nuovamente la capacità in un secondo momento, puoi configurare la prenotazione interrompibile in modo che rimanga attiva a zero istanze. Con questa opzione, puoi allocare istanze alla stessa prenotazione in un secondo momento senza ricrearla.

Puoi controllare questo comportamento con la preferenza di dimensione zero. È possibile impostarlo quando si crea o si modifica un'allocazione di prenotazione della capacità interrompibile, nella console o con. AWS CLI

Console

Nella pagina Crea prenotazione interrompibile o Modifica allocazione interrompibile, per la preferenza Allocazione quando viene recuperata tutta la capacità, scegli una delle seguenti opzioni:

- Impostazione predefinita: Amazon EC2 annulla la prenotazione di capacità interrompibile quando ne riduci l'allocazione a zero.
- Conservazione: la prenotazione della capacità interrompibile rimane attiva a capacità zero quando si riduce l'allocazione a zero. È quindi possibile allocare nuovamente le istanze in un secondo momento.

Dopo aver salvato la modifica, l'impostazione appare come campo di preferenza Zero size di sola lettura nei dettagli della prenotazione della capacità interrompibile.

AWS CLI

Per mantenere attiva la prenotazione della capacità interrompibile a capacità zero, specifica `--zero-size-preference retain` quando chiami create-interruptible-capacity-reservation-allocation o update-interruptible-capacity-reservation-allocation. https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/create-interruptible-capacity-reservation-allocation.html https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/update-interruptible-

capacity-reservation-allocation.html Per cancellare la prenotazione quando la sua allocazione raggiunge lo zero, `default` specifica.

```
aws ec2 update-interruptible-capacity-reservation-allocation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --zero-size-preference retain
```

Processo di recupero e tracciamento

Quando recuperi la capacità:

- Le istanze in esecuzione ricevono un avviso di interruzione di 2 minuti in caso di eventi. EventBridge
- Dopo il periodo di preavviso, le istanze in esecuzione nella capacità recuperata entrano in stato di arresto e vengono terminate.
- Una volta terminate, le istanze recuperate diventano disponibili nella Capacity Reservation di origine per un utilizzo immediato.
- Lo stato dell'allocazione cambia da aggiornamento a attivo una volta completato.

Il recupero completo può richiedere alcuni minuti a seconda del tipo di istanza e del tempo di spegnimento. Per ulteriori informazioni sulla EventBridge notifica che ricevi al termine del processo, consulta. Completamento del recupero

Tieni traccia dello stato del reclamo

Monitora l'avanzamento del recupero descrivendo la tua prenotazione di origine:

```
aws ec2 describe-capacity-reservations \
--capacity-reservation-id cr-1234567890abcdef0
```

La risposta mostra questi campi all'interno dell'oggetto: `interruptibleCapacityAllocation`

- `instance-count`: istanze attualmente allocate
- `target-instance-count`: Quantità richiesta dopo il recupero
- `status`: aggiornato durante il recupero e attivo una volta completato

Condivisione delle prenotazioni interrompibili

Puoi condividere le prenotazioni interrompibili solo all'interno della tua AWS organizzazione utilizzando AWS Resource Access Manager (RAM).

Considerazioni:

- Se un account utente lascia l'organizzazione, la prenotazione interrompibile viene automaticamente annullata da quell'account.
- Tutte le istanze in esecuzione nella prenotazione non condivisa vengono infine interrotte.
- Tutte le altre funzionalità di condivisione funzionano come le prenotazioni di capacità standard.

Per le procedure di condivisione complete, vedere Sharing Capacity Reservations.

Prenotazioni di capacità interrompibile per i consumatori di capacità

Il consumatore di capacità è l'account che avvia le istanze in prenotazioni di capacità interrompibili condivise, fermo restando che le istanze possono essere chiuse quando il proprietario recupera la capacità.

Questa sezione spiega come l'utente (consumatore di capacità) può avviare le istanze in una Capacity Reservation interrompibile e scoprire cosa succede quando la capacità viene recuperata dal proprietario.

Argomenti

- Visualizza una prenotazione di capacità interrompibile
- Avvia le istanze in prenotazioni interrompibili
- Esperienza di interruzione

Visualizza una prenotazione di capacità interrompibile

Utilizza le seguenti procedure per visualizzare una prenotazione di capacità interrompibile.

Console

Per visualizzare le prenotazioni di capacità interrompibile nel tuo account

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Scegli Prenotazioni di capacità.
3. Nella colonna Interrompibile, cerca le prenotazioni contrassegnate con Sì.
4. Annota gli ID di prenotazione da utilizzare nei lanci dell'istanza.

AWS CLI

Per trovare tutte le prenotazioni di capacità interrompibili nel tuo account

Utilizza il comando describe-capacity-reservations:

```
aws ec2 describe-capacity-reservations \
--filters Name=state,Values=active
```

Cerca le prenotazioni dove `Interruptible` è impostato `true` nella risposta.

Per filtrare specificamente le prenotazioni interrompibili

Utilizza il seguente comando:

```
aws ec2 describe-capacity-reservations \
--capacity-reservation-ids cr-example123 \
--query 'CapacityReservations[?Interruptible==`true`]'
```

> **Note**
>
> Le prenotazioni di capacità interrompibile sono per impostazione predefinita mirate alle prenotazioni di capacità, quindi è necessario impostarle in modo specifico al momento del lancio dell'istanza. A differenza delle prenotazioni aperte, le prenotazioni interrompibili non copriranno automaticamente le istanze corrispondenti. È necessario specificare esplicitamente l'ID della prenotazione al momento dell'avvio.

Avvia le istanze in prenotazioni interrompibili

Utilizza la seguente procedura per avviare le istanze Amazon EC2 in prenotazioni di capacità interrompibili all'interno del tuo account.

> **Note**
>
> Ti consigliamo di utilizzare le prenotazioni di capacità interrompibili solo per le applicazioni che possono essere interrotte.

Console

Per avviare le istanze in prenotazioni di capacità interrompibili

1. Apri la console Amazon Amazon EC2 all'indirizzo. https://console.aws.amazon.com/ec2/
2. Dal pannello di controllo Amazon EC2, selezionare Launch Instance (Avvia istanza).
3. Configura le impostazioni dell'istanza.
4. In Dettagli avanzati per Capacity Reservation, scegli Avvia istanze interrompibili nella tua prenotazione attiva.
5. Seleziona l'ID di prenotazione interrompibile e l'opzione di acquisto di una nuova istanza.
6. Scegliere Launch Instance (Avvia istanza).

AWS CLI

```
aws ec2 run-instances \
--instance-type m5.large \
--count 2 \
--image-id ami-12345678 \
--instance-market-options '{
    "MarketType": "interruptible-capacity-reservation"
}' \
--capacity-reservation-specification '{
    "CapacityReservationTarget": {
        "CapacityReservationId": "cr-abcdef1234567890"
    }
}'
```

Avvia le istanze con Auto Scaling Groups

Puoi anche avviare le istanze in prenotazioni interrompibili utilizzando Auto Scaling Groups con modelli di avvio. Configura il modello di lancio con il tipo di mercato interrompibile e l'ID

di prenotazione, quindi crea il tuo Auto Scaling Group utilizzando quel modello. Per ulteriori informazioni, consulta Prenotazioni di capacità interrompibile con EC2 Auto Scaling.

Esperienza di interruzione

Quando la capacità viene recuperata dal proprietario, riceverai un avviso di interruzione 2 minuti prima della chiusura dell'istanza. Questo avviso viene emesso attraverso EventBridge gli eventi, dandoti il tempo di:

- Salvate il vostro lavoro o controllate le vostre candidature
- Chiudi i processi
- Preparati, ad esempio, alla cessazione

L' EventBridge evento include dettagli sulle istanze che verranno chiuse e l'ora esatta di chiusura. Per ulteriori informazioni, consulta Avviso di interruzione dell'istanza.

Monitora le prenotazioni di capacità interrompibile con e EventBridge CloudTrail

Le prenotazioni di capacità interrompibile inviano EventBridge notifiche ed CloudTrail eventi per aiutarti a monitorare e rispondere alle modifiche della capacità.

Argomenti

- EventBridge notifiche
- CloudTrail eventi

EventBridge notifiche

Ricevi due tipi di EventBridge notifiche. Per informazioni su come configurare EventBridge le notifiche, consulta Creazione di EventBridge regole Amazon.

Avviso di interruzione dell'istanza

Se stai eseguendo istanze in una prenotazione interrompibile, ricevi questa notifica 2 minuti prima della chiusura delle istanze:

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Capacity Reservation Instance Interruption Warning",
    "source": "aws.ec2",
```

```
    "account": "[instance owner Account ID]",
    "time": "[Current time in yyyy-mm-ddThh:mm:ssZ]",
    "resources": "[instance arn]",
    "region": "[region]",
    "detail": {
        "instance-id": "[instance-id]",
        "instance-action": "terminate",
        "instance-termination-time": "yyyy-mm-ddThh:mm:ssZ",
        "azId": "[availability-zone-id]"
    }
}
```

Completamento del recupero

Se sei il proprietario della prenotazione di origine, riceverai questa notifica al termine del recupero della capacità:

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Interruptible Capacity Reservation Allocation Reclamation
 Completed",
    "source": "aws.ec2",
    "account": "[source Capacity Reservation Owner Account ID]",
    "time": "[Current time in yyyy-mm-ddThh:mm:ssZ]",
    "region": "us-east-1",
    "resources": ["source_cr_arn"],
    "detail": {
        "sourceCapacityReservationId": "string",
        "instanceType": "string",
        "availabilityZoneId": "string",
        "TotalInstanceCount": "current total count in the source",
        "ReclaimedInstanceCount": "count of instances added to the source",
        "targetInstanceCount": "number"
    }
}
```

CloudTrail eventi

CloudTrail registra questi eventi per le prenotazioni di capacità interrompibili:

- `InterruptibleCapacityReservationCreated`— Quando si crea un'allocazione interrompibile

- `InterruptibleCapacityReservationAllocationUpdated`— Quando si modifica l'allocazione
- `InterruptibleCapacityReservationCancelled`— Quando si annulla l'allocazione
- `CapacityReservationModified`— Quando modifichiamo la prenotazione di origine per l'allocazione
- `InterruptibleCapacityReservationInstancesTerminated`— Quando interrompiamo le istanze durante il recupero

Blocchi di capacità per ML

I Capacity Block for ML consentono di riservare istanze di elaborazione GPU-based accelerate in una data futura per supportare i carichi di lavoro di machine learning (ML) di breve durata. Le istanze eseguite all'interno di un Capacity Block vengono automaticamente posizionate vicine tra loro all'interno di Amazon EC2 UltraClusters, per una rete a bassa latenza, su scala petabit e non bloccante.

Puoi anche utilizzare Capacity Blocks per riservare capacità per Amazon EC2. UltraServers UltraServers connetti più istanze Amazon EC2 all'interno di un'interconnessione acceleratrice a bassa latenza e larghezza di banda elevata. Puoi utilizzarlo UltraServers per gestire i carichi di lavoro più impegnativi AI/ML in termini di elaborazione e memoria durante l'addestramento, la messa a punto e l'inferenza. Per ulteriori informazioni, consulta Amazon EC2 UltraServers.

Con Blocchi di capacità puoi vedere quando la capacità dell'istanza GPU sarà disponibile nelle date future e pianificare l'avvio di un blocco di capacità di modo che inizi nel momento più adatto alle tue esigenze. Quando prenoti un blocco di capacità, ottieni una garanzia di capacità prevedibile per le istanze GPU pagando solo per il tempo necessario. Ti consigliamo di ricorrere ai blocchi di capacità quando hai bisogno di GPU per supportare i tuoi carichi di lavoro ML per giorni o settimane alla volta e non vuoi pagare una prenotazione mentre le tue istanze GPU non sono in uso.

Di seguito sono elencati alcuni casi d'uso comuni dei blocchi di capacità.

- Addestramento e fine-tuning dei modelli di ML: ottieni un accesso ininterrotto alle istanze GPU che hai prenotato per completare l'addestramento e il fine-tuning dei modelli di ML.
- Esperimenti e prototipi di ML: esegui esperimenti e crea prototipi che richiedono istanze GPU per brevi periodi.

I blocchi di capacità sono disponibili per determinati tipi di istanza in alcune regioni. AWS Per ulteriori informazioni, consulta Tipi di istanze e regioni supportati.

Puoi prenotare un blocco di capacità con un orario di inizio della prenotazione fino a otto settimane nel futuro. Ogni blocco di capacità può avere fino a 64 istanze e puoi avere fino a 256 istanze tra i blocchi di capacità.

Argomenti

- Tipi di istanze e regioni supportati
- Piattaforme supportate
- Considerazioni
- Risorse correlate
- Come funzionano i Capacity Block di Amazon EC2
- Prezzi e fatturazione di Blocchi di capacità
- Ricerca e acquisto di blocchi di capacità
- Avvio di istanze utilizzando blocchi di capacità
- Visualizzazione dei blocchi di capacità
- Estensione dei blocchi di capacità
- Condivisione dei blocchi di capacità
- Crea un gruppo di risorse per la prenotazione di UltraServer capacità per i blocchi di capacità
- Monitora i blocchi di capacità utilizzando EventBridge
- La capacità di registrazione blocca le chiamate API con AWS CloudTrail

Tipi di istanze e regioni supportati

I blocchi UltraServer di istanza e capacità possono essere utilizzati con i seguenti tipi di istanza e AWS aree.

> **Note**
>
> Le dimensioni dei blocchi di capacità pari a 64 istanze non sono supportate per tutti i tipi di istanze in tutte le Regioni AWS.

Blocchi di capacità delle istanze

Tipo di istanz	Sta Uni orie (Vir sett ona us-eas	Sta Uni orie (Oh us-eas	Sta Uni occ li (Ca ia sett ona us-wes	Sta Uni occ li (Or us-wes	Eur (Sto a) eu-nor 1	Eur (Lo eu-wes	Eur (Sp eu-sou 2	Asi Pac (To ap-nor ast-	Asi Pac (Se ap-nor ast-	Asi Pac (Mu ap-sou 1	Asi Pac (Hyi d) ap-sou 2	Asi Pac (Sy ap-sou ast-	Asi Pac (Gia) ap-sou ast-	Asi Pac (Me e) ap-sou ast-	Am del Suc (Sa Pac sa-eas	AW Gov (US Eas us-gov ea st-1	AW Gov (US We usa gov w est-	Sta Uni orie (Atl us-eas - atl-2	Stati Uniti occidenta li (Phoenix) us-west-2 - phx-2a
p6-b300. 8xla	✓			✓					✓		✓		✓			✓		✓	
p6-b200. 8xla	✓	✓		✓						✓	✓					✓	✓		
p5.4x e	✓	✓		✓		✓		✓		✓		✓			✓				
p5.48 ge	✓	✓	✓	✓	✓	✓		✓		✓		✓	✓		✓			✓	
p5e.4 rge	✓	✓	✓	✓	✓	✓		✓		✓		✓	✓		✓				✓
p5en. arge	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓						
p4d.2 rge	✓	✓		✓															
p4de. arge	✓			✓															

Tipo di istanz	Sta Uni orie (Vir sett ona us- eas	Sta Uni orie (Oh us- eas	Sta Uni occ li (Ca ia sett ona us- wes	Sta Uni occ li (Or us- wes	Eur (Sto a) eu- nor 1	Eur (Lo eu- wes	Eur (Sp eu- sou 2	Asi Pac (To ap- nor ast-	Asi Pac (Se ap- nor ast-	Asi Pac (Mu ap- sou 1	Asi Pac (Hy d) ap- sou 2	Asi Pac (Sy ap- sou ast-	Asi Pac (Gia) ap- sou ast-	Asi Pac (Me e) ap- sou ast-	Am del Suc (Sa Pac sa- eas	AW Gov (US Eas us- gov ea st-1	AW Gov (US We usa gov w est-	Sta Uni orie (Atl us- eas - atl-2	Stati Uniti occidenta li (Phoenix) us- west-2 - phx-2a
trn1. arge	✓	✓		✓	✓					✓		✓		✓					
trn2. rge														✓	✓				
trn2. arge		✓																	

UltraServer Blocchi di capacità

Tipo di istanza	Stati Uniti orientali (Ohio) us-east-2	Stati Uniti orientali (Dallas) us-east-1-dfw-2a
Trn2	✓	
P6e-GB200		✓

Piattaforme supportate

I Capacity Blocks for ML attualmente supportano solo le istanze e hanno una tenancy predefinita. UltraServers Quando si utilizza Console di gestione AWS per acquistare un Capacity Block, l'opzione predefinita della piattaforma è. Linux/UNIX Quando si utilizza AWS Command Line Interface (AWS CLI) o AWS SDK per acquistare un Capacity Block, sono disponibili le seguenti opzioni di piattaforma:

- Linux/Unix
- Red Hat Enterprise Linux
- RHEL con HA
- SUSE Linux
- Ubuntu Pro

Considerazioni

Prima di utilizzare i blocchi di capacità, considera i seguenti dettagli e limitazioni.

- Se viene rilevata una riduzione di valore in un UltraServer Capacity Block, riceverai una notifica, ma in genere le istanze non vengono terminate sul Capacity Block. Questo serve a ridurre al minimo eventuali interruzioni involontarie dei tuoi carichi di lavoro. Dopo aver ricevuto questa notifica, puoi continuare a utilizzare il UltraServer Capacity Block così com'è oppure richiederne la correzione chiudendo tutte le istanze presenti nel blocco di capacità e inviando una richiesta di supporto. AWS Dopo aver ricevuto la richiesta di supporto, riceverai una notifica quando la correzione è completa e potrai riavviare le istanze sul tuo Capacity Block. UltraServer
- Per i `P6e-GB200` UltraServer Capacity Block, devi chiudere le istanze almeno 60 minuti prima dell'orario di fine del Capacity Block.
- Per acquistare e utilizzare i Capacity Block nelle zone locali, devi aver aderito alle zone locali.
- Ogni blocco di capacità può avere fino a 64 istanze e puoi avere fino a 256 istanze tra i blocchi di capacità.
- Puoi descrivere le offerte dei blocchi di capacità che possono iniziare entro 30 minuti.
- I blocchi di capacità terminano alle 11:30 UTC (tempo coordinato universale).
- Il processo di terminazione per le istanze in esecuzione in un blocco di capacità inizia alle 11:00 UTC (tempo coordinato universale) dell'ultimo giorno della prenotazione.
- I blocchi di capacità possono essere prenotati con un orario di inizio fino a 8 settimane nel futuro.
- Non sono ammesse cancellazioni dei blocchi di capacità.
- UltraServer I blocchi di capacità non possono essere condivisi tra AWS gli account o all'interno AWS dell'organizzazione.
- Il blocco di capacità non può essere spostato o diviso.
- Puoi aggiungere sia blocchi di UltraServer capacità che blocchi di capacità di istanza a un gruppo di risorse per la prenotazione delle capacità. Per ulteriori informazioni, consulta Gruppi di risorse per la prenotazione della capacità.

- I Capacity Block non supportano i gruppi di collocamento. Non puoi specificare un gruppo di collocamento quando avvii le istanze in un Capacity Block, sia che tu scelga come target il Capacity Block tramite il relativo ID di prenotazione o tramite un Capacity Reservation Resource Group.
- Il numero totale di istanze che possono essere prenotate in Capacity Blocks in tutti gli account AWS dell'organizzazione non può superare le 256 istanze in una data particolare.
- Per utilizzare un blocco di capacità, le istanze devono avere come destinazione specifica l'ID di prenotazione.
- Le istanze in un Capacity Block non vengono conteggiate ai fini dei limiti delle istanze. On-Demand
- Per le istanze P5 che utilizzano un'AMI personalizzata, assicurati di disporre del software e della configurazione necessari per EFA.
- Per i gruppi di nodi gestiti di Amazon EKS, consulta Creare un gruppo di nodi gestiti con Blocchi di capacità Amazon EC2 per ML. Per i gruppi di nodi autogestiti di Amazon EKS, consulta Usa blocchi di capacità per ML con nodi autogestiti.

Risorse correlate

Dopo aver creato un blocco di capacità, puoi compiere le operazioni seguenti con il blocco di capacità:

- Avvio di istanze nel blocco di capacità. Per ulteriori informazioni, consulta Avvio di istanze utilizzando blocchi di capacità.
- Gruppo con Amazon EC2 Auto Scaling. Per ulteriori informazioni, consulta Usa i blocchi di capacità per carichi di lavoro di machine learning nella Guida per l'utente di Amazon EC2 Auto Scaling.

> **Note**
>
> Se utilizzi Amazon EC2 Auto Scaling o Amazon EKS, puoi pianificare la scalabilità in modo tale che venga eseguita all'inizio della prenotazione del blocco di capacità. Grazie alla scalabilità pianificata, gestisce AWS automaticamente i tentativi al posto tuo, quindi non devi preoccuparti di implementare la logica dei tentativi per gestire gli errori transitori.

- Migliora i flussi di lavoro ML con Parallel Computing Service. AWS Per ulteriori informazioni, consulta Supporto di Capacity Blocks per AWS Parallel Computing Service.

- Migliora i flussi di lavoro ML con AWS ParallelCluster. Per ulteriori informazioni, consulta Miglioramento dei flussi di lavoro ML con AWS ParallelCluster e Amazon EC2 Capacity Blocks for ML.

Per ulteriori informazioni su AWS Parallel Computing Service, consulta What is AWS Parallel Computing Service.

Per ulteriori informazioni su AWS ParallelCluster, vedi Cos'è AWS ParallelCluster.

Come funzionano i Capacity Block di Amazon EC2

Puoi riservare un blocco di capacità con le seguenti specifiche:

- Riserva un orario di inizio con un anticipo massimo di 8 settimane
- Imposta una durata della prenotazione compresa tra 1 e 14 giorni o un multiplo di 7 giorni, fino a un massimo di 182 giorni (esempi: 21 giorni, 28 giorni)
- Configura fino a 64 istanze per blocco di capacità
- Configura fino a 256 istanze su più blocchi di capacità

Per Amazon EC2 UltraServers, ciascuno UltraServer corrisponde a un blocco di capacità. Puoi richiederne più UltraServers tramite una singola richiesta.

Per prenotare un Capacity Block, devi innanzitutto specificare le tue esigenze di capacità, tra cui il tipo o UltraServer il tipo di istanza, il numero di istanze o UltraServers, la quantità di tempo, la prima data di inizio e la data di fine più recente di cui hai bisogno. Quindi, puoi visualizzare un'offerta per un blocco di capacità disponibile che soddisfa le tue specifiche. L'offerta per il blocco di capacità include dettagli come l'ora di inizio, la zona di disponibilità e il prezzo di prenotazione. Il prezzo di un'offerta per un blocco di capacità dipende dalla domanda e dall'offerta disponibili al momento della trasmissione dell'offerta. Dopo la prenotazione, il prezzo di un blocco di capacità non cambia. Per ulteriori informazioni, consulta Prezzi e fatturazione di Blocchi di capacità.

Quando acquisti un'offerta per un blocco di capacità, la prenotazione viene creata per la data e il numero di istanze che hai selezionato. Quando inizia la prenotazione del blocco di capacità, puoi scegliere come destinazione gli avvii delle istanze specificando l'ID di prenotazione nelle richieste di avvio.

Puoi utilizzare tutte le istanze prenotate fino a 30 minuti (ad esempio i tipi) o 60 minuti (per il UltraServer tipo) prima dell'orario di fine del Capacity Block. Con 30 minuti (ad esempio per i tipi)

o 60 minuti (per UltraServer i tipi) rimasti nella prenotazione del Capacity Block, tutte le istanze in esecuzione nel Capacity Block iniziano a terminare. Questo tempo viene utilizzato per ripulire le istanze prima di consegnare il Capacity Block al cliente successivo. Un evento viene emesso fino a EventBridge 10 minuti prima dell'inizio del processo di terminazione. Per ulteriori informazioni, consulta Monitora i blocchi di capacità utilizzando EventBridge.

Prezzi e fatturazione di Blocchi di capacità

Con Blocchi di capacità per ML di Amazon EC2, il pagamento avviene in base alle prenotazioni. Il prezzo di un blocco di capacità dipende dalla domanda e dall'offerta di blocchi di capacità disponibili al momento dell'acquisto. Puoi visualizzare il prezzo di un'offerta per un blocco di capacità prima di prenotarlo. Il prezzo del blocco di capacità viene addebitato in anticipo al momento della prenotazione. Quando cerchi un Capacity Block in un intervallo di date, viene restituita l'offerta di Capacity Block con il prezzo più basso disponibile. Dopo la prenotazione, il prezzo di un blocco di capacità non cambia.

Quando utilizzi un blocco di capacità, paghi per il sistema operativo che utilizzi quando le istanze sono in esecuzione. Per ulteriori informazioni sui prezzi dei sistemi operativi, consulta Blocchi di capacità Amazon EC2 per ML.

Fatturazione

Il prezzo di un'offerta per un blocco di capacità viene addebitato in anticipo. Il pagamento viene fatturato sul tuo account AWS da 5 minuti a 12 ore dall'acquisto di un blocco di capacità. Durante l'elaborazione del pagamento, la risorsa di prenotazione del blocco di capacità rimane nello stato `payment-pending`. Se il pagamento non può essere elaborato almeno 5 minuti prima dell'inizio del blocco o entro 12 ore (a seconda dell'evento che si verifica per primo), il blocco di capacità viene rilasciato e lo stato della prenotazione cambia in `payment-failed`.

Dopo la corretta elaborazione del pagamento, lo stato delle risorse del blocco di capacità passa da `payment-pending` a `scheduled`. Riceverai una fattura che riflette il pagamento anticipato una tantum. Nella fattura, puoi associare l'importo pagato all'ID di prenotazione del blocco di capacità.

Quando inizia la prenotazione del blocco di capacità, la fatturazione viene effettuata solo in base al sistema operativo utilizzato mentre le istanze sono in esecuzione nella prenotazione. Puoi visualizzare l'utilizzo e gli addebiti associati nella fattura alla ricorrenza dall'attivazione del servizio per il mese di utilizzo nel tuo AWS Cost and Usage Report.

> **Note**
>
> Gli sconti Savings Plans e per le istanze riservate non si applicano ai blocchi di capacità.

Visualizzazione di una fattura

Puoi visualizzare la fattura nella console. Gestione costi e fatturazione AWS Il pagamento anticipato per il blocco di capacità viene visualizzato nel mese in cui hai acquistato la prenotazione.

Dopo l'inizio della prenotazione, la fattura riporta righe separate per il tempo di prenotazione in blocco utilizzato e quello inutilizzato. Puoi utilizzare queste voci per controllare quanto tempo della prenotazione è stato utilizzato. Nella riga verrà visualizzato solo il costo di utilizzo per il tempo impiegato, se utilizzi un sistema operativo premium. Per ulteriori informazioni, consulta Prezzi e fatturazione di Blocchi di capacità. Il tempo inutilizzato non comporta costi supplementari.

Per ulteriori informazioni, consulta Visualizzazione della fattura nella Guida per l'utente di Gestione costi e fatturazione AWS .

Se il blocco di capacità inizia in un mese diverso da quello in cui hai acquistato la prenotazione, il prezzo corrisposto in anticipo e l'utilizzo della prenotazione vengono visualizzati in mesi di fatturazione distinti. Nel tuo AWS Cost and Usage Report, l'ID di prenotazione Capacity Block è riportato nella `reservation/ReservationARN` voce della tariffa anticipata e `lineitem/ResourceID` nella fattura di anniversario, in modo da poter associare l'utilizzo al prezzo iniziale corrispondente.

Ricerca e acquisto di blocchi di capacità

Per prenotare un blocco di capacità, devi prima trovare un periodo di tempo in cui la capacità è disponibile che soddisfi le tue esigenze. Per trovare un blocco di capacità disponibile per la prenotazione, è necessario specificare quanto segue.

- Il numero di istanze necessarie
- Il periodo di tempo per il quale ti occorrono le istanze
- L'intervallo di date per le quali ti occorre la prenotazione

Per cercare un'offerta per un blocco di capacità disponibile, devi specificare la durata della prenotazione e il numero di istanze. Devi specificare la durata della prenotazione in incrementi di 1 giorno fino a un massimo di 14 giorni e in incrementi di 7 giorni fino a un massimo di 182 giorni. Ogni blocco di capacità può avere fino a 64 istanze e puoi avere fino a 256 istanze tra i blocchi di capacità.

Quando richiedi un Capacity Block che corrisponde alle tue specifiche, vengono restituiti i dettagli di un massimo di 6 blocchi disponibili. Tutti i blocchi di capacità terminano alle 11:30 UTC, quindi i blocchi che iniziano lo stesso giorno avranno durate che si avvicinano di più alla durata desiderata. Un blocco avrà una durata leggermente inferiore alla tua durata desiderata, mentre l'altro avrà una durata leggermente superiore alla durata desiderata.

I dettagli dell'offerta includono l'ora di inizio della prenotazione, la zona di disponibilità per la prenotazione e il prezzo della prenotazione. Per ulteriori informazioni, consulta Prezzi e fatturazione di Blocchi di capacità.

Puoi acquistare l'offerta per il blocco di capacità che ti viene mostrata oppure modificare i criteri di ricerca per visualizzare le altre opzioni disponibili. Non esiste una scadenza predefinita per l'offerta, tuttavia le offerte sono assegnate secondo l'ordine di conferma delle richieste.

Quando acquisti un'offerta per un blocco di capacità, ricevi una risposta immediata che conferma che il tuo blocco di capacità è stato prenotato. Dopo la conferma, nel tuo account verrà visualizzata una nuova prenotazione della capacità con un tipo di prenotazione `capacity-block` e un valore `start-date` impostato sull'ora di inizio dell'offerta che hai acquistato. La tua prenotazione di un blocco di capacità viene creata con uno stato di `payment-pending`. Dopo la corretta elaborazione del pagamento anticipato, lo stato della prenotazione diventa `scheduled`. Per ulteriori informazioni, consulta Fatturazione.

> **Note**
>
> Per acquistare e utilizzare i blocchi di capacità nelle zone locali, è necessario accedere alle zone locali.

Console

Ricerca e acquisto di un blocco di capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore della schermata, seleziona una Regione AWS. Questa scelta è importante perché le dimensioni dei blocchi di capacità pari a 64 istanze non sono supportate per tutti i tipi di istanze in tutte le regioni.
3. Nel riquadro di navigazione, scegli Prenotazioni della capacità, Crea blocchi di capacità.
4. In Tipi di blocchi di capacità, scegli Istanze o. UltraServers

5. In Attributi di capacità, puoi definire i parametri di ricerca del blocco di capacità. Per impostazione predefinita, la piattaforma è Linux. Se desideri selezionare un sistema operativo diverso, utilizza la AWS CLI. Per ulteriori informazioni, consulta Piattaforme supportate.
6. In Capacità totale (per istanze) o UltraServer Numero (per UltraServers), specifica il numero di istanze UltraServers che desideri riservare.
7. In Durata, inserisci il numero di giorni o settimane per cui è necessaria la prenotazione.
8. Nella sezione Intervallo di date per la ricerca dei blocchi di capacità, inserisci la prima data in cui desideri iniziare la prenotazione.
9. Scegli Cerca blocchi di capacità.
10. Se è disponibile un blocco di capacità che soddisfa le tue specifiche, vedrai un'offerta nella sezione Blocchi di capacità consigliati. Se sono presenti più offerte che soddisfano le tue specifiche, viene mostrata l'offerta per il blocco di capacità più in anticipo possibile. Per visualizzare altre offerte per blocchi di capacità, modifica gli input di ricerca e scegli nuovamente Cerca blocchi di capacità.
11. Quando trovi un'offerta per un blocco di capacità che desideri acquistare, scegli Avanti.
12. (Facoltativo) Nella pagina Aggiungi tag, scegli Aggiungi nuovo tag.
13. La pagina Verifica e acquista elenca la data di inizio e di fine, la durata, il numero totale di istanze e il prezzo.

> **Note**
>
> Non è possibile annullare i blocchi di capacità dopo averli prenotati.

14. Nella finestra popup Acquista un blocco di capacità, digita conferma, quindi scegli Acquista.

AWS CLI

Per trovare un'istanza Blocco di capacità

Utilizza il comando describe-capacity-block-offerings.

Il seguente esempio trova l'istanza Blocchi di capacità.

```
aws ec2 describe-capacity-block-offerings \
--instance-type p5.48xlarge \
--instance-count 16 \
```

```
--start-date-range 2023-08-14T00:00:00Z \
--end-date-range 2023-10-22-T00:00:00Z \
--capacity-duration-hours 48 \
--all-availability-zones
```

L'esempio seguente trova i blocchi di UltraServer capacità.

```
aws ec2 describe-capacity-block-offerings \
--ultraserver-type u-p6e-gb200x72 \
--ultraserver-count 1 \
--start-date-range 2023-08-14T00:00:00Z \
--end-date-range 2023-10-22-T00:00:00Z \
--capacity-duration-hours 48
```

Per acquistare un blocco di capacità

Utilizza il comando purchase-capacity-block con l'ID dell'offerta del blocco di capacità dall'output dell'esempio precedente.

```
aws ec2 purchase-capacity-block \
--capacity-block-offering-id cb-0123456789abcdefg \
--instance-platform Linux/UNIX
```

PowerShell

Per trovare i blocchi di capacità

Utilizza il cmdlet Get-EC2CapacityBlockOffering.

Il seguente esempio trova l'istanza Blocchi di capacità.

```
Get-EC2CapacityBlockOffering `
-InstanceType p5.48xlarge `
-InstanceCount 16 `
-CapacityDurationHour 48 `
-StartDateRange 2023-08-14T00:00:00Z `
-EndDateRange 2023-10-22-T00:00:00Z `
-AllAvailabilityZones $true
```

L'esempio seguente trova i Blocchi UltraServer di capacità.

```
Get-EC2CapacityBlockOffering `
-UltraserverType u-p6e-gb200x72 `
-UltraserverCount  1 `
-CapacityDurationHour 48 `
-StartDateRange 2023-08-14T00:00:00Z `
-EndDateRange 2023-10-22-T00:00:00Z
```

Per acquistare un blocco di capacità

Utilizza il New-EC2EC2CapacityBlock cmdlet con l'ID di offerta del Capacity Block indicato nell'output dell'esempio precedente.

```
New-EC2EC2CapacityBlock `
-CapacityBlockOfferingId cb-0123456789abcdefg `
-InstancePlatform Linux/UNIX
```

Avvio di istanze utilizzando blocchi di capacità

Per utilizzare il blocco di capacità, devi specificare l'ID di prenotazione del blocco di capacità all'avvio delle istanze. L'avvio di un'istanza in un blocco di capacità ne riduce la capacità disponibile in misura pari al numero di istanze avviate. Ad esempio, se la capacità dell'istanza acquistata è di otto istanze e ne avvii quattro, la capacità disponibile viene ridotta di quattro unità.

Se termini un'istanza in esecuzione nel blocco di capacità prima della fine della prenotazione, puoi avviare una nuova istanza al suo posto. Quando si arresta o si termina un'istanza in un blocco di capacità, occorrono diversi minuti per ripulire l'istanza prima di poterne avviare un'altra per sostituirla. Durante questo periodo, l'istanza si troverà in uno stato di arresto o `shutting-down`. Una volta completato questo processo, lo stato dell'istanza diventa `stopped` o `terminated`. Quindi, la capacità disponibile nel blocco di capacità verrà aggiornata per mostrare un'altra istanza disponibile per l'uso.

Requisiti

- L'istanza non può essere avviata in una sottorete ubicata in una zona di disponibilità diversa da quella in cui si trova il blocco di capacità.
- L'istanza non può essere avviata utilizzando un'AMI con una piattaforma diversa da quella per il blocco di capacità.
- Per utilizzare i blocchi di capacità nelle zone locali, è necessario accedere alla zona locale.

Console

Avvio di istanze in un blocco di capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore della schermata, seleziona la regione della prenotazione del blocco di capacità.
3. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).
4. Segui la procedura per avviare un'istanza.
5. Espandi Dettagli avanzati e, come Opzione di acquisto, scegli Blocchi di capacità. Poi esegui una delle seguenti operazioni:
   - Per avviare le istanze in un blocco di capacità specifico, per Prenotazione della capacità seleziona Specifica la prenotazione della capacità, quindi seleziona il blocco di capacità.
   - (UltraServers solo) Per avviare le istanze in un gruppo di risorse UltraServer Capacity Block Capacity Reservation, per Capacity Reservation scegli Specifica Capacity Reservation Resource Group, quindi seleziona il Capacity Reservation Resource Group.
6. Scegliere Launch Instance (Avvia istanza).

AWS CLI

Avvio di istanze in un blocco di capacità

Utilizza il comando run-instances con l'opzione `instance-market-options MarketType`.

L'esempio seguente avvia un'istanza in un blocco di capacità specifico.

```
aws ec2 run-instances \
--image-id ami-0abcdef1234567890 \
--count 1 \
--instance-type p5.48xlarge \
--key-name my-key-pair \
--subnet-id subnet-0abcdef1234567890 \
--instance-market-options MarketType='capacity-block' \
--capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_block_id}
```

L'esempio seguente avvia un'istanza in un UltraServer Capacity Block Capacity Reservation Reservation Group.

```
aws ec2 run-instances \
--image-id ami-0abcdef1234567890 \
--count 1 \
--instance-type p6e-gb200.36xlarge \
--key-name my-key-pair \
--subnet-id subnet-0abcdef1234567890 \
--instance-market-options MarketType='capacity-block' \
--capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=resource_group_arn}
```

PowerShell

Avvio di istanze in un blocco di capacità

Utilizzare il New-EC2Instance cmdlet con l'`-InstanceMarketOption`opzione definita come segue.

```
$marketoption = New-Object Amazon.EC2.Model.InstanceMarketOptionsRequest
$marketoption.MarketType = "capacity-block"
```

L'esempio seguente avvia un'istanza in un blocco di capacità specifico.

```
New-EC2Instance `
-ImageId ami-0abcdef1234567890 `
-InstanceType p5.48xlarge `
-KeyName "my-key-pair" `
-SubnetId subnet-0abcdef1234567890 `
-InstanceMarketOptions $marketoption `
-CapacityReservationTarget_CapacityReservationId capacity_block_id
```

L'esempio seguente avvia un'istanza in un gruppo di risorse UltraServer Capacity Block Capacity Reservation.

```
New-EC2Instance `
-ImageId ami-0abcdef1234567890 `
-InstanceType p6e-gb200.36xlarge `
-KeyName "my-key-pair" `
-SubnetId subnet-0abcdef1234567890 `
-InstanceMarketOptions $marketoption `
-CapacityReservationTarget_CapacityReservationResourceGroupArn "resource_group_arn"
```

Risorse correlate

- Per creare un modello di avvio destinato a un blocco di capacità, consulta the section called "Modelli di avvio".
- Per avviare le istanze in un blocco di capacità utilizzando il parco istanze EC2, consulta Tutorial: Configura il tuo parco istanze EC2 per avviare istanze in Blocchi di capacità.
- Per configurare un gruppo di nodi gestito da EKS con un blocco di capacità, consulta Creare un gruppo di nodi gestito con blocchi di capacità per il ML nella Guida per l'utente di Amazon EKS.
- Per configurare AWS ParallelCluster l'utilizzo di un Capacity Block, vedere ML on AWS ParallelCluster.

Visualizzazione dei blocchi di capacità

Dopo aver prenotato un blocco di capacità, puoi visualizzare la rispettiva prenotazione nel tuo account AWS . Puoi visualizzare `start-date` e `end-date` per vedere quando la prenotazione avrà inizio e fine. Prima dell'inizio di una prenotazione di blocco di capacità, la capacità disponibile visualizzata è pari a zero. Puoi vedere quante istanze saranno disponibili nel blocco di capacità in base al valore del tag per la chiave del tag `aws:ec2capacityreservation:incrementalRequestedQuantity`.

Quando inizia la prenotazione di un blocco di capacità, lo stato della prenotazione passa da `scheduled` a `active`. Un evento viene emesso tramite Amazon EventBridge per notificarti che il Capacity Block è disponibile per l'uso. Per ulteriori informazioni, consulta Monitora i blocchi di capacità utilizzando EventBridge.

I blocchi di capacità possono assumere i seguenti stati:

- `payment-pending`: il pagamento anticipato non è stato ancora elaborato.
- `payment-failed`: non è stato possibile elaborare il pagamento nell'arco di 12 ore. Il tuo blocco di capacità è stato rilasciato.
- `scheduled`: il pagamento è stato elaborato e la prenotazione del blocco di capacità non è ancora iniziata.
- `active`: la capacità riservata è disponibile per l'utilizzo.
- `expired`: la prenotazione del blocco di capacità è scaduta automaticamente alla data e ora specificate nella richiesta di prenotazione. La capacità riservata non è più disponibile per l'utilizzo.

Console

Per visualizzare i blocchi di capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Nella pagina Panoramica delle prenotazioni di capacità, viene visualizzata una tabella delle risorse con i dettagli su tutte le tue risorse di prenotazione della capacità. Per trovare le tue prenotazioni di blocchi di capacità, seleziona Blocchi di capacità dall'elenco a discesa sopra l'ID di prenotazione della capacità. Nella tabella puoi visualizzare informazioni sui tuoi blocchi di capacità, come date di inizio e fine, durata e stato.
4. Per maggiori dettagli su un blocco di capacità, seleziona l'ID di prenotazione corrispondente al blocco di capacità che desideri visualizzare. La pagina Dettagli della prenotazione della capacità mostra tutte le proprietà della prenotazione e il numero di istanze in uso e disponibili nel blocco di capacità.

> **Note**
>
> Prima dell'inizio di una prenotazione di blocco di capacità, la capacità disponibile visualizzata è pari a zero. Puoi vedere quante istanze saranno disponibili quando inizia la prenotazione del blocco di capacità in base al valore del tag per la chiave del tag `aws:ec2capacityreservation:incrementalRequestedQuantity`.

AWS CLI

Per visualizzare i blocchi di capacità

Usa il comando describe-capacity-blocks per visualizzare i dettagli sulle tue prenotazioni Capacity Block.

```
aws ec2 describe-capacity-blocks
```

PowerShell

Per visualizzare i blocchi di capacità

Usa il Get-EC2CapacityBlock cmdlet per visualizzare i dettagli sulle tue prenotazioni Capacity Block.

```
Get-EC2CapacityBlock
```

Estensione dei blocchi di capacità

Con i blocchi di capacità, prenoti la capacità di elaborazione per i tuoi carichi di lavoro, garantendo disponibilità e coerenza. Per adattare al mutamento delle esigenze, puoi estendere la durata dei blocchi di capacità esistenti, in base alla necessità.

Per estendere un blocco di capacità, deve avere uno stato di `active` o `scheduled` e non avere estensioni che sono `payment-pending`. Puoi richiedere di estendere la durata del Capacity Block fino a un minimo di 1 ora o un massimo di 57 giorni prima della scadenza. Puoi estendere il tuo blocco di capacità con incrementi di 1 giorno fino a 14 giorni e con incrementi di 7 giorni fino a un massimo di 182 giorni (26 settimane) in totale. Quando estendi il blocco di capacità, la data di fine verrà aggiornata in modo tale che le istanze possano continuare a funzionare senza interruzioni.

- Non esiste alcun limite al numero di estensioni che è possibile applicare a un blocco di capacità
- L'ID di prenotazione della capacità rimarrà lo stesso dopo aver esteso il blocco
- I blocchi di capacità possono essere estesi solo se è disponibile una capacità sufficiente per supportarli, il che non è garantito.

Fatturazione

Il prezzo di un'offerta per un blocco di capacità viene addebitato in anticipo. L'estensione rimarrà in `payment-pending` fino al pagamento della fattura. Se il pagamento non può essere elaborato entro 12 ore o fino a 35 minuti prima del termine programmato del blocco di capacità (a seconda dell'evento che si verifica per primo), l'estensione avrà esito negativo e lo stato cambierà in `payment-failed`. La prenotazione del blocco di capacità rimarrà `active` e terminerà alla data di fine originale.

Una volta che il pagamento è stato elaborato con successo, lo stato di estensione del blocco di capacità cambia in `payment-succeeded` e la data di fine della prenotazione del blocco di capacità verrà aggiornata alla nuova data di fine. I dettagli dell'estensione possono essere visualizzati nella sezione Dettagli di estensione del blocco di capacità della console o utilizzando il comando describe-capacity-block-extension-history.

Estensione del blocco di capacità

Console

Per estendere il blocco di capacità

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Nella pagina Panoramica delle prenotazioni della capacità, viene visualizzata una tabella delle risorse con i dettagli su tutte le tue risorse di prenotazione della capacità. Seleziona l'ID della prenotazione per il blocco di capacità che desideri estendere.
4. Dal menu a discesa Operazioni, scegli Estendi blocco di capacità.
5. In Durata, inserisci il numero di giorni o settimane per cui è necessario estendere la prenotazione.
6. Scegli Cerca blocco di capacità.
7. Se è disponibile un blocco di capacità che soddisfa le tue specifiche, appare un'offerta nella sezione Blocchi di capacità consigliati. Per visualizzare altre offerte per blocchi di capacità, modifica gli input di ricerca e scegli nuovamente Cerca blocchi di capacità.
8. Quando trovi un'offerta per un blocco di capacità che desideri acquistare, scegli Estendi.
9. Nella finestra pop-up Estendi blocco di capacità, inserisci Conferma, poi scegli Estendi.

AWS CLI

Per cercare un'estensione del blocco di capacità

Utilizza il comando describe-capacity-block-extension-offerings. L'esempio seguente cerca un'estensione del blocco di capacità di 48 ore per la prenotazione specificata.

```
aws ec2 describe-capacity-block-extension-offerings \
    --capacity-reservation-id cr-1234567890abcdefg \
    --capacity-block-extension-duration-hours 48
```

Per estendere il blocco di capacità

Utilizza il comando purchase-capacity-block-extension. Specifica l'ID dell'offerta dell'estensione dall'output dell'esempio precedente.

```
aws ec2 purchase-capacity-block-extension \
```

```
    --capacity-block-extension-offering-id cbe-0123456789abcdefg \
    --capacity-reservation-id cr-1234567890abcdefg
```

PowerShell

Per cercare un'estensione del blocco di capacità

Utilizza il cmdlet Get-EC2CapacityBlockExtensionOffering. L'esempio seguente cerca un'estensione del blocco di capacità di 48 ore per la prenotazione specificata.

```
Get-EC2CapacityBlockExtensionOffering `
    -CapacityReservationId cr-1234567890abcdefg `
    -CapacityBlockExtensionDurationHour 48
```

Per estendere il blocco di capacità

Utilizza il cmdlet Invoke-EC2CapacityBlockExtension. Specifica l'ID dell'offerta dell'estensione dall'output dell'esempio precedente.

```
Invoke-EC2CapacityBlockExtension `
    -CapacityBlockExtensionOfferingId cbe-0123456789abcdefg `
    -CapacityReservationId cr-1234567890abcdefg
```

Condivisione dei blocchi di capacità

La condivisione dei Capacity Block consente ai proprietari di Capacity Block di condividere i Capacity Block di Amazon EC2 con altri AWS account all'interno di un' AWS organizzazione. Ciò consente di massimizzare l'utilizzo della capacità GPU riservata tra diversi team e progetti per utilizzare in modo efficiente i Capacity Block.

L' AWS account che possiede il Capacity Block (proprietario) può condividerlo con altri AWS account (consumatori). Un proprietario può condividere un Capacity Block con AWS account specifici all'interno della propria AWS organizzazione, con un'unità organizzativa all'interno AWS dell'organizzazione o con l'intera AWS organizzazione. I consumatori possono avviare le istanze nei Capacity Block condivisi con loro nello stesso modo in cui avviano le istanze nei Capacity Block di loro proprietà.

Prerequisiti per la condivisione dei blocchi di capacità

Prima di poter condividere un Blocco di Capacità, devono essere soddisfatte le seguenti condizioni:

- Devi essere il proprietario del Blocco di capacità: non puoi condividere un Blocco di capacità che è stato condiviso con te.
- Lo stato del Blocco di capacità deve essere attivo o pianificato: i Blocchi di capacità che si trovano in altri stati, ad esempio `expired` o `payment-pending` non possono essere condivisi.
- Condivisione solo all'interno AWS della propria organizzazione: un proprietario può condividere un Blocco di capacità con AWS account specifici all'interno AWS della propria organizzazione, un'unità organizzativa all'interno della propria AWS organizzazione o l'intera AWS organizzazione.
- UltraServer Blocchi di capacità non supportati: non è possibile condividere blocchi di capacità per Amazon EC2 UltraServers.
- Idoneità dell'account: la condivisione dei Capacity Block non è disponibile per AWS i nuovi account o per AWS gli account con una cronologia di fatturazione limitata.

Servizi correlati

La condivisione di Capacity Block si integra con AWS Resource Access Manager ().AWS RAM AWS RAM è un servizio che ti consente di condividere AWS le tue risorse con qualsiasi AWS account o tramite AWS Organizations. Con AWS RAM, condividi le risorse di cui sei proprietario creando una condivisione delle risorse. Una condivisione delle risorse specifica le risorse da condividere e gli utenti con cui condividerle. I consumatori possono essere singoli AWS account, unità organizzative o un'intera organizzazione di AWS Organizations.

Per ulteriori informazioni AWS RAM, consulta la Guida AWS RAM per l'utente .

Autorizzazioni Shared Capacity Block

Autorizzazioni per i proprietari

Il proprietario del Capacity Block rimane responsabile della gestione del Capacity Block (ad esempio, dell'estensione e della condivisione) e delle istanze in cui viene avviato. I proprietari non possono modificare le istanze che i consumatori avviano nei Capacity Block che hanno condiviso.

Autorizzazioni per gli utenti

I consumatori possono avviare le istanze nella capacità condivisa e sono responsabili della gestione di tali istanze. I consumatori non possono visualizzare o modificare le istanze di proprietà di altri consumatori o del proprietario del Capacity Block. I consumatori possono inoltre visualizzare solo la capacità totale e la capacità disponibile nel Blocco di capacità condiviso.

Condividere un blocco di capacità

Per condividere un Blocco di capacità, devi aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una AWS RAM risorsa che ti consente di condividere le tue risorse tra di loro Account AWS.

Se hai aggiunto il Capacity Block a una condivisione di risorse condivisa con l'intera AWS organizzazione, ai consumatori dell'organizzazione viene concesso l'accesso al Capacity Block condiviso.

Console

Per condividere un Capacity Block di tua proprietà utilizzando la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Seleziona il Capacity Block da condividere e scegli Azioni, Condividi prenotazione.
4. Seleziona la quota di risorse a cui aggiungere il Blocco di capacità e scegli Condividi prenotazione di capacità.

   I consumatori potrebbero impiegare alcuni minuti per accedere al Capacity Block condiviso.

Per aggiungere un Capacity Block a una nuova condivisione di risorse

È necessario innanzitutto creare la condivisione delle risorse utilizzando la AWS RAM console. Per ulteriori informazioni, consulta l'argomento relativo alla creazione di una condivisione di risorse nella Guida per l'utente di AWS RAM .

AWS CLI

Per condividere un Capacity Block di tua proprietà

Utilizzare i comandi create-resource-share e associate-resource-share.

```
aws ram create-resource-share \
    --name my-resource-share \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE
```

```
aws ram associate-resource-share \
```

```
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-
b505-7e2a-420d-6f5d3EXAMPLE \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE
```

PowerShell

Per condividere un Capacity Block di tua proprietà

Usa i Connect-RAMResourceShare cmdlet New-RAMResourceShare and.

```
New-RAMResourceShare `
    -Name my-resource-share `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE"
```

```
Connect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-
b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE"
```

I Capacity Block funzionano in base al principio «primo arrivato, primo servito» per tutti gli account, indipendentemente dallo stato di proprietà. Quando condividi un Capacity Block, se un consumatore avvia le istanze prima del proprietario, tali istanze occupano la capacità fino a quando il consumatore non termina le istanze o fino a 30 minuti prima della scadenza del Capacity Block.

Smetti di condividere un Capacity Block

Puoi interrompere la condivisione di un Blocco di capacità in qualsiasi momento fino a 30 minuti prima della data di scadenza del blocco.

Cosa succede quando interrompi la condivisione:

- I consumatori non possono più lanciare nuove istanze nel Capacity Block che non erano condivise.
- Le istanze in esecuzione continuano a funzionare fino a 30 minuti prima della data di scadenza del Capacity Block, a meno che non venga interrotta dal consumatore.

Console

Per interrompere la condivisione di un Capacity Block di tua proprietà, utilizza la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Seleziona il Capacity Block e scegli la scheda Sharing.
4. La scheda Condivisione elenca le condivisioni di risorse a cui è stato aggiunto il Blocco di capacità. Seleziona la condivisione di risorse da cui rimuovere il Blocco di capacità.
5. Scegli Rimuovi dalla condivisione delle risorse.

AWS CLI

Per interrompere la condivisione di un Capacity Block di tua proprietà

Utilizza il comando disassociate-resource-share.

```
aws ram disassociate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE
```

PowerShell

Per interrompere la condivisione di un Capacity Block di tua proprietà

Utilizza il cmdlet Disconnect-RAMResourceShare.

```
Disconnect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE"
```

Monitora l'utilizzo di Capacity Block

I proprietari dei Capacity Block possono monitorare quali account utilizzano i Capacity Block condivisi e tenere traccia dell'utilizzo delle istanze per account.

AWS CLI

Per monitorare l'utilizzo di un Capacity Block

Usa il comando get-capacity-reservation-usage.

```
aws ec2 get-capacity-reservation-usage \
    --capacity-reservation-id cr-1234abcd56EXAMPLE
```

Questa API consente ai proprietari di:

- Visualizza quali account utilizzano attualmente il Capacity Block.
- Visualizza il numero di istanze in esecuzione per ogni account.

Avvisi di chiusura delle istanze

Gli account proprietario e consumatore con istanze in esecuzione nel Capacity Block riceveranno un EventBridge evento 40 minuti prima della fine della prenotazione del Capacity Block, a indicare che tutte le istanze in esecuzione nella prenotazione inizieranno a terminare tra 10 minuti. Per ulteriori informazioni, consulta Monitora i blocchi di capacità utilizzando EventBridge.

Estensioni Capacity Block

I Capacity Block possono essere estesi mentre sono condivisi. Solo l'account proprietario può estendere un Capacity Block condiviso.

Quando un Capacity Block viene esteso, le istanze in esecuzione avviate dal proprietario o dai consumatori ereditano automaticamente la nuova data di scadenza e i consumatori possono continuare a utilizzare la capacità condivisa fino alla nuova data di scadenza senza alcuna interruzione dell'istanza.

Prezzi e fatturazione

Ai proprietari vengono fatturati i Capacity Block che condividono e pagano in anticipo i Capacity Block al momento dell'acquisto. I proprietari pagano anche i costi del sistema operativo per le istanze eseguite sul Capacity Block.

Ai consumatori vengono fatturati solo i costi del sistema operativo per le istanze eseguite nel Capacity Block condiviso. Ai consumatori non viene addebitato alcun costo per la prenotazione del Capacity Block in sé.

Crea un gruppo di risorse per la prenotazione di UltraServer capacità per i blocchi di capacità

È possibile AWS Resource Groups utilizzarlo per creare raccolte logiche di blocchi di UltraServer capacità. Dopo aver creato il Capacity Reservation Resource Group, puoi aggiungere i UltraServer Capacity Block di tua proprietà nel tuo account. Dopo aver aggiunto i blocchi di UltraServer capacità, puoi indirizzare i lanci delle istanze al Capacity Reservation Resource Group anziché ai singoli blocchi di capacità. Le istanze destinate a un gruppo di risorse per la prenotazione della capacità corrispondono a tutti i blocchi di UltraServer capacità del gruppo con attributi corrispondenti e capacità disponibile. Se il Capacity Reservation Resource Group non dispone di un UltraServer Capacity Block con attributi corrispondenti e capacità disponibile, l'avvio dell'istanza ha esito negativo.

Se un UltraServer Capacity Block viene rimosso da un Capacity Reservation Resource Group mentre vi sono istanze in esecuzione, tali istanze continuano a essere eseguite nel Capacity Block. Se un UltraServer Capacity Block di un gruppo termina mentre sono in esecuzione delle istanze, le istanze vengono terminate.

Per aggiungere blocchi di capacità di istanza a un gruppo di risorse per la prenotazione di capacità, consulta. Gruppi di risorse per la prenotazione della capacità

Per creare un gruppo di risorse di prenotazione delle UltraServer capacità per i blocchi di capacità, utilizza uno dei seguenti metodi.

AWS CLI

Per creare un gruppo di risorse per la prenotazione della capacità per i blocchi UltraServer di capacità

Utilizza il comando AWS CLI create-group e, per `--configuration`, specifica quanto segue:

```
{
  "Configuration": [
    {
      "Type": "AWS::EC2::CapacityReservationPool",
      "Parameters": [
        {
          "Name": "instance-type",
          "Values": [
            "instance_type"
          ]
        },
```

```
        {
          "Name": "reservation-type",
          "Values": [
            "capacity-block"
          ]
        }
      ]
    },
    {
      "Type": "AWS::ResourceGroups::Generic",
      "Parameters": [
        {
          "Name": "allowed-resource-types",
          "Values": [
            "AWS::EC2::CapacityReservation"
          ]
        }
      ]
    }
  ]
}
```

PowerShell

Per creare un gruppo di risorse per la prenotazione della capacità per i blocchi UltraServer di capacità

Utilizza il cmdlet New-RGGroup. Per `-Configuration`, specifica quanto segue:

```
{
  "Configuration": [
    {
      "Type": "AWS::EC2::CapacityReservationPool",
      "Parameters": [
        {
          "Name": "instance-type",
          "Values": [
            "instance_type"
          ]
        },
        {
          "Name": "reservation-type",
          "Values": [
            "capacity-block"
```

```
          ]
        }
      ]
    },
    {
      "Type": "AWS::ResourceGroups::Generic",
      "Parameters": [
        {
          "Name": "allowed-resource-types",
          "Values": [
            "AWS::EC2::CapacityReservation"
          ]
        }
      ]
    }
  ]
}
```

> **Note**
>
> Per aggiungere vari tipi di Capacity Reservation a un UltraServer-only gruppo esistente, devi prima modificare la configurazione del gruppo utilizzando l'API put-group-configuration e rimuovere le `instance-type` sezioni di configurazione e. `reservation-type` Una volta completato, vedi Gruppi di risorse per la prenotazione della capacità per ulteriori operazioni di raggruppamento.

Dopo aver creato un Capacity Resource Group per UltraServer Capacity Block, utilizza uno dei seguenti metodi per aggiungervi i UltraServer Capacity Block esistenti.

AWS CLI

Per aggiungere un blocco UltraServer di capacità a un gruppo di risorse per la prenotazione della capacità

Utilizza il comando group-resources. Per `--group` specificare il nome del gruppo di risorse per la prenotazione delle capacità che hai creato. Per`--resource-arns`, specifica gli ARN dei blocchi di UltraServer capacità da aggiungere.

```
aws resource-groups group-resources \
```

```
--group MyCRGroup \
--resource-arns CapacityReservationArn
```

PowerShell

Per aggiungere un blocco di UltraServer capacità a un gruppo di risorse per la prenotazione di capacità

Utilizza il cmdlet Add-RGResource. Per `-Group` specificare il nome del gruppo di risorse per la prenotazione delle capacità che hai creato. Per`-ResourceArn` , specifica gli ARN dei blocchi di UltraServer capacità da aggiungere.

L'esempio seguente aggiunge due prenotazioni della capacità al gruppo specificato.

```
Add-RGResource `
-Group MyCRGroup `
-ResourceArn CapacityReservationArn
```

Monitora i blocchi di capacità utilizzando EventBridge

Quando inizia la prenotazione di Capacity Block, Amazon EC2 emetterà un evento EventBridge che indica che la capacità è pronta per l'uso. Quaranta minuti prima della scadenza della prenotazione Capacity Block, ricevi un altro EventBridge evento che ti informa che tutte le istanze in esecuzione nella prenotazione inizieranno a terminare tra 10 minuti. Per ulteriori informazioni sugli EventBridge eventi, consulta Amazon Events. EventBridge

Le seguenti strutture di eventi per gli eventi emessi per i blocchi di capacità:

Blocco di capacità fornito

Nell'esempio seguente viene illustrato un evento per un blocco di capacità fornito.

```
{
  "customer_event_id": "[Capacity Reservation Id]-delivered",
  "detail_type": "Capacity Block Delivered",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
```

```
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Avviso di scadenza del blocco di capacità

Nell'esempio seguente viene illustrato un avviso di scadenza per un blocco di capacità.

```
{
  "customer_event_id": "[Capacity Reservation Id]-approaching-expiry",
  "detail_type": "Capacity Block Expiration Warning",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Avviso di interruzione dell'istanza di prenotazione della capacità

L'esempio seguente mostra un evento per l'avviso di interruzione dell'istanza di prenotazione della capacità di EC2.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail_type": "EC2 Capacity Reservation Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "[Customer Account ID]",
    "time": "[Current time]",
    "region": "[Region]",
    "resources": [
        "[Instance ARN]"
    ],
    "detail": {
```

```
        "instance-id": "[Instance ID]",
        "instance-action": "terminate",
        "instance-termination-time": "[Current time]",
        "availability-zone-id": "[Availability Zone ID]",
        "instance-lifecycle": "capacity-block"
    }
}
```

La capacità di registrazione blocca le chiamate API con AWS CloudTrail

Capacity Blocks è integrato con AWS CloudTrail un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Capacity Blocks. CloudTrail acquisisce le chiamate API per i Capacity Blocks come eventi. Le chiamate acquisite includono le chiamate dalla console di Blocchi di capacità e le chiamate di codice alle operazioni delle API di Blocchi di capacità. Se crei un percorso, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per i Capacity Blocks. Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata a Capacity Blocks, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per saperne di più CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni sui blocchi di capacità in CloudTrail

CloudTrail è abilitato sul tuo Account AWS computer quando crei l'account. Quando si verifica un'attività in Capacity Blocks, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo Account AWS, inclusi gli eventi relativi ai Capacity Blocks, crea un percorso. Un percorso consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati degli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso

- CloudTrail servizi e integrazioni supportati
- 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

Tutte le azioni di Capacity Blocks vengono registrate CloudTrail e documentate nell'API Reference di Amazon EC2. Ad esempio, le chiamate e le `CapacityBlockScheduled` `CapacityBlockActive` 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 credenziali utente root o AWS Identity and Access Management (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 AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci di file di log di Blocchi di capacità

Un trail è una configurazione che consente l'invio di eventi come file di registro a un bucket Amazon S3 specificato. CloudTrail i file di log contengono una o più voci di registro. Un evento rappresenta una singola richiesta da qualsiasi sorgente e include informazioni sull'azione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. I file di log di CloudTrail non sono una traccia di stack ordinata delle chiamate API pubbliche, pertanto non vengono visualizzati in un ordine specifico.

Gli esempi seguenti mostrano le voci di CloudTrail registro per:

- TerminateCapacityBlocksInstances
- CapacityBlockPaymentFailed
- CapacityBlockScheduled
- CapacityBlockActive
- CapacityBlockFailed
- CapacityBlockExpired

> **Note**
>
> Alcuni campi degli esempi sono stati oscurati per la privacy dei dati.

TerminateCapacityBlocksInstances

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "TerminateCapacityBlockInstances",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
    }
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:us-east-1:123456789012:instance/i-0598c7d356eba48d7"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      }
}
```

CapacityBlockPaymentFailed


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockPaymentFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "payment-failed"
      }
}
```


CapacityBlockScheduled


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
```

```
  "eventName": "CapacityBlockScheduled",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "scheduled"
      }
}
```

CapacityBlockActive

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockActive",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
```

```
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "active"
      }
 }
```

CapacityBlockFailed

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "failed"
```

```
      }
 }
```

CapacityBlockExpired

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockExpired",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "expired"
      }
 }
```

Gruppi di risorse per la prenotazione della capacità

È possibile utilizzarlo AWS Resource Groups per creare raccolte logiche di prenotazioni di capacità, denominate gruppi di risorse per la prenotazione di capacità (gruppo). Un Capacity Reservation Resource Group è un gruppo di risorse che contiene le prenotazioni di capacità e consente di avviare istanze in più prenotazioni di capacità specificando un singolo ARN del Capacity Reservation

Resource Group. Per ulteriori informazioni sui gruppi di risorse per la prenotazione di capacità, vedi Cosa sono i gruppi di risorse? nella Guida AWS Resource Groups per l'utente.

Quando si specifica un gruppo per avviare le istanze, Amazon EC2 abbina le istanze a qualsiasi Capacity Reservation del gruppo con attributi corrispondenti e capacità disponibile.

Puoi includere le prenotazioni di capacità che possiedi nel tuo account e le prenotazioni di capacità condivise con te da altri AWS account in un unico gruppo. Puoi anche includere le prenotazioni di capacità con attributi diversi (tipo di istanza, piattaforma, zona di disponibilità, locazione e gruppo di collocamento) in un unico gruppo.

Un gruppo supporta tutti i tipi di prenotazione, tra cui On-Demand Capacity Reservations, Capacity Reservations https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/interruptible-capacity-reservations.html interruptible e Capacity Blocks for ML. Puoi aggiungere qualsiasi combinazione di tipi di prenotazione a un singolo gruppo.

Processi

- Creazione di un gruppo
- Aggiungi le prenotazioni di capacità a un gruppo
- Avvia le istanze in Capacity Reservations in un gruppo
- Rimuovi le prenotazioni di capacità da un gruppo
- Ciclo di vita dell'istanza in un gruppo
- Eliminazione di un gruppo

Creazione di un gruppo

Puoi creare un gruppo per organizzare le tue prenotazioni di capacità. Dopo aver creato un gruppo, puoi aggiungere le prenotazioni della capacità al gruppo.

Console

Come creare un gruppo

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Scegli Capacity Reservation Resource Group.
4. Selezionare Create Group (Crea gruppo).

5. Inserisci il nome del gruppo e, facoltativamente, aggiungi una descrizione, Capacity Reservations e tag.
6. Scegli Crea.

AWS CLI

Creazione di un gruppo per le prenotazioni di capacità

Usa il AWS CLI comando create-group con i seguenti parametri di richiesta.

- `AWS::EC2::CapacityReservationPool`— Assicura che il Capacity Reservation Resource Group possa essere mirato, ad esempio, ai lanci.
- `AWS::ResourceGroups::Generic`con `allowed-resource-types` impostato su `AWS::EC2::CapacityReservation` — Assicura che il Capacity Reservation Resource Group accetti solo le prenotazioni di capacità.

```
aws resource-groups create-group \
    --name MyCRGroup \
    --configuration \
        '{"Type": "AWS::EC2::CapacityReservationPool"}' \
        '{"Type": "AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-
resource-types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

PowerShell

Creazione di un gruppo per le prenotazioni di capacità

Utilizza il cmdlet New-RGGroup.

```
New-RGGroup `
    -Name MyCRGroup `
    -Configuration `
        @{"Type"="AWS::EC2::CapacityReservationPool"} `
        @{"Type"="AWS::ResourceGroups::Generic"; "Parameters"=@{"allowed-resource-
types"=@{"Values"="AWS::EC2::CapacityReservation"}}}
```

Per creare un gruppo che accetta solo blocchi di UltraServer capacità di un tipo di istanza specifico, consultaCrea un gruppo di risorse per la prenotazione di UltraServer capacità per i blocchi di capacità.

Aggiungi le prenotazioni di capacità a un gruppo

Puoi aggiungere le prenotazioni di capacità che possiedi nel tuo account o le prenotazioni di capacità condivise con te da altri AWS account di un gruppo.

Considerazioni

- Puoi aggiungere a un gruppo solo le prenotazioni di capacità `active` nello stato.
- Se una prenotazione di capacità condivisa viene successivamente annullata dal suo proprietario, Amazon EC2 la rimuove automaticamente dal tuo gruppo.

Console

Puoi aggiungere Capacity Reservations a un gruppo dalla pagina dei dettagli del Capacity Reservation Reservation Reservation Group o dalla console Capacity Reservation.

Per aggiungere Capacity Reservations dalla pagina Capacity Reservation Resource Group

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Scegli Capacity Reservation Resource Group.
4. Seleziona il nome del gruppo per aprire la relativa pagina dei dettagli.
5. Nella sezione Prenotazioni di capacità, scegli Aggiungi.
6. Seleziona le prenotazioni di capacità che desideri aggiungere, quindi scegli Aggiungi.

Per aggiungere Capacity Reservations dalla console Capacity Reservation

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Seleziona la prenotazione di capacità che desideri aggiungere a un gruppo.
4. Scegli Azione, quindi scegli Aggiungi al gruppo.
5. Seleziona il gruppo, quindi scegli Aggiungi.

AWS CLI

Per aggiungere Capacity Reservations a un gruppo

Utilizza il comando group-resources. Fornisci l'ARN di ogni prenotazione di capacità che desideri aggiungere.

L'esempio seguente aggiunge due prenotazioni della capacità al gruppo specificato.

```
aws resource-groups group-resources \
    --group MyCRGroup \
    --resource-arns \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1
 \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

PowerShell

Per aggiungere le prenotazioni di capacità a un gruppo

Utilizza il cmdlet Add-RGResource.

L'esempio seguente aggiunge due prenotazioni della capacità al gruppo specificato.

```
Add-RGResource `
    -Group MyCRGroup `
    -ResourceArn `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-1234567890abcdef1", `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-54321abcdef567890"
```

Avvia le istanze in Capacity Reservations in un gruppo

È possibile avviare le istanze nelle prenotazioni di capacità esistenti specificando un ARN del Capacity Reservation Resource Group. Le istanze destinate a un gruppo corrispondono a qualsiasi Capacity Reservation del gruppo con attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy) e capacità disponibile corrispondenti.

Quando avvii le istanze utilizzando la procedura guidata di avvio delle istanze o l' RunInstances API, puoi specificare una sola opzione di acquisto (un tipo di prenotazione) per avvio. Per avviare

contemporaneamente più tipi di prenotazione all'interno del gruppo, utilizza i gruppi Amazon EC2 Fleet o Auto Scaling.

Per istruzioni dettagliate su come avviare istanze in più tipi di prenotazione di capacità utilizzando un gruppo di risorse per la prenotazione di capacità, consulta i seguenti tutorial: tramite EC2 Fleet e tramite Amazon EC2 Auto Scaling. ??? https://docs.aws.amazon.com/autoscaling/ec2/userguide/use-distribution-segments.html

On-Demand Prenotazioni di capacità

Per avviare le istanze in On-Demand Capacity Reservations in un gruppo, specifica l'ARN del gruppo utilizzando il `CapacityReservationTarget` parametro con il `CapacityReservationResourceGroupArn` campo.

Amazon EC2 avvia le istanze in qualsiasi On-Demand Capacity Reservation corrispondente nel gruppo. Se non è disponibile alcuna capacità corrispondente, le istanze vengono avviate utilizzando la capacità. On-Demand

Se non desideri che le istanze vengano avviate come On-Demand quando non è disponibile alcuna capacità corrispondente, imposta `CapacityReservationPreference` su. `capacity-reservations-only` Con questa impostazione, le istanze non vengono avviate se nessuna prenotazione di On-Demand capacità corrispondente nel gruppo ha una capacità disponibile.

Console

Per avviare le istanze in On-Demand Capacity Reservations in un gruppo

1. Segui la procedura per avviare un'istanza, ma non avviarla prima di aver completato i passaggi seguenti.
2. Espandi Advanced details (Dettagli avanzati).
3. Per l'opzione Acquisti, lascia come Nessuno (impostazione predefinita).
4. Per Capacity Reservation, scegli Specifica Capacity Reservation Resource Group (impostazione predefinita) o Avvia solo in un Capacity Reservation Resource Group (per evitare il On-Demand fallback), quindi seleziona il gruppo.
5. Scegliere Launch Instance (Avvia istanza).

AWS CLI

Per avviare le istanze in On-Demand Capacity Reservations in un gruppo

Usa il comando run-instances con il parametro. `--capacity-reservation-specification`

L'esempio seguente avvia le istanze in un gruppo. Se il gruppo non dispone di un ODCR con attributi corrispondenti e capacità disponibile, le istanze vengono avviate come istanze. On-Demand

```
aws ec2 run-instances \
    --instance-type c5.xlarge \
    --image-id ami-0abcdef1234567890 \
    --count 3 \
    --capacity-reservation-specification \

 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:sa-east-1:123456789012:group/MyCRGroup}
```

L'esempio seguente avvia le istanze in un gruppo. Se il gruppo non dispone di un ODCR con attributi corrispondenti e capacità disponibile, le istanze non vengono avviate.

```
aws ec2 run-instances \
    --instance-type c5.xlarge \
    --image-id ami-0abcdef1234567890 \
    --count 3 \
    --capacity-reservation-specification \
        CapacityReservationPreference=capacity-reservations-
only,CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:sa-east-1:123456789012:group/MyCRGroup}
```

Destinarsi a un gruppo di collocamento specifico

Facoltativamente, se il tuo gruppo contiene On-Demand Capacity Reservations in un gruppo di collocamento, puoi anche specificare l'ID del gruppo di collocamento insieme all'ARN del Capacity Reservation Resource Group per inserire tutte le istanze avviate in quel gruppo di collocamento.

> **Note**
>
> I Capacity Block non supportano i gruppi di collocamento. Non è possibile specificare un gruppo di collocamento quando la richiesta è indirizzata ai Blocchi di capacità in un gruppo di risorse per la prenotazione delle capacità.

Prenotazioni di capacità interrompibile

Per avviare le istanze in prenotazioni di capacità interrompibile in un gruppo, specifica l'ARN del gruppo e seleziona l'opzione di acquisto interrompibile. Amazon EC2 inserisce le istanze in qualsiasi riserva di capacità interrompibile attiva del gruppo con attributi corrispondenti e capacità disponibile. Se non è disponibile alcuna capacità corrispondente, le istanze non vengono avviate.

Console

Per avviare le istanze in prenotazioni di capacità interrompibili in un gruppo

1. Segui la procedura per avviare un'istanza, ma non avviarla prima di aver completato i passaggi seguenti.
2. Espandi Advanced details (Dettagli avanzati).
3. Per l'opzione di acquisto, scegli Prenotazioni di capacità interrompibile.
4. Per Capacity Reservation, scegli Specifica il gruppo di risorse per la prenotazione della capacità e seleziona il gruppo.
5. Scegliere Launch Instance (Avvia istanza).

AWS CLI

Per avviare le istanze in Capacity Reservations interrompibili in un gruppo

Usa il comando run-instances con i parametri and. `--instance-market-options` `--capacity-reservation-specification`

```
aws ec2 run-instances \
    --instance-type c5.xlarge \
    --image-id ami-0abcdef1234567890 \
    --count 3 \
    --instance-market-options MarketType=interruptible-capacity-reservation \
    --capacity-reservation-specification \

 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup}
```

Blocchi di capacità

Per avviare le istanze nei Capacity Blocks di un gruppo, specifica l'ARN del gruppo e seleziona l'opzione di acquisto dei Capacity Blocks. Amazon EC2 colloca le istanze in qualsiasi Capacity Block attivo del gruppo con attributi corrispondenti e capacità disponibile. Se non è disponibile alcuna capacità corrispondente, le istanze non vengono avviate.

> **Note**
>
> Non è possibile specificare un gruppo di collocamento quando si accede ai blocchi di capacità in un gruppo di risorse per la prenotazione delle capacità.

Console

Per avviare le istanze nei Capacity Blocks di un gruppo

1. Segui la procedura per avviare un'istanza, ma non avviarla prima di aver completato i passaggi seguenti.
2. Espandi Advanced details (Dettagli avanzati).
3. Per l'opzione di acquisto, scegli blocchi di capacità.
4. Per Capacity Reservation, scegli Specifica il gruppo di risorse per la prenotazione della capacità e seleziona il gruppo.
5. Scegliere Launch Instance (Avvia istanza).

AWS CLI

Per avviare le istanze nei blocchi di capacità di un gruppo

Usa il comando run-instances con i parametri and. `--instance-market-options` `--capacity-reservation-specification`

```
aws ec2 run-instances \
    --instance-type p5.48xlarge \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-market-options MarketType=capacity-block \
    --capacity-reservation-specification \
```

```
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:sa-east-1:123456789012:group/MyCRGroup}
```

Rimuovi le prenotazioni di capacità da un gruppo

Puoi rimuovere una prenotazione di capacità da un gruppo in qualsiasi momento. Le istanze destinate al gruppo continuano a funzionare nella loro attuale Capacity Reservation e non sono interessate dalla rimozione. La Capacity Reservation ripristina la capacità solo quando si terminano le istanze.

> **Note**
>
> Se una prenotazione di capacità condivisa con te viene successivamente annullata, Amazon EC2 la rimuove automaticamente dal gruppo.

Console

Per rimuovere Capacity Reservations da un gruppo

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Scegli Capacity Reservation Resource Group.
4. Seleziona il nome del gruppo per aprire la relativa pagina dei dettagli.
5. Nella sezione Prenotazioni di capacità, seleziona le prenotazioni di capacità da rimuovere, quindi scegli Rimuovi.

AWS CLI

Per rimuovere le prenotazioni di capacità da un gruppo

Utilizza il comando ungroup-resources.

Nell'esempio seguente vengono rimosse due prenotazioni della capacità dal gruppo specificato.

```
aws resource-groups ungroup-resources \
    --group MyCRGroup \
```

```
    --resource-arns \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd
\
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

PowerShell

Per rimuovere le prenotazioni di capacità da un gruppo

Utilizza il cmdlet Remove-RGResource.

Nell'esempio seguente vengono rimosse due prenotazioni della capacità dal gruppo specificato.

```
Remove-RGResource `
    -Group MyCRGroup `
    -ResourceArn `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-0e154d26a16094dd", `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-54321abcdef567890"
```

Ciclo di vita dell'istanza in un gruppo

Quando una prenotazione di capacità in un gruppo cambia stato, l'impatto sulle istanze in esecuzione dipende dal tipo di prenotazione.

On-Demand Prenotazioni di capacità

Quando una prenotazione di On-Demand capacità in un gruppo viene annullata, scade o la sua capacità è ridotta, le istanze destinate al gruppo corrispondono a qualsiasi altra prenotazione di On-Demand capacità del gruppo con attributi corrispondenti (tipo di istanza, piattaforma, zona di disponibilità e tenancy) e capacità disponibile. Se il gruppo non dispone di una On-Demand Capacity Reservation con attributi corrispondenti e capacità disponibile, le istanze vengono eseguite utilizzando la capacità. On-Demand Se in un secondo momento aggiungi una prenotazione di On-Demand capacità corrispondente al gruppo, Amazon EC2 sposta automaticamente le istanze nella sua capacità riservata.

Prenotazioni di capacità interrompibile

Quando viene recuperata la capacità di una prenotazione di capacità interrompibile, le istanze ricevono un avviso di interruzione 2 minuti prima della cessazione. Per ulteriori informazioni, consulta

Esperienza di interruzione. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/interruptible-capacity-reservations.html#interruption-experience

Blocchi di capacità

Le istanze in esecuzione in un Capacity Block in un Capacity Reservation Resource Group vengono terminate prima della fine del Capacity Block, come avviene per un Capacity Block indirizzato direttamente. Per ulteriori informazioni, consulta Come funzionano i Capacity Block di Amazon EC2.

Eliminazione di un gruppo

Se non hai più bisogno del tuo gruppo, puoi eliminarlo in qualsiasi momento. Quando elimini un gruppo con istanze in esecuzione e prenotazioni di capacità attive, le istanze destinate al gruppo continuano a funzionare nella loro prenotazione di capacità corrente dopo l'eliminazione del gruppo. Amazon EC2 ripristina la capacità della Capacity Reservation quando si terminano le istanze.

Console

Come eliminare un gruppo

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Prenotazioni di capacità (Host dedicati).
3. Scegli Capacity Reservation Resource Group.
4. Seleziona il gruppo che desideri eliminare, scegli Azione, quindi scegli Elimina.
5. Quando ti viene richiesto di confermare, scegli Elimina.

AWS CLI

Per eliminare un gruppo

Utilizza il comando delete-group.

```
aws resource-groups delete-group --group MyCRGroup
```

PowerShell

Come eliminare un gruppo

Utilizza il cmdlet Remove-RGGroup.

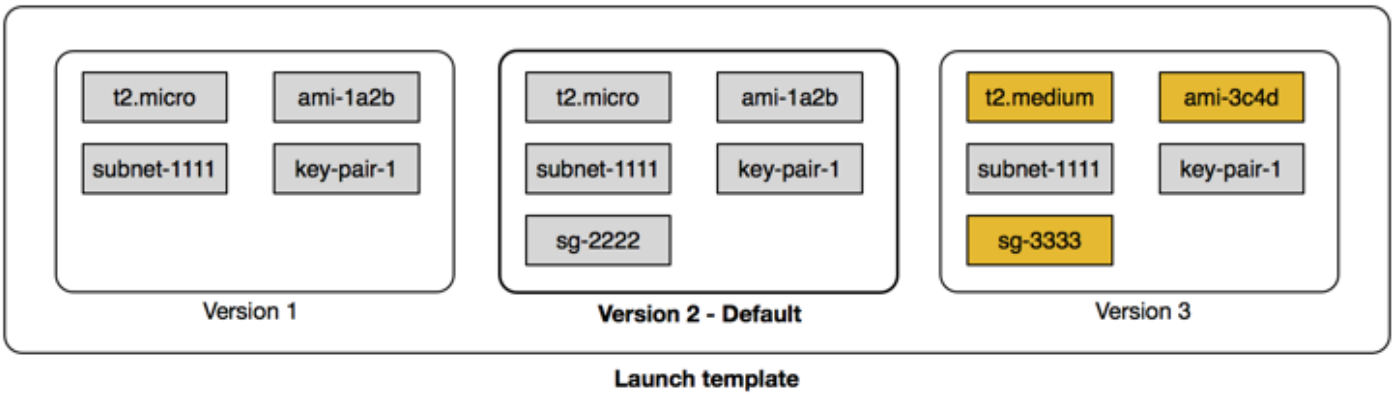
```
Remove-RGGroup -GroupName MyCRGroup
```

Archivia i parametri di avvio dell'istanza nei modelli di avvio di Amazon EC2

È possibile usare modelli di avvio di Amazon EC2 per archiviare i parametri di avvio di istanze in modo da non doverli specificare ogni volta che si avvia un'istanza Amazon EC2. Ad esempio, puoi creare un modello di avvio che archivia l'ID AMI, il tipo di istanza e le impostazioni di rete utilizzati in genere per avviare le istanze. Quando avvii un'istanza utilizzando la console Amazon EC2, un AWS SDK o uno strumento da riga di comando, puoi specificare il modello di avvio invece di immettere nuovamente i parametri.

Per ogni modello di avvio, è possibile creare una o più versioni del modello di avvio numerate. Ogni versione può avere parametri di lancio diversi. Quando avvii un'istanza da un modello di avvio, è possibile utilizzare qualsiasi versione del modello di avvio. Se non specifichi una versione, viene utilizzata la versione predefinita. È possibile impostare qualsiasi versione del modello di avvio come versione predefinita; per impostazione predefinita, è la prima versione del modello di avvio.

Nel seguente diagramma viene indicato il modello di avvio con tre versioni. La prima versione specifica il tipo di istanza, l'ID istanza AMI, la sottorete e la coppia di chiavi da utilizzare per avviare l'istanza. La seconda versione è basata sulla prima versione e specifica anche un gruppo di sicurezza per l'istanza. La terza versione utilizza valori diversi per alcuni parametri. La versione 2 è impostata come versione predefinita. Se avviassi un'istanza da questo modello di avvio, i parametri di lancio dalla versione 2 verrebbero utilizzati se non fosse stata specificata un'altra versione.



Indice

- Restrizioni per i modelli di avvio Amazon EC2
- Autorizzazioni IAM per i modelli di avvio Amazon EC2
- Usa i modelli di avvio di Amazon EC2 per controllare l'avvio delle istanze Amazon EC2
- Creare un modello di avvio Amazon EC2
- Modificare un modello di avvio (gestire le versioni dei modelli di avvio)
- Eliminazione di un modello di avvio o di una versione del modello di avvio

Restrizioni per i modelli di avvio Amazon EC2

Le seguenti restrizioni si applicano ai modelli di avvio e alle versioni del modello di avvio:

- Quote: per visualizzare le quote per i modelli di avvio e le versioni dei modelli di avvio, apri la console Service Quotas o utilizza il comando list-service-quotas. https://docs.aws.amazon.com/cli/latest/reference/service-quotas/list-service-quotas.html AWS CLI Ogni AWS account può avere fino a un massimo di 5.000 modelli di lancio per regione e fino a 10.000 versioni per modello di lancio. I tuoi account potrebbero avere quote diverse in base all'età e alla cronologia di utilizzo.
- I parametri sono facoltativi: i parametri del modello di avvio sono facoltativi. Tuttavia, è necessario verificare che la richiesta di avvio dell'istanza includa tutti i parametri necessari. Ad esempio, se il modello di avvio non include un ID dell'AMI, è necessario specificare sia un ID dell'AMI durante l'avvio di un'istanza con questo modello di avvio.
- I parametri non sono convalidati: i parametri del modello di avvio non sono pienamente convalidati quando crei il modello di avvio. Se si specificano valori errati o si utilizzano combinazioni di parametri non supportate, non sarà possibile avviare istanze utilizzando questo modello di avvio. Per evitare problemi, assicurati di specificare i valori corretti e di utilizzare combinazioni di parametri supportate. Ad esempio, per avviare un'istanza in un gruppo di collocamento, è necessario specificare un tipo di istanza supportato.
- Tag – È possibile assegnare dei tag a un modello di avvio, ma non è possibile assegnare tag a una versione del modello di avvio.
- Immutabilità: i modelli di avvio sono immutabili. Per modificare un modello di avvio, è necessario creare una nuova versione del modello di avvio.
- Numeri di versione: le versioni del modello di avvio sono numerate nell'ordine in cui sono state create. Quando crei una versione del modello di avvio, non è possibile specificare il numero di versione.

Autorizzazioni IAM per i modelli di avvio Amazon EC2

È possibile utilizzare le autorizzazioni IAM per controllare se gli utenti possono elencare, visualizzare, creare o eliminare modelli di avvio o versioni dei modelli di avvio.

> **Important**
>
> Non puoi utilizzare le autorizzazioni a livello di risorsa per limitare le risorse che gli utenti possono specificare in un modello di avvio quando creano un modello di avvio o una versione del modello di avvio. Pertanto, assicurati che solo gli amministratori fidati abbiano l'autorizzazione per creare modelli di avvio e versioni dei modelli di avvio.

Devi concedere a chiunque utilizzerà un modello di avvio le autorizzazioni richieste per creare e accedere alle risorse specificate nel modello di avvio. Ad esempio:

- Per avviare un'istanza da un'Amazon Machine Image (AMI) privata e condivisa, l'utente del modello di avvio deve disporre dell'autorizzazione di avvio per l'AMI.
- Per creare volumi EBS con tag da istantanee esistenti, l'utente del modello di avvio deve disporre dell'accesso in lettura alle istantanee e delle autorizzazioni per creare e contrassegnare i volumi.

Indice

- ec2: CreateLaunchTemplate
- ec2: DescribeLaunchTemplates
- ec2: DescribeLaunchTemplateVersions
- ec2: DeleteLaunchTemplate
- Controllo delle autorizzazioni di controllo delle versioni
- Controllo dell'accesso ai tag sui modelli di avvio

ec2: CreateLaunchTemplate

Per creare un modello di avvio nella console o utilizzando le API, il principale deve disporre dell'autorizzazione `ec2:CreateLaunchTemplate` in una policy IAM. Quando possibile, è consigliabile utilizzare i tag per controllare l'accesso ai modelli di avvio nell'account.

Ad esempio, la seguente istruzione di policy IAM fornisce al principale l'autorizzazione per creare modelli di avvio solo se il modello utilizza il tag specificato (*purpose*=*testing*).

```
{
    "Sid": "IAMPolicyForCreatingTaggedLaunchTemplates",
    "Action": "ec2:CreateLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

I principali che creano i modelli di avvio potrebbero richiedere alcune autorizzazioni correlate, come ad esempio:

- ec2: CreateTags — Per aggiungere tag al modello di avvio durante l'`CreateLaunchTemplate`operazione, il `CreateLaunchTemplate` chiamante deve disporre dell'`ec2:CreateTags`autorizzazione prevista da una policy IAM.
- ec2: RunInstances — Per avviare le istanze EC2 dal modello di lancio che hanno creato, il principale deve inoltre disporre dell'`ec2:RunInstances`autorizzazione prevista da una policy IAM.

Per le operazioni di creazione delle risorse in cui vengono applicati i tag, gli utenti devono disporre dell'autorizzazione `ec2:CreateTags`. La seguente istruzione di policy IAM utilizza la chiave di condizione `ec2:CreateAction` per consentire agli utenti di creare i tag soltanto nel contesto di `CreateLaunchTemplate`. Gli utenti non possono aggiungere tag ai modelli di avvio o altre risorse esistenti. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag Amazon EC2 per le risorse durante la creazione.

```
{
    "Sid": "IAMPolicyForTaggingLaunchTemplatesOnCreation",
    "Action": "ec2:CreateTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateLaunchTemplate"
        }
```

```
    }
}
```

L'utente IAM che crea un modello di avvio non dispone automaticamente dell'autorizzazione a utilizzare il modello di avvio che ha creato. Come qualsiasi altro principale, il creatore del modello di avvio deve ottenere l'autorizzazione tramite una policy IAM. Se un utente IAM desidera avviare un'istanza EC2 da un modello di avvio, deve disporre dell'autorizzazione `ec2:RunInstances`. Quando si concedono queste autorizzazioni, è possibile specificare che gli utenti possono utilizzare solo modelli di avvio con tag o ID specifici. Inoltre, è possibile controllare l'AMI e altre risorse alle quali chiunque utilizzi i modelli di avvio può fare riferimento e che può utilizzare per avviare le istanze specificando le autorizzazioni a livello di risorsa per la chiamata `RunInstances`. Per esempi di policy, consulta Modelli di avvio.

ec2: DescribeLaunchTemplates

Per elencare e visualizzare i modelli di avvio nell'account, il principale deve disporre dell'autorizzazione `ec2:DescribeLaunchTemplates` in una policy IAM. Dato che le operazioni `Describe` non supportano le autorizzazioni a livello di risorsa, devono essere specificate senza condizioni e il valore dell'elemento risorsa nella policy deve essere `"*"`.

Ad esempio, la seguente istruzione di policy IAM concede al principale l'autorizzazione per elencare e visualizzare tutti i modelli di avvio nell'account.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplates",
    "Action": "ec2:DescribeLaunchTemplates",
    "Effect": "Allow",
    "Resource": "*"
}
```

ec2: DescribeLaunchTemplateVersions

I responsabili che elencano e visualizzano i modelli di avvio dovrebbero inoltre disporre dell'autorizzazione `ec2:DescribeLaunchTemplateVersions` per recuperare l'intero set di attributi che compongono i modelli di avvio.

Per elencare e visualizzare le versioni del modello di avvio nell'account, il principale deve disporre dell'autorizzazione `ec2:DescribeLaunchTemplateVersions` in una policy IAM. Dato che le operazioni `Describe` non supportano le autorizzazioni a livello di risorsa, devono essere specificate senza condizioni e il valore dell'elemento risorsa nella policy deve essere `"*"`.

Ad esempio, la seguente istruzione di policy IAM concede al principale l'autorizzazione per elencare e visualizzare tutte le versioni del modello di avvio nell'account.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplateVersions",
    "Effect": "Allow",
    "Action": "ec2:DescribeLaunchTemplateVersions",
    "Resource": "*"
}
```

ec2: DeleteLaunchTemplate

> **Important**
>
> È necessario prestare attenzione quando si concedono ai principali le autorizzazioni per eliminare una risorsa. L'eliminazione di un modello di avvio potrebbe causare un errore in una AWS risorsa che si basa sul modello di avvio.

Per eliminare un modello di avvio, il principale deve disporre dell'autorizzazione `ec2:DeleteLaunchTemplate` in una policy IAM. Quando possibile, si consiglia di utilizzare le chiavi di condizione basate su tag per limitare le autorizzazioni.

Ad esempio, la seguente istruzione di policy IAM concede al principale l'autorizzazione per eliminare modelli di avvio solo se il modello dispone del tag specificato (*purpose*=*testing*).

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplates",
    "Action": "ec2:DeleteLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

In alternativa, è possibile utilizzare gli ARN per identificare il modello di avvio a cui si applica la policy IAM.

Un modello di avvio ha il seguente ARN.

```
"Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/lt-09477bcd97b0d310e"
```

È possibile specificare più ARN del modello di avvio fornendo un elenco oppure un valore `Resource` di `"*"` senza l'elemento `Condition` per consentire al principale di eliminare qualsiasi modello di avvio nell'account.

Controllo delle autorizzazioni di controllo delle versioni

Agli amministratori attendibili, è possibile concedere l'accesso per la creazione e l'eliminazione delle versioni di un modello di avvio e per modificare la versione predefinita di un modello di avvio utilizzando policy IAM simili agli esempi seguenti.

Important

Fai attenzione quando concedi ai principali il permesso di creare versioni dei modelli di avvio o modificare i modelli di avvio.

- Quando si crea una versione del modello di avvio, si influisce su qualsiasi risorsa AWS che consente ad Amazon EC2 di avviare istanze per proprio conto con la versione `Latest`.
- Quando modifichi un modello di avvio, puoi cambiare la versione `Default` e quindi influire su tutte AWS le risorse che consentono ad Amazon EC2 di avviare istanze per tuo conto con questa versione modificata.

È inoltre necessario prestare attenzione nel modo in cui gestisci AWS le risorse che interagiscono con la versione del modello `Latest` o `Default` lanci, come EC2 Fleet e Spot Fleet. Quando viene utilizzata una versione diversa del modello di avvio per `Latest` o `Default`, Amazon EC2 non ricontrolla le autorizzazioni per le operazioni da completare quando si avviano nuove istanze per soddisfare la capacità prevista del parco istanze, poiché non avviene alcuna interazione fra l'utente e la risorsa AWS . Concedendo a un utente l'autorizzazione a richiamare le API `CreateLaunchTemplateVersion` e `ModifyLaunchTemplate`, all'utente viene effettivamente concessa anche l'autorizzazione `iam:PassRole` se indirizza il parco istanze a una versione diversa del modello di avvio che contiene un profilo dell'istanza (un container per un ruolo IAM). Significa che un utente può potenzialmente aggiornare un modello di avvio per passare un ruolo IAM a un'istanza anche se non dispone dell'autorizzazione `iam:PassRole`. È possibile gestire questo rischio

prestando attenzione quando si concedono le autorizzazioni a chi può creare e gestire le versioni dei modelli di avvio.

ec2: CreateLaunchTemplateVersion

Per creare una nuova versione di un modello di avvio, il principale deve disporre dell'autorizzazione `ec2:CreateLaunchTemplateVersion` per il modello di avvio in una policy IAM.

Ad esempio, la seguente istruzione di policy IAM concede al principale l'autorizzazione per creare versioni dei modelli di avvio solo se la versione utilizza il tag specificato (*`environment`*=*`production`*). In alternativa, è possibile specificare uno o più ARN del modello di avvio oppure un valore `Resource` di `"*"` senza l'elemento `Condition` per consentire al principale di creare versioni di qualsiasi modello di avvio nell'account.

```
{
    "Sid": "IAMPolicyForCreatingLaunchTemplateVersions",
    "Action": "ec2:CreateLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2: DeleteLaunchTemplateVersion

Important

Come sempre, è necessario prestare attenzione quando si concedono le autorizzazioni per eliminare una risorsa. L'eliminazione di una versione del modello di avvio potrebbe causare un errore in una AWS risorsa che si basa sulla versione del modello di avvio.

Per eliminare una versione di un modello di avvio, il principale deve disporre dell'autorizzazione `ec2:DeleteLaunchTemplateVersion` per il modello di avvio in una policy IAM.

Ad esempio, la seguente istruzione di policy IAM concede al principale l'autorizzazione per eliminare versioni dei modelli di avvio solo se la versione utilizza il tag specificato (*environment*=*production*). In alternativa, è possibile specificare uno o più ARN del modello di avvio oppure un valore `Resource` di `"*"` senza l'elemento `Condition` per consentire al principale di eliminare versioni di qualsiasi modello di avvio nell'account.

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplateVersions",
    "Action": "ec2:DeleteLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2: ModifyLaunchTemplate

Per modificare la versione `Default` associata a un modello di avvio, il principale deve disporre dell'autorizzazione `ec2:ModifyLaunchTemplate` per il modello di avvio in una policy IAM.

Ad esempio, la seguente istruzione di policy IAM concede al principale l'autorizzazione per modificare i modelli di avvio solo se il modello di avvio utilizza il tag specificato (*environment*=*production*). In alternativa, è possibile specificare uno o più ARN del modello di avvio oppure un valore `Resource` di `"*"` senza l'elemento `Condition` per consentire al principale di modificare qualsiasi modello di avvio nell'account.

```
{
    "Sid": "IAMPolicyForModifyingLaunchTemplates",
    "Action": "ec2:ModifyLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

Controllo dell'accesso ai tag sui modelli di avvio

È possibile utilizzare le chiavi di condizione per limitare le autorizzazioni di applicazione di tag quando la risorsa è un modello di avvio. Ad esempio, la seguente policy IAM consente di rimuovere solo il tag con la chiave *temporary* dai modelli di avvio nell'account e nella regione specificati.

```
{
    "Sid": "IAMPolicyForDeletingTagsOnLaunchTemplates",
    "Action": "ec2:DeleteTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
    "Condition": {
        "ForAllValues:StringEquals": {
            "aws:TagKeys": ["temporary"]
        }
    }
}
```

Per ulteriori informazioni sulle chiavi di condizione utilizzabili per controllare le chiavi e i valori dei tag che possono essere applicati alle risorse Amazon EC2, consulta la pagina Controllo dell'accesso a tag specifici.

Usa i modelli di avvio di Amazon EC2 per controllare l'avvio delle istanze Amazon EC2

È possibile controllare la configurazione delle istanze Amazon EC2 specificando che gli utenti possono avviare istanze solo se utilizzando un modello di avvio, e che possono usare solo un modello di avvio specifico. Puoi anche controllare chi può creare, modificare, descrivere ed eliminare i modelli di avvio e le versioni del modello di avvio.

Utilizzo dei modelli di avvio per controllare i parametri di avvio

Un modello di avvio può contenere tutti o alcuni dei parametri per configurare un'istanza al momento dell'avvio. Tuttavia, quando avvii un'istanza utilizzando un modello di avvio, puoi sostituire i parametri specificati nel modello di avvio. Oppure puoi specificare parametri aggiuntivi che non si trovano nel modello di avvio.

> **Note**
>
> Non è possibile rimuovere i parametri del modello di avvio durante l'avvio (ad esempio, non è possibile specificare un valore nullo per il parametro). Per rimuovere un parametro, crea una nuova versione del modello di avvio senza il parametro e utilizza tale versione per avviare l'istanza.

Per avviare le istanze, gli utenti devono disporre dell'autorizzazione per utilizzare l'operazione `ec2:RunInstances`. Gli utenti devono anche disporre delle autorizzazioni per creare o utilizzare le risorse create o associate all'istanza. Puoi utilizzare le autorizzazioni a livello di risorsa per l'operazione `ec2:RunInstances` per controllare i parametri di avvio che gli utenti possono specificare. In alternativa, puoi concedere agli utenti le autorizzazioni per avviare un'istanza utilizzando un modello di avvio. Ciò consente di gestire i parametri di lancio in un modello di avvio anziché in una policy IAM e utilizzare un modello di avvio come veicolo di autorizzazione per l'avvio delle istanze. Ad esempio, è possibile specificare che gli utenti possono solo avviare istanze utilizzando un solo modello di avvio specifico. È anche possibile controllare i parametri di lancio che gli utenti possono sovrascrivere nel modello di avvio. Per esempi di policy, consulta Modelli di avvio.

Controllo dell'utilizzo dei modelli di avvio

Per impostazione predefinita, gli utenti non dispongono delle autorizzazioni per lavorare con i modelli di lancio. Puoi creare una policy dell'utente che concede agli utenti le autorizzazioni per creare, modificare, descrivere ed eliminare i modelli di avvio e le versioni del modello di avvio. È anche possibile applicare le autorizzazioni a livello di risorsa ad alcune operazioni del modello di avvio per controllare la capacità di un utente di utilizzare risorse specifiche per tali azioni. Per ulteriori informazioni, consulta le seguenti policy di esempio: Esempio: utilizzo dei modelli di avvio.

Fai attenzione quando concedi agli utenti le autorizzazioni per utilizzare le operazioni `ec2:CreateLaunchTemplate` e `ec2:CreateLaunchTemplateVersion`. Non è possibile utilizzare le autorizzazioni a livello di risorse per controllare le risorse che gli utenti possono specificare nel modello di avvio. Per limitare le risorse utilizzate per avviare un'istanza, assicurarsi di concedere le autorizzazioni per creare modelli di avvio e le versioni del modello di avvio solo agli amministratori appropriati.

Importanti problemi di sicurezza quando si utilizzano modelli di avvio con parchi istanze EC2 o serie di istanze spot

> **Note**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Per utilizzare i modelli di avvio, devi concedere agli utenti le autorizzazioni per creare, modificare, descrivere ed eliminare tali modelli e le relative versioni. Puoi controllare chi può creare modelli di avvio e versioni del modello di avvio controllando l'accesso alle operazioni `ec2:CreateLaunchTemplate` e `ec2:CreateLaunchTemplateVersion`. Puoi anche controllare chi può modificare i modelli di avvio controllando l'accesso all'operazione `ec2:ModifyLaunchTemplate`.

> **Important**
>
> Se un parco istanze EC2 o una serie di istanze spot è configurata per utilizzare la versione più recente o predefinita del modello di avvio, il parco istanze non sa se la versione Più recente o Predefinita viene successivamente modificata per puntare a una versione del modello di avvio diversa. Quando viene utilizzata una versione diversa del modello di avvio per Più recente o Predefinita, Amazon EC2 non ricontrolla le autorizzazioni per le operazioni da completare quando si avviano nuove istanze per soddisfare la capacità prevista del parco istanze. Questa è una considerazione importante quando si concedono le autorizzazioni a chi può creare e gestire le versioni dei modelli di avvio, in particolare l'operazione `ec2:ModifyLaunchTemplate` che consente a un utente di modificare la versione predefinita del modello di avvio.

Concedendo a un utente l'autorizzazione a utilizzare le operazioni EC2 per le API dei modelli di avvio, all'utente viene effettivamente concessa anche l'autorizzazione `iam:PassRole` se crea o aggiorna un parco istanze EC2 o una serie di istanze spot in modo che punti a una versione diversa del modello di avvio che contiene un profilo dell'istanza (un container per un ruolo IAM). Significa che un utente può potenzialmente aggiornare un modello di avvio per passare un ruolo IAM a un'istanza anche se non dispone dell'autorizzazione `iam:PassRole`. Per ulteriori informazioni e per una

policy IAM di esempio, consulta la sezione Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per ulteriori informazioni, consultare Controllo dell'utilizzo dei modelli di avvio e Esempio: utilizzo dei modelli di avvio.

Creare un modello di avvio Amazon EC2

Puoi creare un modello di avvio Amazon EC2 specificando i tuoi valori per i parametri di configurazione dell'istanza, oppure ottenendo i valori da un modello di avvio o da un'istanza Amazon EC2 esistente.

Non è necessario specificare un valore per ogni parametro nel modello di avvio; è sufficiente specificare un solo parametro di configurazione dell'istanza per creare un modello di avvio. Per indicare i parametri che scegli di non specificare, seleziona Non includere nel modello di avvio quando usi la console. Quando usi uno strumento a riga di comando, non includere i parametri per indicare che stai scegliendo di non specificarli nel modello di avvio.

Se desideri specificare un'AMI nel modello di avvio, puoi selezionare un'AMI o specificare un parametro Systems Manager che punterà a un'AMI all'avvio dell'istanza.

Quando un'istanza viene avviata con un modello di avvio, i valori specificati nel modello di avvio vengono utilizzati per configurare i parametri di istanza corrispondenti. Se non è specificato un valore nel modello di avvio, viene utilizzato il valore predefinito per il parametro di istanza corrispondente.

Processi

- Creare un modello di avvio specificando i parametri
- Creazione di un modello di avvio da un modello di avvio esistente
- Creazione di un modello di avvio da un'istanza
- Usare un parametro Systems Manager invece di un'ID AMI

Creare un modello di avvio specificando i parametri

Per creare un modello di avvio, è necessario specificare il nome del modello di avvio e almeno un parametro di configurazione dell'istanza.

Per una descrizione di ciascun parametro, consulta Riferimento per i parametri di configurazione delle EC2 istanze Amazon.

Console

Per creare un modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Modelli di avvio quindi Crea modello di avvio.
3. In Nome e descrizione del modello di avvio, procedi come indicato di seguito:

   a. In nome modello di avvio, inserire un nome descrittivo per il modello di avvio.

   b. In Template version description (Descrizione versione modello), fornire una breve descrizione della versione del modello di avvio.

   c. Per applicare un tag al modello di avvio al momento della creazione, espandi Tag del modello, scegli Aggiungi nuovo tag, poi inserisci una coppia chiave/valore di tag. Scegli Aggiungi tag per ogni tag aggiuntivo.

   > **Note**
   >
   > Per applicare un tag alle risorse create all'avvio di un'istanza, è necessario specificare i tag in Resource tags (Tag delle risorse). Per ulteriori informazioni, consulta la fase 9 in questa procedura.

4. In Immagini di applicazioni e sistema operativo (Amazon Machine Image), puoi mantenere selezionata la voce Non includere nel modello di avvio o scegliere il sistema operativo (SO) per l'istanza, quindi scegliere un'AMI. In alternativa, puoi specificare un parametro Systems Manager anziché specificare un'AMI. Per ulteriori informazioni, consulta Usare un parametro Systems Manager invece di un'ID AMI.

   Un'AMI è un modello che contiene il sistema operativo e il software necessari per avviare un'istanza.

5. Per Tipo di istanza, puoi tenere selezionata la voce Non includere nel modello di avvio, oppure seleziona un tipo di istanza, oppure specifica gli attributi di istanza e consenti ad Amazon EC2 di identificare i tipi di istanza con questi attributi.

   > **Note**
   >
   > La specifica degli attributi di istanza è supportata solo quando il modello di avvio viene utilizzato dai gruppi Auto Scaling, dal parco istanze EC2 e dal parco istanze spot per l'avvio delle istanze. Per ulteriori informazioni, consulta Create mixed

instances group using attribute-based instance type selection e Specifica gli attributi per la selezione del tipo di istanza per il parco del tipo per il parco istanze EC2 o il parco istanze Spot.
Se prevedi di utilizzare il modello di lancio nella procedura guidata di avvio dell'istanza o con l'RunInstances API, non puoi specificare gli attributi del tipo di istanza.

Il tipo di istanza determina la configurazione hardware (capacità in termini di CPU, memoria, storage e rete) e le dimensioni del computer host utilizzato per un'istanza.

Se hai dei dubbi sul tipo di istanza da scegliere, puoi effettuare le seguenti operazioni:

- Scegli Confronto dei tipi di istanza per confrontare diversi tipi di istanza con i seguenti attributi: numero di vCPUs, architettura, quantità di memoria (GiB), quantità di archiviazione (GB), tipo di archiviazione e prestazioni di rete.
- Scegli Fatti consigliare per ottenere indicazioni e suggerimenti per i tipi di istanza dal selettore dei tipi di istanza EC2. Per ulteriori informazioni, consulta Ottieni consigli dallo strumento di ricerca del tipo di istanza EC2.

Note

A seconda di quando hai creato l'account, potresti aver diritto a utilizzare Amazon EC2 nell'ambito del Piano gratuito.
Se l'hai creato Account AWS prima del 15 luglio 2025 e ha meno di 12 mesi, puoi utilizzare Amazon EC2 con il livello gratuito selezionando il tipo di istanza t2.micro o il tipo di istanza t3.micro nelle regioni in cui t2.micro non è disponibile. Tieni presente che quando avvii un'istanza t3.micro, l'impostazione predefinita è la modalità Illimitata, che potrebbe comportare costi aggiuntivi in base all'utilizzo della CPU. Se un tipo di istanza può essere utilizzato nell'ambito del Piano gratuito, è etichettato come Idoneo per il Piano gratuito.
Se hai creato la tua il Account AWS 15 luglio 2025 o dopo, puoi utilizzare i tipi di istanza t3.micro , t3.small, t4g.micro, t4g.small, c7i-flex.large e m7i-flex.large per 6 mesi o fino all'esaurimento dei crediti.
Per ulteriori informazioni, consulta Vantaggi del piano gratuito prima e dopo il 15 luglio 2025.

6. In Coppia di chiavi (login), per Nome della coppia di chiavi, mantieni selezionata la voce Non includere nel modello di avvio, oppure scegli una coppia di chiavi esistente, o creane una nuova.
7. In Impostazioni di rete, puoi mantenere selezionata la voce Non includere nel modello di avvio, oppure puoi specificare i valori per le varie impostazioni di rete.
8. In Configura archiviazione, se hai specificato un'AMI nel modello di avvio, l'AMI include uno o più volumi di archiviazione, compreso il volume root (Volume 1 [AMI Root]). Facoltativamente, è possibile specificare altri volumi da collegare all'istanza. Per aggiungere un nuovo volume, scegli Add new volume (Aggiungi nuovo volume).
9. In Tag delle risorse, per applicare un tag alle risorse create all'avvio di un'istanza, scegli Aggiungi tag, quindi inserisci una coppia chiave/valore di tag. Per Resource types (Tipi di risorsa), specifica le risorse alle quali applicare un tag al momento della creazione. È possibile specificare lo stesso tag per tutte le risorse o specificare tag diversi per risorse diverse. Scegliere Add tag (Aggiungi tag) per ogni tag aggiuntivo.

   È possibile specificare i tag per le seguenti risorse che vengono create quando si utilizza un modello di avvio:

   - Istanze
   - Volumi
   - Grafica elastica
   - Richieste di istanza spot
   - Interfacce di rete

   > **Note**
   >
   > Per applicare un tag al modello di avvio stesso, è necessario specificare i tag in Template tags (Tag del modello). Per ulteriori informazioni, consulta la fase 3 in questa procedura.

10. Per Dettagli avanzati, espandi la sezione per visualizzare i campi e specifica facoltativamente gli eventuali parametri aggiuntivi per l'istanza.
11. Utilizza il pannello Riepilogo per esaminare la configurazione del modello di avvio. Puoi accedere a qualsiasi sezione selezionando il relativo link e quindi apportare le modifiche necessarie.

12. Quando è tutto pronto per creare il modello di avvio, scegliere Create launch template (Crea modello di avvio).

AWS CLI

Per creare un modello di avvio

Utilizzare il comando create-launch-template.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --version-description WebVersion1 \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Di seguito è riportato un JSON di esempio che specifica i dati del modello di avvio per la configurazione dell'istanza. Salva il JSON in un file e includilo nel parametro `--launch-template-data` come mostrato nel comando di esempio.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-0abcdef1234567890"
    }],
    "ImageId": "ami-0abcdef1234567890",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":2
    }
}
```

Di seguito è riportato un output di esempio.

```
{
    "LaunchTemplate": {
        "LatestVersionNumber": 1,
        "LaunchTemplateId": "lt-01238c059e3466abc",
        "LaunchTemplateName": "TemplateForWebServer",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:root",
        "CreateTime": "2017-11-27T09:13:24.000Z"
    }
}
```

PowerShell

Per creare un modello di avvio

Utilizza il cmdlet New-EC2LaunchTemplate.

```
$launchTemplateData = [Amazon.EC2.Model.RequestLaunchTemplateData]@{
    ImageId = 'ami-0abcdef1234567890'
    InstanceType = 'r5.4xlarge'
    NetworkInterfaces = @(

 [Amazon.EC2.Model.LaunchTemplateInstanceNetworkInterfaceSpecificationRequest]@{
            AssociatePublicIpAddress = $true
            DeviceIndex = 0
            Ipv6AddressCount = 1
            SubnetId = 'subnet-0abcdef1234567890'
        }
    )
    TagSpecifications = @(
        [Amazon.EC2.Model.LaunchTemplateTagSpecificationRequest]@{
            ResourceType = 'instance'
            Tags = [Amazon.EC2.Model.Tag]@{
                Key = 'Name'
                Value = 'webserver'
            }
        }
    )
    CpuOptions = [Amazon.EC2.Model.LaunchTemplateCpuOptionsRequest]@{
        CoreCount = 4
        ThreadsPerCore = 2
```

```
    }
}
$tagSpecificationData = [Amazon.EC2.Model.TagSpecification]@{
    ResourceType = 'launch-template'
    Tags = [Amazon.EC2.Model.Tag]@{
        Key = 'purpose'
        Value = 'production'
    }
}
New-EC2LaunchTemplate -LaunchTemplateName 'TemplateForWebServer' `
    -VersionDescription 'WebVersion1' `
    -LaunchTemplateData $launchTemplateData `
    -TagSpecification $tagSpecificationData
```

Di seguito è riportato un output di esempio.

```
CreatedBy            : arn:aws:iam::123456789012:root
CreateTime           : 9/19/2023 16:57:55
DefaultVersionNumber : 1
LatestVersionNumber  : 1
LaunchTemplateId     : lt-01238c059eEXAMPLE
LaunchTemplateName   : TemplateForWebServer
Tags                 : {purpose}
```

Creazione di un modello di avvio da un modello di avvio esistente

È possibile clonare un modello di avvio esistente e quindi modificare i parametri per crearne uno nuovo. Tuttavia, è possibile farlo solo utilizzando la console Amazon EC2. AWS CLI Non supporta la clonazione di un modello. Per una descrizione di ciascun parametro, consulta Riferimento per i parametri di configurazione delle EC2 istanze Amazon.

Console

Creazione di un modello di avvio da un modello di avvio esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Modelli di avvio quindi Crea modello di avvio.
3. In nome modello di avvio, inserire un nome descrittivo per il modello di avvio.
4. In Template version description (Descrizione versione modello), fornire una breve descrizione della versione del modello di avvio.

5. Per applicare un tag al modello di avvio al momento della creazione, espandi Tag del modello, scegli Aggiungi nuovo tag, poi inserisci una coppia chiave/valore di tag.
6. Espandere Modello origine e per Nome modello di avvio scegliere un modello di avvio su cui basare il nuovo modello di avvio.
7. Per Source template version (Versione modello origine), scegli la versione del modello di avvio su cui basare il nuovo modello di avvio.
8. Regola i parametri di lancio come necessario e scegli Create launch template (Crea modello di avvio).

Creazione di un modello di avvio da un'istanza

È possibile clonare i parametri di un'istanza Amazon EC2 e quindi modificare i parametri per creare un modello di avvio. Per una descrizione di ciascun parametro, consulta Riferimento per i parametri di configurazione delle EC2 istanze Amazon.

Console

Creazione di un modello di avvio da un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e scegli Operazioni, Immagini e modelli, Crea modello dall'istanza.
4. Specificare un nome, una descrizione e i tag e modificare i parametri di lancio come necessario.

> **Note**
>
> Quando si crea un modello di avvio da un'istanza, gli ID dell'interfaccia di rete e gli indirizzi IP dell'istanza non sono inclusi nel modello.

5. Scegli Create launch template (Crea modello di avvio).

AWS CLI

È possibile utilizzare il AWS CLI per creare un modello di avvio da un'istanza esistente recuperando prima i dati del modello di avvio da un'istanza e quindi creando un modello di avvio utilizzando i dati del modello di avvio.

Recupero dei dati del modello di avvio da un'istanza

- Utilizzare il comando get-launch-template-data e specificare l'ID dell'istanza. È possibile utilizzare l'output come base per creare un nuovo modello di avvio o una nuova versione del modello di avvio. Per impostazione predefinita, l'output include un oggetto `LaunchTemplateData` di primo livello, che non può essere specificato nei dati del modello di avvio. Utilizzare l'opzione `--query` per escludere questo oggetto.

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData"
```

Di seguito è riportato un output di esempio.

```
    {
        "Monitoring": {},
        "ImageId": "ami-8c1be5f6",
        "BlockDeviceMappings": [
            {
                "DeviceName": "/dev/xvda",
                "Ebs": {
                    "DeleteOnTermination": true
                }
            }
        ],
        "EbsOptimized": false,
        "Placement": {
            "Tenancy": "default",
            "GroupName": "",
            "AvailabilityZone": "us-east-1a"
        },
        "InstanceType": "t2.micro",
        "NetworkInterfaces": [
            {
                "Description": "",
                "NetworkInterfaceId": "eni-35306abc",
                "PrivateIpAddresses": [
                    {
                        "Primary": true,
                        "PrivateIpAddress": "10.0.0.72"
                    }
                ],
```

```
                "SubnetId": "subnet-7b16de0c",
                "Groups": [
                    "sg-7c227019"
                ],
                "Ipv6Addresses": [
                    {
                        "Ipv6Address": "2001:db8:1234:1a00::123"
                    }
                ],
                "PrivateIpAddress": "10.0.0.72"
            }
        ]
    }
```

È possibile scrivere l'output direttamente su un file, ad esempio:

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData" >> instance-data.json
```

Creazione di un modello di avvio utilizzando i dati del modello di avvio

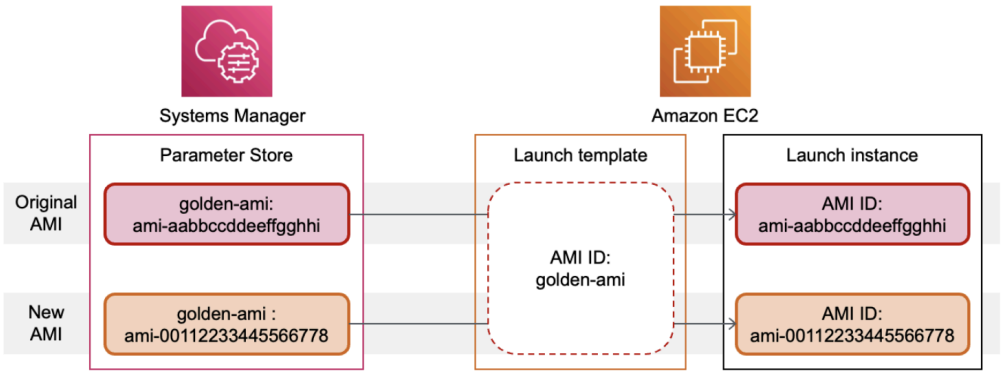
- Utilizzare il comando create-launch-template per creare un modello di avvio utilizzando l'output della procedura precedente. Per ulteriori informazioni sulla creazione di un modello di lancio utilizzando il AWS CLI, vedereCreare un modello di avvio specificando i parametri.

Usare un parametro Systems Manager invece di un'ID AMI

Anziché specificare un ID AMI nei modelli di avvio, puoi specificare un parametro AWS Systems Manager . Se l'ID AMI cambia, è possibile aggiornare l'ID AMI in un'unica posizione aggiornando il parametro Systems Manager nel Parameter Store di Systems Manager. I parametri possono anche essere condivisi con altri Account AWS. È possibile archiviare e gestire centralmente i parametri dell'AMI in un account e condividerli con ogni altro account a cui deve farvi riferimento. Utilizzando un parametro Systems Manager, tutti i modelli di avvio possono essere aggiornati con un'unica operazione.

Un parametro Systems Manager è una coppia chiave-valore definita dall'utente creata nel AWS Systems Manager Parameter. Parameter Store fornisce un luogo centralizzato per archiviare i valori di configurazione dell'applicazione.

Nel diagramma seguente, il parametro `golden-ami` viene prima mappato all'AMI originale `ami-aabbccddeeffgghhi` nel Parameter Store. Nel modello di avvio, il valore dell'ID AMI è `golden-ami`. Quando un'istanza viene avviata utilizzando questo modello di avvio, l'ID AMI si risolve nell'`ami-aabbccddeeffgghhi`. Successivamente, l'AMI viene aggiornata con il risultato di un nuovo ID AMI. Nel Parameter Store, il parametro `golden-ami` è mappato alla nuova `ami-00112233445566778`. Il modello di avvio rimane invariato. Quando un'istanza viene avviata utilizzando questo modello di avvio, l'ID AMI si risolve nella nuova `ami-00112233445566778`.



Formato dei parametri Systems Manager per gli ID AMI

I modelli di avvio richiedono che i parametri Systems Manager definiti dall'utente rispettino il seguente formato quando vengono utilizzati al posto di un ID AMI:

- Tipo parametro: `String`
- Tipo di dati del parametro: `aws:ec2:image`. Garantisce che Parameter Store convalidi che il valore immesso sia nel formato corretto per un ID AMI.

Per ulteriori informazioni sulla creazione di un parametro valido per un ID AMI, consulta Creazione dei parametri Systems Manager nella Guida per l'utente AWS Systems Manager .

Formato dei parametri Systems Manager nei modelli di avvio

Per utilizzare un parametro Systems Manager al posto di un ID AMI in un modello di avvio, è necessario utilizzare uno dei seguenti formati quando si specifica il parametro nel modello di avvio:

Per fare riferimento a un parametro pubblico:

- `resolve:ssm:`*`public-parameter`*

Per fare riferimento a un parametro memorizzato nello stesso account:

- `resolve:ssm:parameter-name`
- `resolve:ssm:parameter-name:version-number`: il numero di versione stesso è un'etichetta predefinita
- `resolve:ssm:parameter-name:label`

Per fare riferimento a un parametro condiviso da un altro Account AWS:

- `resolve:ssm:parameter-ARN`
- `resolve:ssm:parameter-ARN:version-number`
- `resolve:ssm:parameter-ARN:label`

Versioni dei parametri

I parametri Systems Manager sono risorse con versione. Quando si aggiorna un parametro, si creano nuove versioni successive del parametro. Systems Manager supporta etichette dei parametri che è possibile mappare a versioni specifiche di un parametro.

Ad esempio, il parametro `golden-ami` può avere tre versioni: `1`, `2` e `3`. È possibile creare un'etichetta del parametro `beta` che corrisponde alla versione `2` e un'etichetta del parametro `prod` che corrisponde alla versione `3`.

In un modello di avvio, è possibile specificare la versione 3 del parametro `golden-ami` utilizzando uno dei seguenti formati:

- `resolve:ssm:golden-ami:3`
- `resolve:ssm:golden-ami:prod`

Specificare la versione o l'etichetta è facoltativo. Quando non è specificata alcuna versione viene utilizzata la versione più recente del parametro.

Specificare un parametro Systems Manager in un modello di avvio

È possibile specificare un parametro Systems Manager in un modello di avvio anziché un ID AMI quando si crea un modello di avvio o una nuova versione di un modello di avvio.

Console

Per specificare un parametro Systems Manager in un modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Modelli di avvio quindi Crea modello di avvio.
3. In nome modello di avvio, inserire un nome descrittivo per il modello di avvio.
4. In Applicazioni e immagini SO (Amazon Machine Image), scegli Sfoglia altre AMI.
5. Scegli il pulsante freccia a destra della barra di ricerca, quindi scegli Specifica il parametro personalizzato di value/Systems Manager.
6. Nella finestra di dialogo Specifica valore personalizzato o parametro Systems Manager, segui questi passaggi:

   a. Per la stringa ID AMI o parametro Manager Systems, inserisci il nome del parametro Systems Manager utilizzando uno dei seguenti formati:

      Per fare riferimento a un parametro pubblico:

      - **resolve:ssm:*public-parameter***

      Per fare riferimento a un parametro memorizzato nello stesso account:

      - **resolve:ssm:*parameter-name***
      - **resolve:ssm:*parameter-name*:*version-number***
      - **resolve:ssm:*parameter-name*:*label***

      Per fare riferimento a un parametro condiviso da un altro Account AWS:

      - **resolve:ssm:*parameter-ARN***
      - **resolve:ssm:*parameter-ARN*:*version-number***
      - **resolve:ssm:*parameter-ARN*:*label***

   b. Scegli Save (Salva).
7. Specifica qualsiasi altro parametro del modello di avvio, se necessario, quindi scegli Crea modello di avvio.

Per ulteriori informazioni, consulta Creare un modello di avvio specificando i parametri.

AWS CLI

Per specificare un parametro Systems Manager in un modello di avvio

- Utilizza il comando create-launch-template per creare il modello di avvio. Per specificare l'AMI da utilizzare, inserisci il nome del parametro Systems Manager utilizzando uno dei seguenti formati:

  Per fare riferimento a un parametro pubblico:

  - **resolve:ssm:*public-parameter***

  Per fare riferimento a un parametro memorizzato nello stesso account:

  - **resolve:ssm:*parameter-name***
  - **resolve:ssm:*parameter-name*:*version-number***
  - **resolve:ssm:*parameter-name*:*label***

  Per fare riferimento a un parametro condiviso da un altro Account AWS:

  - **resolve:ssm:*parameter-ARN***
  - **resolve:ssm:*parameter-ARN*:*version-number***
  - **resolve:ssm:*parameter-ARN*:*label***

  L'esempio seguente crea un modello di avvio che specifica quanto segue:

  - Un nome per il modello di avvio (*TemplateForWebServer*)
  - Un tag per il modello di avvio (*purpose*=*production*)
  - I dati per la configurazione dell'istanza, specificati in un file JSON:
    - L'AMI da usare (`resolve:ssm:`*golden-ami*)
    - Il tipo di istanza da avviare (*m5.4xlarge*)
    - Un tag per l'istanza (*Name*=*webserver*)

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
```

```
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Di seguito è riportato un file JSON di esempio che contiene i dati del modello di avvio per la configurazione dell'istanza. Il valore di `ImageId` è il nome del parametro Systems Manager, inserito nel formato`resolve:ssm:golden-ami` richiesto.

```
{"LaunchTemplateData": {
    "ImageId": "resolve:ssm:golden-ami",
    "InstanceType": "m5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }]
  }
}
```

Verifica che un modello di avvio riceva l'ID AMI corretto

Per risolvere il parametro Systems Manager nell'ID AMI effettivo

Utilizza il comando describe-launch-template-versions e includi il parametro `--resolve-alias`.

```
aws ec2 describe-launch-template-versions \
    --launch-template-name my-launch-template \
    --versions $Default \
    --resolve-alias
```

La risposta include l'ID AMI per `ImageId`. In questo esempio, quando un'istanza viene avviata utilizzando questo modello di avvio, l'ID AMI si risolve in `ami-0ac394d6a3example`.

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-089c023a30example",
            "LaunchTemplateName": "my-launch-template",
```

```
            "VersionNumber": 1,
            "CreateTime": "2022-12-28T19:52:27.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0ac394d6a3example",
                "InstanceType": "t3.micro",
            }
        }
    ]
}
```

Risorse correlate

Per ulteriori informazioni sull'utilizzo dei parametri Systems Manager, consulta i seguenti materiali di riferimento nella documentazione di Systems Manager.

- Per informazioni su come cercare i parametri pubblici dell'AMI supportati da Amazon EC2, consulta Chiamata dei parametri pubblici dell'AMI.
- Per informazioni sulla condivisione dei parametri con altri AWS account o tramite AWS Organizations, vedi Utilizzo dei parametri condivisi.
- Per informazioni su come verificare se i parametri vengono creati correttamente, consulta Supporto dei parametri nativi per gli ID di Amazon Machine Image.

Limitazioni

- Solo i parchi istanze EC2 di tipo `instant` supportano l'utilizzo di un modello di avvio per cui è specificato un parametro System Manager anziché un ID AMI.
- I parchi istanze EC2 di tipo `maintain` e `request`, e i parchi istanze spot non supportano l'utilizzo di un modello di avvio per cui è specificato un parametro System Manager anziché un ID AMI. Per i parchi istanze EC2 di tipo `maintain` e `request`, e i parchi istanze spot, se nel modello di avvio specifichi un'AMI, devi specificare l'ID dell'AMI.
- Se utilizzi la selezione di istanze basata sugli attributi nel tuo parco istanze EC2, non puoi specificare un parametro Systems Manager al posto di un ID dell'AMI. Quando si utilizza la selezione di istanze basata sugli attributi, devi specificare l'ID dell'AMI.
- Amazon EC2 Auto Scaling fornisce altre restrizioni. Per ulteriori informazioni, consulta Utilizzare AWS Systems Manager i parametri anziché gli ID AMI nei modelli di avvio nella Amazon EC2 Auto Scaling User Guide.

Modificare un modello di avvio (gestire le versioni dei modelli di avvio)

I modelli di avvio sono immutabili; dopo aver creato un modello di avvio, non puoi più modificarlo. È invece possibile creare una nuova versione del modello di avvio che includa tutte le modifiche necessarie.

Per un modello di avvio puoi creare due diverse versioni, impostare la versione di default, descrivere una versione del modello di avvio ed eliminare le versioni non più necessarie.

Processi

- Creazione di una versione del modello di avvio
- Impostazione della versione del modello di avvio predefinita
- Descrizione di una versione del modello di avvio

Creazione di una versione del modello di avvio

Quando crei una versione del modello di avvio, è possibile specificare nuovi parametri di lancio o utilizzare una versione esistente come base per la nuova versione. Per una descrizione di ciascun parametro, consulta Riferimento per i parametri di configurazione delle EC2 istanze Amazon.

Console

Come creare una versione del modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Launch Templates (modelli di avvio) nel riquadro di navigazione.
3. Scegli un modello di avvio, quindi scegli Azioni, Modifica modello (Crea nuova versione).
4. Alla voce Template version description (Descrizione della versione del modello), inserire una descrizione per la versione del modello di avvio.
5. (Facoltativo) Espandere Source template (Modello origine) e selezionare una versione del modello di avvio da utilizzare come base per la nuova versione del modello di avvio. La nuova versione del modello di avvio eredita i parametri di avvio da questa versione del modello di avvio.
6. Modificare i parametri di lancio come richiesto.
7. Scegli Crea modello di avvio.

AWS CLI

Come creare una versione del modello di avvio

Utilizzare il comando create-launch-template-version. È possibile specificare una versione di origine su cui basare la nuova versione. La nuova versione eredita gli stessi parametri di avvio da questa versione ed è possibile sovrascrivere i parametri utilizzando `--launch-template-data`. L'esempio seguente crea una nuova versione basata sulla versione 1 del modello di avvio e specifica un ID AMI diverso.

```
aws ec2 create-launch-template-version \
    --launch-template-id lt-0abcd290751193123 \
    --version-description WebVersion2 \
    --source-version 1 \
    --launch-template-data "ImageId=ami-0abcdef1234567890"
```

PowerShell

Come creare una versione del modello di avvio

Usa il New-EC2LaunchTemplateVersion cmdlet. È possibile specificare una versione di origine su cui basare la nuova versione. La nuova versione eredita gli stessi parametri di avvio da questa versione ed è possibile sovrascrivere i parametri utilizzando `LaunchTemplateData`. L'esempio seguente crea una nuova versione basata sulla versione 1 del modello di avvio e specifica un ID AMI diverso.

```
New-EC2LaunchTemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -VersionDescription WebVersion2 `
    -SourceVersion 1 `
    -LaunchTemplateData (
        New-Object `
            -TypeName Amazon.EC2.Model.RequestLaunchTemplateData `
            -Property @{ImageId = 'ami-0abcdef1234567890'}
    )
```

Impostazione della versione del modello di avvio predefinita

È possibile impostare la versione predefinita per il modello di avvio. Quando avvii un'istanza da un modello di avvio e non specifichi una versione, l'istanza viene avviata utilizzando i parametri della versione predefinita.

Console

Impostazione della versione del modello di avvio predefinita

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Launch Templates (modelli di avvio) nel riquadro di navigazione.
3. Scegli il modello di avvio e scegli Azioni, Imposta versione predefinita.
4. Per Template version (Versione modello), selezionare il numero di versione da impostare come versione predefinita e scegliere Set as default version (Imposta come versione predefinita).

AWS CLI

Impostazione della versione del modello di avvio predefinita

Utilizza il comando modify-launch-template.

```
aws ec2 modify-launch-template \
    --launch-template-id lt-0abcd290751193123 \
    --default-version 2
```

PowerShell

Impostazione della versione del modello di avvio predefinita

Utilizza il cmdlet Edit-EC2LaunchTemplate.

```
Edit-EC2LaunchTemplate `
    -LaunchTemplateId lt-0abcd290751193123 `
    -DefaultVersion 2
```

Descrizione di una versione del modello di avvio

Utilizzando la console, è possibile visualizzare tutte le versioni del modello di avvio selezionato o ottenere un elenco dei modelli di avvio la cui versione più recente o predefinita corrisponde a un numero di versione specifico. Usando il AWS CLI, puoi descrivere tutte le versioni, le singole versioni o un intervallo di versioni di un modello di avvio specificato. Puoi anche descrivere tutte le versioni più recenti o tutte le versioni predefinite di tutti i modelli di lancio nel tuo account.

Console

Descrizione di una versione del modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Launch Templates (modelli di avvio) nel riquadro di navigazione.
3. Puoi visualizzare una versione di un modello di avvio specifico o ottenere un elenco dei modelli di avvio la cui versione più recente o predefinita corrisponde a un numero di versione specifico.
   - Per visualizzare una versione di un modello di lancio: scegli il modello di avvio. Nella scheda Versioni, da Versione, scegli una versione per visualizzarne i dettagli.
   - Per ottenere un elenco di tutti i modelli di avvio la cui versione più recente corrisponde a un numero di versione specifico: dalla barra di ricerca scegliere Versione più recente, quindi scegliere un numero di versione.
   - Per ottenere un elenco di tutti i modelli di avvio la cui versione predefinita corrisponde a un numero di versione specifico: dalla barra di ricerca scegliere Versione predefinita, quindi scegliere un numero di versione.

AWS CLI

Descrizione di una versione del modello di avvio

Utilizzare il comando describe-launch-template-versions e specificare i numeri di versione. Nell'esempio seguente vengono specificate le versioni *1* e *3*.

```
aws ec2 describe-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1 3
```

Per descrivere tutte le versioni più recenti e predefinite del modello di avvio nell'account

Utilizza il comando describe-launch-template-versions e specifica `$Latest`, `$Default` o entrambi. Nella chiamata ometti il nome e l'ID del modello di avvio. Non puoi specificare i numeri di versione.

```
aws ec2 describe-launch-template-versions \
    --versions "$Latest,$Default"
```

PowerShell

Descrizione di una versione del modello di avvio

Usa il Get-EC2TemplateVersion cmdlet e specifica i numeri di versione. Nell'esempio seguente vengono specificate le versioni *1* e *3*.

```
Get-EC2TemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -Version 1,3
```

Per descrivere tutte le versioni più recenti e predefinite del modello di avvio nell'account

Utilizzare il Get-EC2TemplateVersion cmdlet e specificare`$Latest`, `$Default` o entrambi. Nella chiamata ometti il nome e l'ID del modello di avvio. Non puoi specificare i numeri di versione.

```
Get-EC2TemplateVersion `
    -Version '$Latest','$Default'
```

Eliminazione di un modello di avvio o di una versione del modello di avvio

Se non è più necessario un modello di avvio, è possibile eliminarlo. L'eliminazione di un modello di avvio ne elimina tutte le versioni. Se desideri eliminare solo una versione specifica di un modello di avvio, puoi farlo mantenendo le altre versioni del modello di avvio.

L'eliminazione di un modello di avvio o di una versione del modello di avvio non influisce sulle istanze avviate da tale modello.

Elimina un modello di avvio e tutte le sue versioni

Se non è più necessario un modello di avvio, comprese tutte le sue versioni, puoi eliminare il modello di avvio. L'eliminazione di un modello di avvio ne elimina tutte le versioni.

Console

Per eliminare un modello di avvio e tutte le sue versioni

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Launch Templates (modelli di avvio) nel riquadro di navigazione.
3. Scegli il modello di avvio e scegli Azioni, Elimina modello.
4. Immettere **Delete** per confermare l'eliminazione, quindi scegliere Delete (Elimina).

AWS CLI

Per eliminare un modello di avvio e tutte le sue versioni

Utilizza il comando delete-launch-template e specifica il modello di avvio.

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

PowerShell

Per eliminare un modello di avvio e tutte le sue versioni

Utilizzate il comando Remove-EC2LaunchTemplate (AWS Strumenti per PowerShell) e specificate il modello di avvio. Se `-Force` viene omesso, PowerShell richiede una conferma.

```
Remove-EC2LaunchTemplate -LaunchTemplateId lt-0123456789example -Force
```

Eliminazione di una versione del modello di avvio

Se non è più necessaria una versione del modello di avvio, è possibile eliminarla.

Considerazioni

- Non è possibile sostituire il numero di versione dopo averlo eliminato.

- Non è possibile eliminare la versione predefinita del modello di avvio; è necessario prima assegnare una versione diversa come predefinita. Se la versione predefinita è l'unica versione del modello di avvio, devi eliminare l'intero modello di avvio.
- Utilizzando la console, puoi eliminare una versione del modello alla volta. Quando si utilizza il AWS CLI, è possibile eliminare fino a 200 versioni del modello di avvio in una singola richiesta. Per eliminare più di 200 versioni con una sola richiesta, puoi eliminare il modello di avvio, che elimina anche tutte le sue versioni.

Console

Come eliminare una versione del modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Launch Templates (modelli di avvio) nel riquadro di navigazione.
3. Scegli il modello di avvio e scegli Azioni, Elimina versione modello.
4. Scegli la versione da eliminare e scegli Elimina.

AWS CLI

Come eliminare una versione del modello di avvio

Utilizzare il comando delete-launch-template-versions e specificare i numeri di versione da eliminare. Puoi specificare fino a 200 versioni del modello di avvio da eliminare in una singola richiesta.

```
aws ec2 delete-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1
```

PowerShell

Come eliminare una versione del modello di avvio

Utilizza il Remove-EC2TemplateVersion cmdlet e specifica i numeri di versione da eliminare. Puoi specificare fino a 200 versioni del modello di avvio da eliminare in una singola richiesta.

```
Remove-EC2TemplateVersion `
```

```
    -LaunchTemplateId lt-0abcd290751193123 `
    -Version 1
```

Avviare un'istanza Amazon EC2

Un'istanza è un server virtuale nel AWS cloud. Puoi avviare un'istanza da un'Amazon Machine Image (AMI). L'AMI fornisce il sistema operativo, il server applicazioni e le applicazioni per l'istanza.

Quando crei il tuo Account AWS, puoi iniziare a usare Amazon EC2 gratuitamente utilizzando. Piano gratuito di AWS I vantaggi del Piano gratuito dipendono da quando hai creato il tuo Account AWS. Se hai creato il tuo Account AWS prima del 15 luglio 2025, quindi da meno di 12 mesi, puoi utilizzare il Piano gratuito per avviare e utilizzare un'istanza `t2.micro` gratuitamente (nelle Regioni in cui `t2.micro` non è disponibile, puoi usare un'istanza `t3.micro` nell'ambito del Piano gratuito). Viene addebitato un costo per l'istanza o l'utilizzo che rientra nei limiti del piano gratuito mentre l'istanza viene eseguita, anche se rimane inattiva. Per ulteriori informazioni, consulta Prezzi di Amazon EC2. Se hai creato il tuo Account AWS a partire dal 15 luglio 2025, puoi utilizzare i tipi di istanza `t3.micro`, `t3.small`, `t4g.micro`, `t4g.small`, `c7i-flex.large` e `m7i-flex.large` per 6 mesi o fino all'esaurimento dei crediti. Per ulteriori informazioni, consulta Vantaggi del piano gratuito prima e dopo il 15 luglio 2025.

Quando si avvia l'istanza, è possibile avviarla in una sottorete associata a una delle seguenti risorse:

- Una zona di disponibilità: è l'opzione predefinita.
- Local Zone - Per avviare un'istanza in una Local Zone è necessario accettare esplicitamene la Local Zone e quindi creare una sottorete nella zona. Per ulteriori informazioni, consulta Nozioni di base sulle zone locali.
- Zona Wavelength: per avviare un'istanza in una zona Wavelength è necessario accettare esplicitamente la zona Wavelength e quindi creare una sottorete nella zona. Per informazioni su come avviare un'istanza in una zona Wavelength, consulta Nozioni di base su AWS Wavelength.
- Un Outpost: per avviare un'istanza in un Outpost, è necessario crearlo. Per informazioni su come creare un avamposto, vedi Guida introduttiva AWS Outposts.

Dopo aver avviato l'istanza, puoi stabilire una connessione e utilizzarla. All'inizio lo stato dell'istanza è `pending`. Quando lo stato dell'istanza è `running`, significa che è iniziato l'avvio dell'istanza. Potrebbe passare qualche minuto prima di riuscire a connetterti all'istanza. Si noti che i tipi di istanza bare metal potrebbero richiedere più tempo per l'avvio.

A seconda di come intendi connetterti all'istanza, potresti voler applicare determinate configurazioni al momento dell'avvio dell'istanza. Queste configurazioni potrebbero includere la specificazione di regole del gruppo di sicurezza in entrata per un determinato traffico o l'associazione di un ruolo del profilo dell'istanza. Per ulteriori informazioni sui metodi di connessione che puoi utilizzare per la connessione e i relativi requisiti, consulta Connettiti all'istanza EC2.

L'istanza riceve un nome DNS pubblico che potrai utilizzare per contattare l'istanza da Internet. L'istanza riceve inoltre un nome DNS privato che le altre istanze all'interno dello stesso VPC potranno utilizzare per contattare l'istanza.

Quando un'istanza non è più necessaria, assicurati di interromperla per evitare di incorrere in costi inutili. Per ulteriori informazioni, consulta Terminare le istanze Amazon EC2.

Se devi avviare un numero elevato di istanze, utilizzare più tipi di istanze o utilizzare più opzioni di acquisto come Instance, Reserved Instance e Spot On-Demand Instance, prendi in considerazione l'utilizzo di EC2 Fleet. Per ulteriori informazioni, consulta EC2 Fleet e parco istanze spot.

Se desideri automatizzare il ciclo di vita delle tue istanze, incluso il ridimensionamento automatico, i controlli di integrità e la sostituzione delle istanze non integre, prendi in considerazione l'utilizzo di Amazon EC2 Auto Scaling. https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html

I metodi seguenti sono alcuni dei modi in cui è possibile avviare un'istanza.

Metodo	Strumento	Documentazione
Utilizzare la procedura guidata di avvio dell'istanza per specificare i parametri di avvio.	Console Amazon EC2	Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console
Creare un modello di avvio e avviare l'istanza dal modello di avvio.	Console Amazon EC2	Avvio di istanze EC2 usando un modello di avvio
Utilizzare un'istanza esistente come base.	Console Amazon EC2	Avvia un'istanza EC2 usando i dettagli da un'istanza esistente
Utilizzare un'AMI acquistata da Marketplace AWS.	Console Amazon EC2	Avvia un'istanza Amazon EC2 da un'AMI Marketplace AWS

Metodo	Strumento	Documentazione
Utilizzare un'AMI da te specificata.	AWS CLI	Avvio, elenco ed eliminazione delle istanze Amazon EC2 nel AWS CLI
Utilizzare un'AMI da te specificata.	AWS Tools for Windows PowerShell	Avvia un'istanza Amazon EC2 utilizzando Windows PowerShell
Usa EC2 Fleet per fornire capacità tra diversi tipi di istanze EC2 e zone di disponibilità e tra opzioni di acquisto di On-Demand istanze, istanze riservate e istanze Spot.	AWS CLI	EC2 Fleet e parco istanze spot
Utilizza un CloudFormation modello per specificare un'istanza.	AWS CloudFormation	AWS::EC2::Instance nella Guida per l'utente di AWS CloudFormation
Usa un AWS SDK specifico per la lingua per avviare un'istanza.	AWS SDK	AWS SDK per .NET AWS SDK per C++ AWS SDK per Go AWS SDK per Java AWS SDK per JavaScript AWS SDK per PHP V3 AWS SDK per Python AWS SDK per Ruby V3

Tutorial per avviare istanze EC2

Esistono diversi modi per avviare e configurare un'istanza Amazon EC2. Il metodo e la configurazione utilizzati dipendono dal caso d'uso specifico.

I seguenti tutorial possono aiutarti a imparare come avviare le istanze EC2. Se non sei esperto di Amazon EC2, ti consigliamo di iniziare dal primo tutorial. I tutorial iniziano presentandoti le nozioni di base e ti aiutano a sviluppare tali nozioni introducendo ulteriori opzioni di configurazione.

Obiettivo	Link al tutorial
Avvia la mia primissima istanza EC2 Scopri come avviare rapidamente un'istanz a Amazon EC2 utilizzando le impostazioni predefinite nella procedura guidata di avvio dell'istanza Amazon EC2. Scopri anche come rivedere i campi di configurazione dell'istanza e come terminarla. Durata: 10 minuti	Tutorial 1: Avvio della primissima istanza Amazon EC2
Avvia un'istanza EC2 di prova e connettiti a essa Scopri come avviare un'istanza Amazon EC2 da utilizzare a scopo di prova. Questa istanza non avrà alcuna configurazione avanzata e non memorizzerà informazioni sensibili. Scoprirai anche le impostazioni essenziali di configura zione dell'istanza, come connetterti all'istanza e come arrestarla. Durata: 30 minuti	Tutorial 2: Avvia un'istanza EC2 di prova e connettiti a essa

Cerchi altri tutorial?

- Tutorial: Installazione di un server LAMP su AL2023

- Tutorial: Configurazione SSL/TLS su AL2023
- Tutorial: Ospita un WordPress blog su AL2023
- Tutorial: Completa la configurazione richiesta per connettersi all'istanza tramite EC2 Instance Connect
- Tutorial: Connessione di un'istanza Amazon EC2 a un database Amazon RDS

Tutorial 1: Avvio della primissima istanza Amazon EC2

Attributo	Valore
Obiettivo del tutorial	Scopri come avviare rapidamente un'istanza Amazon EC2 utilizzando le impostazioni predefinite nella procedura guidata di avvio dell'istanza Amazon EC2. Scopri anche come rivedere i campi di configurazione dell'istanza e come terminarla.
Esperienza EC2	Principiante
Durata	10 minuti
Costo	Idoneo per il Piano gratuito Quando crei il tuo Account AWS, puoi iniziare a usare Amazon EC2 gratuitamente utilizzando il. Piano gratuito di AWS Se hai creato il tuo Account AWS prima del 15 luglio 2025, ha meno di 12 mesi e non hai ancora superato i vantaggi del piano gratuito per Amazon EC2, completare questo tutorial non ti costerà nulla, perché ti aiuteremo a selezionare le opzioni che rientrano nei vantaggi del piano gratuito. In caso contrario, ti verranno addebitati i costi di utilizzo standard di Amazon EC2 dal momento in cui avvii l'istanza

Attributo	Valore
	(anche se rimane inattiva) fino alla sua interruzione. Se hai creato il tuo Account AWS account il 15 luglio 2025 o dopo tale data, ha meno di 6 mesi e non hai esaurito tutti i crediti, completare questo tutorial non ti costerà nulla, perché ti aiutiamo a selezionare le opzioni che rientrano nei vantaggi del livello gratuito. Per informazioni su come determinare se disponi dell'idoneità al Piano gratuito, consulta the section called "Monitoraggio dell'utilizzo del piano gratuito".
Prerequisiti	• Devi disporre di un AWS account, configurare un utente con accesso amministratore e utilizzare l'utente amministratore per accedere al Console di gestione AWS. Non sai come procedere? Prova questo tutorial: Configurazione dell' AWS ambiente • È necessario avere una conoscenza generale della AWS console. Non sai da dove iniziare? Prova questa guida introduttiva: Guida introduttiva a Console di gestione AWS

Panoramica del tutorial

Questo tutorial è progettato per i principianti senza alcuna esperienza precedente nell'uso di Amazon EC2. Ti guideremo attraverso i passaggi per creare, o come diciamo noi, avviare, la tua primissima istanza EC2 utilizzando la console EC2. Un'istanza è essenzialmente un server web nel AWS cloud. Dopo aver avviato l'istanza, ti mostreremo come trovarla nella console. Infine, per aiutarti a gestire i costi, ti mostreremo come eliminare l'istanza, o come diciamo noi, interromperla.

Il tutorial si divide nelle seguenti attività brevi. Devi completare ogni attività prima di passare a quella successiva.

- Attività 1: Avvia la tua istanza
- Attività 2: Trovare l'istanza
- Attività 3: Visualizzazione della configurazione dell'istanza
- Attività 4: Interruzione di un'istanza

Attività 1: Avvia la tua istanza

In questa attività, intraprenderai il percorso più rapido per avviare l'istanza eseguendo solo le operazioni essenziali. Utilizzeremo la procedura guidata di avvio dell'istanza EC2, un modulo basato sul web che fornisce tutti i campi per la configurazione e l'avvio dell'istanza. Semplifica il processo fornendo valori predefiniti per i campi di configurazione dell'istanza.

Prima di iniziare

Assicurati di aver completato i prerequisiti elencati nella tabella precedente, incluso l'accesso Console di gestione AWS con il tuo utente amministratore.

Attieniti alla seguente procedura per avviare rapidamente la tua istanza

1. Aprire la console Amazon EC2:

   Passa a https://console.aws.amazon.com/ec2/.
2. Apri la procedura guidata di avvio dell'istanza EC2:

   Dal pannello di controllo EC2, scegli Avvia istanza.

   Viene visualizzato il modulo basato sul web Avvia un'istanza. Questa è la procedura guidata di avvio dell'istanza EC2.
3. Denomina l'istanza:

   In Nome e tag, per Nome, inserisci un nome descrittivo come **`My first EC2 instance`**.

   Sebbene non sia obbligatorio assegnare un nome all'istanza, ciò consente di identificarla in un secondo momento.
4. Procedi senza una coppia di chiavi:

In Coppia di chiavi (login), per Nome della coppia di chiavi, scegli Procedi senza una coppia di chiavi (non consigliato).

È possibile utilizzare una coppia di chiavi per un accesso sicuro. Tuttavia, poiché non accederemo all'istanza in questo tutorial, per ora non è necessaria una coppia di chiavi.

5. Avvio dell'istanza:

   Nel pannello Riepilogo a destra scegli Avvia istanza .

   Amazon EC2 avvia rapidamente l'istanza usando le impostazioni predefinite. Un banner di successo conferma l'avvio.

Complimenti! Hai avviato con successo la tua prima istanza EC2!

Attività 2: Trovare l'istanza

In questa attività, individuerai l'istanza che hai appena avviato nella console EC2.

Segui queste fasi per trovare l'istanza nella console EC2

1. Apri la pagina Istanze:

   Se sei ancora nella pagina di successo, scegli Istanze nel percorso di navigazione nella parte superiore dello schermo. Potresti dover selezionare prima i tre puntini per accedervi.

   Se hai abbandonato la pagina, scegli Istanze dal pannello di navigazione.
2. Individua la tua istanza:

   Nella colonna Nome, trova l'istanza in base al nome che le hai assegnato.

Attività 3: Visualizzazione della configurazione dell'istanza

In questa attività, acquisirai familiarità con la visualizzazione dei dettagli di configurazione dell'istanza.

Segui questi passaggi per visualizzare la configurazione dell'istanza

1. Individua l'ID dell'istanza:

   Nella colonna ID istanza, annota nota l'ID univoco della tua istanza. Inizia con i- seguito da 17 caratteri alfanumerici, ad esempio i-01aeed690c9fb5322.

L'ID dell'istanza viene assegnato automaticamente all'istanza quando viene avviata.

2. Apri la pagina dei dettagli dell'istanza:

   Nella colonna ID istanza, scegli il link dell'ID per aprire la pagina dei dettagli dell'istanza in cui puoi esaminarne la configurazione.

3. Esplora i dettagli della configurazione dell'istanza:

   Dedica qualche minuto a esplorare i dettagli di configurazione della tua istanza. Nel prossimo tutorial, approfondiremo la configurazione. Per il momento, sfrutta questo tempo per acquisire familiarità con la pagina dei dettagli dell'istanza.

   Suggerimento: per trovare rapidamente un campo, premi Ctrl+F o command+F sulla tastiera.

   a. Tipo di istanza: riesci a trovare il tipo di istanza? Potrebbe essere t3.micro, ad esempio.
   b. Indirizzo IPv4 pubblico: riesci a trovare l'indirizzo IPv4 pubblico che è stato assegnato alla tua istanza? È in un formato simile al seguente esempio: 34.242.148.128.
   c. Proprietario dell'istanza: riesci a identificare il proprietario di questa istanza? Sei tu! Il tuo Account AWS numero è riportato nel campo Proprietario.
   d. Tag dell'istanza: il nome che hai assegnato all'istanza è in realtà un tag. Riesci a trovare i tag della tua istanza? Selezionare la scheda Tag. La chiave è Nome e il valore è il nome che hai fornito.
   e. Ora di avvio: riesci a scoprire quando hai lanciato l'istanza? Scegli la scheda Dettagli e trova il campo Ora di avvio.
   f. Stato dell'istanza: riesci a verificare lo stato della tua istanza? Dovrebbe essere In esecuzione.

Dedica qualche altro minuto a esplorare gli altri dettagli di configurazione della tua istanza. Quando sei pronto, procedi all'attività successiva.

Attività 4: Interruzione di un'istanza

> ⚠ Warning
>
> La terminazione di un'istanza è permanente e irreversibile.
> Dopo aver terminato un'istanza, non puoi più connetterti a essa e non puoi ripristinarla.
> Inoltre, tutti i volumi Amazon EBS collegati e configurati per essere eliminati in caso di

terminazione vengono eliminati in modo definitivo e non possono essere recuperati. Tutti i dati archiviati nei volumi di archivio dell'istanza vengono persi in modo definitivo. Per ulteriori informazioni, consulta Come funziona la terminazione delle istanze.
Prima di terminare un'istanza, assicurati di aver eseguito il backup di tutti i dati che devi mantenere dopo la terminazione sull'archivio persistente.

In questa attività, eliminerai l'istanza per mantenere i vantaggi del piano gratuito. In EC2, interruzione è il termine usato per eliminare un'istanza.

Segui questi passaggi per interrompere l'istanza

1. Avvia l'interruzione:

   Se sei ancora nella pagina dei dettagli dell'istanza, scegli il menu Stato dell'istanza (in alto a destra), poi scegli Interrompi (elimina) istanza.

   Se hai abbandonato la pagina, scegli Istanze dal pannello di navigazione. Poi, nella pagina Istanze, seleziona la casella di spunta accanto al nome dell'istanza, quindi scegli il menu Stato dell'istanza (in alto a destra) e scegli Interrompi (elimina) istanza.
2. Conferma l'interruzione:

   Nella finestra Interrompi (elimina) istanza che si apre, scegli il pulsante Interrompi (elimina) per confermare che desideri interrompere l'istanza.
3. Monitora lo stato dell'istanza:

   Nella pagina Istanze, controlla la colonna Stato dell'istanza. Lo stato della tua istanza cambia in Shutting-down. Se non vedi il testo completo, prova ad allargare la colonna.

   Dopo la chiusura dell'istanza, Amazon EC2 la elimina e scompare dalla pagina Istanze.

Punti principali

In questo tutorial, abbiamo trattato i seguenti concetti chiave:

- L'istanza si riferisce a un server Web Amazon EC2 nel cloud. AWS
- Avvio si riferisce alla creazione di un'istanza EC2.
- Interruzione si riferisce all'eliminazione di un'istanza EC2.

- La procedura guidata di avvio dell'istanza EC2 contiene valori predefiniti per la configurazione dell'istanza, che consentono un avvio rapido e semplice dell'istanza.
- L'ID dell'istanza è un identificatore univoco assegnato automaticamente all'istanza, mentre il nome dell'istanza è un tag facoltativo che è possibile assegnare per facilitare l'identificazione.

Fasi successive

Per aumentare la sicurezza nell'avvio e nell'interruzione delle istanze, prova a ripetere i passaggi di questo tutorial. Assicurati di interrompere tutte le istanze che avvii per mantenere i vantaggi del piano gratuito.

Dopo aver acquisito dimestichezza con queste nozioni di base, passa al tutorial successivo, che fornisce un'analisi più approfondita dei principali campi di configurazione delle istanze.

Tutorial 2: Avvia un'istanza EC2 di prova e connettiti a essa

Attributo	Valore
Obiettivo del tutorial	Scopri come avviare un'istanza Amazon EC2 da utilizzare a scopo di prova. Questa istanza non avrà alcuna configurazione avanzata e non memorizzerà informazioni sensibili. Scoprirai anche le impostazioni essenziali di configura zione dell'istanza, come connetterti all'istanza e come arrestarla.
Esperienza EC2	Principiante
Durata	30 minuti
Costo	Idoneo per il Piano gratuito Quando crei il tuo Account AWS, puoi iniziare a usare Amazon EC2 gratuitamente utilizzando. Piano gratuito di AWS Se hai creato il tuo Account AWS prima del 15 luglio 2025, ha meno di 12 mesi e non hai ancora superato i vantaggi del piano

Attributo	Valore
	gratuito per Amazon EC2, completare questo tutorial non ti costerà nulla, perché ti aiuteremo a selezionare le opzioni che rientrano nei vantaggi del piano gratuito. In caso contrario, ti verranno addebitati i costi di utilizzo standard di Amazon EC2 dal momento in cui avvii l'istanza (anche se rimane inattiva) fino alla sua interruzione. Se hai creato il tuo Account AWS account il 15 luglio 2025 o dopo tale data, ha meno di 6 mesi e non hai esaurito tutti i crediti, completare questo tutorial non ti costerà nulla, perché ti aiutiamo a selezionare le opzioni che rientrano nei vantaggi del livello gratuito. Per informazioni su come determinare se disponi dell'idoneità al Piano gratuito, consulta the section called "Monitoraggio dell'utilizzo del piano gratuito".
Prerequisiti	Completo Tutorial 1: Avvio della primissima istanza Amazon EC2.

Panoramica del tutorial

Questo tutorial è progettato per i principianti che desiderano avviare un'istanza EC2 da utilizzare a scopo di prova.

Spiegheremo i campi di configurazione principali dell'istanza e poi ti guideremo attraverso i passaggi per avviare un'istanza di prova utilizzando i valori predefiniti nella console EC2. Dopo aver avviato l'istanza, ti mostreremo come accedere alla tua istanza (come diciamo noi, connettersi all'istanza). In questo tutorial, ti mostreremo anche come creare una coppia di chiavi, necessaria per connetterti alla tua istanza. Infine, per aiutarti a gestire i costi, ti mostreremo come arrestare l'istanza per evitare le commissioni di utilizzo.

In questo tutorial, avvierai un'istanza Linux. Sebbene i passaggi di questo tutorial possano essere utilizzati per avviare istanze con altri sistemi operativi, le istruzioni per la connessione a un'istanza sono specifiche per le istanze Linux.

Il tutorial si divide nelle seguenti attività brevi. Devi completare ogni attività prima di passare a quella successiva.

- Attività 1: Acquisisci familiarità con i componenti principali per l'avvio di un'istanza
- Attività 2: Revisione di un diagramma tecnico
- Attività 3: Crea una coppia di chiavi
- Attività 4: Avvia la tua istanza di prova
- Attività 5: Trovare l'istanza
- Attività 6: Visualizzazione della configurazione dell'istanza
- Attività 7: Acquisisci familiarità con i componenti principali per la connessione a un'istanza
- Attività 8: Connessione all'istanza
- Attività 9: Arrestare l'istanza

Attività 1: Acquisisci familiarità con i componenti principali per l'avvio di un'istanza

In questa attività, analizzerai i componenti principali necessari per avviare un'istanza EC2. Questi sono l'AMI, il tipo di istanza, la coppia di chiavi, il gruppo di sicurezza, la rete (VPC e sottorete) e il volume Amazon EBS. Scoprirai anche un componente opzionale, il tag Nome.

Per facilitare la visualizzazione di questi componenti, immagina un'istanza come una casa in affitto. Proprio come l'affitto di una casa ti offre un posto dove vivere senza dover possedere e mantenere la proprietà, le istanze EC2 forniscono potenza di elaborazione senza che tu debba possedere e mantenere l'infrastruttura sottostante.

Al momento di decidere il tipo di istanza da avviare, prenderai in considerazione i criteri di configurazione dell'istanza, proprio come analizzeresti i criteri che vorresti in una casa. Pur semplificando le cose, questa analogia offre un modo utile per visualizzare i componenti finché non li conosci meglio.

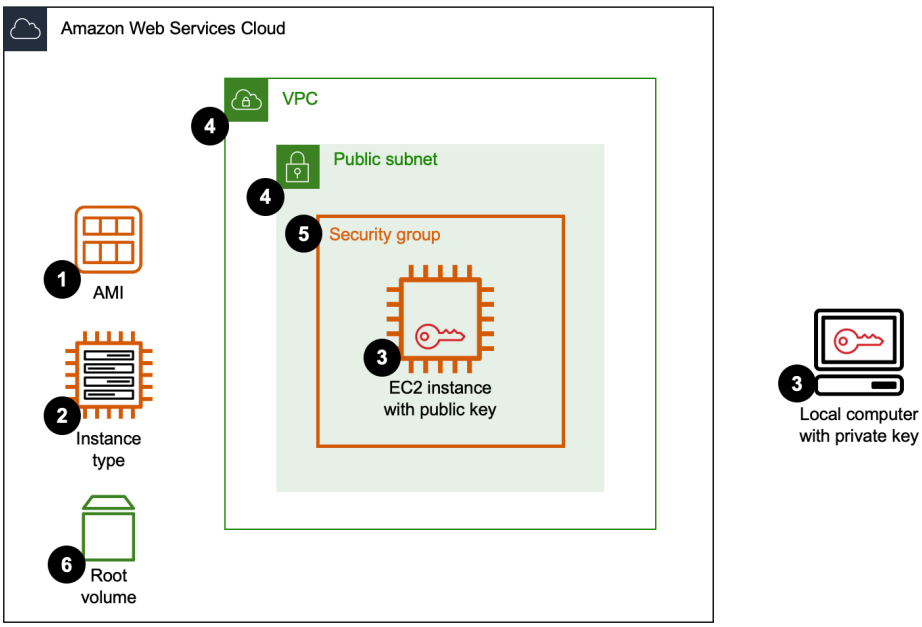
- AMI – Materiali da costruzione e accessori per la casa: l'Amazon Machine Image (AMI) determina il sistema operativo e le applicazioni con cui inizia l'istanza. È come scegliere i materiali da costruzione (come mattoni, acciaio o legno) e i servizi (come elettrodomestici e arredi) della

casa. Un'AMI di base è come una casa non arredata con elettrodomestici di base, mentre un'AMI personalizzata con software preinstallato è come una casa completamente ammobiliata.

- Tipo di istanza – Dimensioni e potenza della casa: il tipo di istanza definisce le dimensioni e le funzionalità dell'istanza EC2, proprio come scegliere le dimensioni di una casa, il numero di stanze e la capacità energetica. Ogni tipo di istanza determina la quantità di CPU, memoria, archiviazione e capacità di rete dell'istanza. L'AMI selezionata potrebbe limitare i tipi di istanza che puoi scegliere.
- Coppia di chiavi – Chiave della porta d'ingresso: una coppia di chiavi è come la serratura e la chiave della porta di casa. La chiave pubblica funge da blocco dell'istanza, mentre la chiave privata è la chiave da conservare in modo sicuro sul computer locale. Se qualcun altro entra in possesso della tua chiave privata, può accedere alla tua istanza, proprio come qualcuno con la chiave della porta di casa può entrare in casa tua.
- Rete (VPC e sottorete) – Confini della proprietà, aree sezionate e numero civico: il tuo cloud privato virtuale (VPC) è simile all'intera proprietà in cui si trova la casa e la sottorete è l'area sezionata intorno alla casa. Se nella proprietà sono presenti più case (istanze), è consigliabile suddividerle in aree distinte (sottoreti diverse) a seconda dello scopo. Alcune case consentono ai visitatori di muoversi liberamente nei giardini (sottoreti pubbliche con accesso a Internet), mentre altre dispongono di giardini recintati per limitare l'ingresso (sottoreti private senza accesso a Internet). Ogni sottorete contiene un intervallo di indirizzi IP, proprio come i numeri civici, che possono essere assegnati alle istanze nella sottorete.
- Gruppo di sicurezza: il portinaio – Il gruppo di sicurezza svolge la funzione di un portinaio, che controlla chi è autorizzato a visitare la tua casa. Applica un insieme di regole che controllano il traffico autorizzato a raggiungere la tua istanza. Ad esempio, una regola che consente il traffico SSH da un indirizzo IP specifico è come se il portinaio consentisse solo a una persona specifica di consegnare la spesa. Allo stesso modo, consentire il traffico HTTPS da qualsiasi luogo è come lasciare che il pubblico venga a dare un'occhiata all'esterno della casa.
- Volume Amazon EBS – Unità di archiviazione: i volumi EBS sono come unità di stoccaggio in cui è possibile riporre i propri effetti personali. Ogni istanza ha un volume root (dove è archiviata l'AMI) ed è possibile aggiungere altri volumi (archiviazione) in qualsiasi momento, se necessario.
- Tag del nome – Il nome della casa: il tag del Nome funge da insegna su una casa, aiutandoti a identificare facilmente chi ci vive. Sebbene il tag del Nome faciliti la distinzione tra le istanze, non è obbligatorio all'avvio di un'istanza.

Attività 2: Revisione di un diagramma tecnico

In questa attività, acquisirai familiarità con un tipico diagramma tecnico che utilizziamo nella AWS documentazione. Il seguente diagramma rappresenta la configurazione per l'istanza di prova che avvierai in questo tutorial. Nell'attività precedente, abbiamo introdotto questi componenti usando l'analogia di una casa in affitto. Ora ci concentreremo sui componenti EC2. Le etichette numerate corrispondono alle descrizioni che seguono.



1. AMI – L'AMI è l'immagine che scegli quando avvii un'istanza. Si tratta di un modello che contiene il sistema operativo e il software che verranno eseguiti sull'istanza. Ad esempio, se desideri avviare un'istanza Linux, puoi scegliere l'AMI Amazon Linux 2023. Oppure, se desideri avviare un'istanza Windows, puoi scegliere l'AMI di base di Microsoft Windows Server 2022. Il catalogo delle AMI nella console Amazon EC2 contiene migliaia di immagini tra cui scegliere.
2. Tipo di istanza – Il tipo di istanza è l'hardware che determina CPU, memoria, archiviazione e capacità di rete del computer host utilizzato per l'istanza. Amazon EC2 offre oltre 600 tipi di istanze tra cui scegliere, ognuna con configurazione hardware e dimensioni diverse, consentendoti di scegliere la soluzione più adatta alle esigenze della tua applicazione.
3. Coppia di chiavi – Una coppia di chiavi è un set di credenziali di sicurezza che puoi utilizzare per dimostrare la tua identità quando ti colleghi alla tua istanza. La chiave pubblica è nella tua istanza e la chiave privata è nel tuo computer locale.

   In EC2, la connessione all'istanza si riferisce all'accesso all'istanza dal computer locale. Sebbene esistano altri modi per connettersi in modo sicuro alla tua istanza, in questo tutorial utilizziamo una coppia di chiavi.

4. Rete – La rete è composta da un VPC e da una o più sottoreti. Un VPC è una rete virtuale all'interno di Cloud AWS. Ogni AWS cliente ha il proprio VPC dedicato al proprio. Account AWS Avvierai l'istanza in una sottorete nel VPC. Una sottorete è un intervallo di indirizzi IP all'interno di un VPC. La sottorete predefinita è una sottorete pubblica, il che significa che assegnerà un indirizzo IP pubblico e fornirà l'accesso a Internet all'istanza dall'esterno della rete Amazon.
5. Gruppo di sicurezza – Un gruppo di sicurezza agisce come un firewall per controllare il traffico verso l'istanza. Un gruppo di sicurezza contiene regole che consentono a determinati tipi di traffico di entrare nell'istanza. Per connetterti tramite SSH dal tuo computer locale all'istanza (usando la tua coppia di chiavi), ti serve una regola che consenta il traffico SSH dal tuo computer locale.
6. Volume EBS – Un volume Amazon EBS è un dispositivo di archiviazione che funziona come un disco rigido fisico. L'istanza è dotata di un volume root, che è un volume EBS speciale che memorizza l'AMI con il sistema operativo e il software necessari per avviare l'istanza. Facoltativamente, è possibile anche aggiungere volumi di dati. Tuttavia, poiché l'istanza di prova non archivia dati sensibili, non sono necessari volumi di dati crittografati aggiuntivi.

Complimenti! Hai completato le attività concettuali di questo tutorial. Nelle seguenti attività, utilizzerai la console Amazon EC2 per creare i componenti che hai studiato.

Attività 3: Crea una coppia di chiavi

In questa attività, creerai una coppia di chiavi. Una coppia di chiavi è composta da due parti: una chiave pubblica, che aggiungerai all'istanza, e una chiave privata corrispondente, che utilizzerai per connetterti in modo sicuro all'istanza. Nell'attività successiva, selezionerai questa coppia di chiavi quando avvii l'istanza, cosa che aggiunge automaticamente la chiave pubblica all'istanza. È fondamentale conservare la chiave privata in modo sicuro sul computer locale, perché chiunque vi acceda può connettersi all'istanza.

Se preferisci usare una coppia di chiavi esistente quando avvii l'istanza di prova, puoi saltare questa attività. Altrimenti, procedi con la creazione di una nuova coppia di chiavi.

Prima di iniziare

Assicurati di aver completato i prerequisiti elencati nella tabella precedente, incluso l'accesso Console di gestione AWS con il tuo utente amministratore.

Segui la procedura indicata di seguito per creare una coppia di chiavi

1. Aprire la console Amazon EC2:

Passa a https://console.aws.amazon.com/ec2/.

2. Vai alla pagina Coppia di chiavi della console:

   Nel riquadro di navigazione, sotto Network & Security (Rete e sicurezza), scegliere Key Pairs (Coppie di chiavi).

   - Se in precedenza hai creato coppie di chiavi, queste sono visualizzate nella tabella.
   - Se non esistono coppie di chiavi, la tabella è vuota.

3. Creazione di una nuova coppia di chiavi:

   Scegli il pulsante Crea coppia di chiavi (in alto a destra) per aprire il modulo basato sul web Crea coppia di chiavi e inserisci i dettagli della tua coppia di chiavi, nel modo seguente:

   a. Denomina la coppia di chiavi: per il Nome, inserisci un nome che ti aiuti a riconoscere la coppia di chiavi, come **`test-instance-key-pair`**.

      Il nome può essere composto da un massimo di 255 caratteri ASCII. Non può includere spazi iniziali o finali.

   b. Scegli il tipo di coppia di chiavi: per il Tipo di coppia di chiavi, scegli ED25519.

      Le istanze Linux supportano i tipi di chiave RSA e ED25519, mentre le istanze Windows supportano solo RSA. Poiché in questo tutorial avvierai un'istanza Linux, puoi usare una chiave ED25519.

   c. Scegli il formato del file per la chiave privata: per Formato file chiave privata, scegli .pem.

      Questo è il formato in cui verrà salvato il file della chiave privata.

4. Salva la chiave pubblica in Amazon EC2 e scarica la chiave privata:

   Scegli il pulsante Crea coppia di chiavi (in basso a destra).

   Amazon EC2 salva la chiave pubblica, mentre il browser scarica automaticamente il file della chiave privata sul tuo computer locale. Il file viene denominato in base al nome specificato per coppia di chiavi e l'estensione è il formato di file scelto. Sposta il file della chiave privata in una posizione sicura sul computer.

> **Important**
>
> Questo è l'unico momento che avrai per salvare il file della chiave privata.

5. Imposta le autorizzazioni sulla chiave (per utenti macOS e Linux):

   Se prevedi di connetterti alla tua istanza tramite SSH su un computer macOS o Linux, devi impostare le autorizzazioni corrette per il file della chiave privata. Apri una finestra di terminale ed esegui il comando seguente, sostituendolo *test-instance-key-pair* con il nome della tua coppia di chiavi:

   ```
   chmod 400 test-instance-key-pair.pem
   ```

   Questo comando garantisce che solo tu possa leggere il file della chiave privata, che è obbligatorio per stabilire una connessione sicura all'istanza. Senza queste autorizzazioni, non sarai in grado di connetterti tramite questa coppia di chiavi.

Complimenti! Hai creato con successo una coppia di chiavi!

Attività 4: Avvia la tua istanza di prova

In questa attività, avvierai rapidamente un'istanza di prova utilizzando la procedura guidata di avvio dell'istanza EC2. Preparerai le impostazioni di configurazione principali dell'istanza per un'istanza Linux e utilizzerai i valori predefiniti per gli altri campi.

Per aiutarti a gestire i costi, ti consigliamo di scegliere componenti idonei al livello gratuito.

Attieniti alla seguente procedura per avviare un'istanza di prova

1. Aprire la console Amazon EC2:

   Passa a https://console.aws.amazon.com/ec2/.

2. Apri la procedura guidata di avvio dell'istanza EC2:

   Dal pannello di controllo EC2, scegli Avvia istanza.

   Viene visualizzato il modulo basato sul web Avvia un'istanza. Questa è la procedura guidata di avvio dell'istanza EC2.

3. Denomina l'istanza:

In Nome e tag, per Nome, inserisci un nome descrittivo come **`Test instance`**.

Il nome dell'istanza è un tag, dove la chiave è Name (Nome) e il valore è il nome specificato.

Suggerimento: per le istanze di prova, è sufficiente un tag del nome. Tuttavia, per le istanze di produzione, è consigliabile stabilire una politica di etichettatura per standardizzare l'etichettatura su tutte le risorse.

4. Scegli il tuo sistema operativo e software – L'Amazon Machine Image (AMI):

   In Immagini di applicazioni e sistema operativo (Amazon Machine Image), per Amazon Machine Image (AMI), la selezione predefinita è Amazon Linux 2023 AMI. Questa AMI è contrassegnata Idonea per il piano gratuito. In questo tutorial, avvierai un'istanza Linux, quindi lascia l'impostazione predefinita per rimanere all'interno dei limiti del Piano gratuito.

5. Scegli il tuo hardware, ossia il tipo di istanza:

   In Tipo di istanza, per Tipo di istanza, mantieni la selezione predefinita per questo tutorial. Il tipo di istanza predefinito può essere utilizzato nell'ambito del Piano gratuito e il suo hardware è adatto all'istanza di test.

6. Preparati per accedere in modo sicuro con una coppia di chiavi:

   In Coppia di chiavi (login), per Nome coppia di chiavi, scegli la coppia di chiavi creata nell'attività precedente. Se la coppia di chiavi non è visualizzata nell'elenco, scegli l'icona di aggiornamento (a destra dell'elenco).

   All'avvio, la chiave pubblica sarà posizionata sull'istanza. Per connetterti all'istanza dopo l'avvio, userai la chiave privata corrispondente che hai scaricato nell'attività precedente.

7. Configura le impostazioni di rete per abilitare l'accesso a Internet:

   In Impostazioni di rete, i campi Rete (VPC) e Sottorete sono configurati per impostazione predefinita. Mantieni le impostazioni predefinite per questo tutorial per aiutarti a iniziare rapidamente. Se non hai modificato la sottorete predefinita, l'istanza avrà accesso a Internet.

   Suggerimento: la sottorete predefinita è una sottorete pubblica, il che significa che assegnerà un indirizzo IP pubblico e fornirà l'accesso a Internet all'istanza dall'esterno della rete Amazon. Per le istanze di prova, puoi utilizzare le impostazioni di sottorete predefinite che forniscono accesso a Internet. Tuttavia, per le istanze di produzione, è consigliabile assegnare un indirizzo IP pubblico e utilizzare una sottorete con accesso a Internet solo quando assolutamente necessario.

8. Configura il firewall dell'istanza (gruppo di sicurezza):

   In Impostazioni di rete, in Firewall (gruppi di sicurezza), mantieni selezionata la casella di spunta Consenti traffico SSH da qualsiasi luogo (0.0.0.0). Questo creerà un nuovo gruppo di sicurezza per l'istanza di prova che consente il traffico SSH da qualsiasi indirizzo IP.

   Un gruppo di sicurezza agisce come un firewall per controllare il traffico verso l'istanza. Per connetterti tramite SSH dal tuo computer locale all'istanza, ti serve una regola che consenta il traffico SSH dal tuo computer locale.

   Suggerimento: l'indirizzo IP del computer locale potrebbe cambiare nel tempo se il provider di servizi Internet usa l'assegnazione IP dinamica. Partiamo dal presupposto che quando utilizzi un'istanza a scopo di prova, non la utilizzerai per archiviare informazioni sensibili e pertanto le misure di sicurezza possano essere meno restrittive. Per le istanze di prova, è generalmente accettabile consentire il traffico proveniente da qualsiasi indirizzo IP (`0.0.0.0/0`) in modo da poterti connettere sempre anche se l'indirizzo IP cambia. Tuttavia, per le istanze di produzione, in particolare quelle con dati sensibili, è consigliabile consentire il traffico solo da indirizzi IP conosciuti.

9. Configura l'archiviazione dell'istanza:

   In Configura archiviazione, i campi Volume root (crittografato) sono configurati per impostazione predefinita. Lascia le impostazioni così come sono affinché rimangano al di sotto dei limiti previsti dal Piano gratuito.

   Poiché la nostra istanza di prova non archivia dati sensibili, non sono necessari volumi di dati crittografati aggiuntivi.

10. Esamina la configurazione dell'istanza:

    Nel pannello Riepilogo a destra puoi esaminare le impostazioni di alto livello prima di avviare l'istanza.

11. Avvio dell'istanza:

    Quando sei pronto per avviare l'istanza, nel pannello Riepilogo, scegli Avvia istanza.

    Amazon EC2 avvia rapidamente l'istanza usando le impostazioni da te specificate. Se non hai specificato un'impostazione, viene utilizzata quella predefinita. Un banner di successo conferma l'avvio.

Complimenti! Hai avviato con successo la tua istanza di prova!

Attività 5: Trovare l'istanza

In questa attività, individuerai l'istanza che hai appena avviato nella console EC2.

Segui queste fasi per trovare l'istanza nella console EC2

1. Apri la pagina Istanze:

   Se sei ancora nella pagina di successo, scegli l'ID dell'istanza nel banner di Successo.

   Se hai abbandonato la pagina, scegli Istanze dal pannello di navigazione.
2. Individua la tua istanza:

   Nella colonna Nome, trova l'istanza in base al nome che le hai assegnato.

Attività 6: Visualizzazione della configurazione dell'istanza

In questa attività, acquisirai familiarità con la visualizzazione dei dettagli di configurazione dell'istanza.

Segui questi passaggi per visualizzare la configurazione dell'istanza

1. Individua la tua istanza:

   Nella colonna Nome, trova l'istanza in base al nome che le hai assegnato.
2. Apri la pagina dei dettagli dell'istanza:

   Seleziona la casella di spunta accanto al nome dell'istanza, poi scegli il menu Operazioni (in alto a destra) e scegli Visualizza dettagli per aprire la pagina dei dettagli dell'istanza in cui puoi esaminarne la configurazione.

   Nel tutorial precedente, hai scelto il link ID dell'istanza per aprire la relativa pagina dei dettagli. Scoprirai che esiste più di un modo per eseguire un'attività nella console EC2.
3. Esplora i dettagli della configurazione dell'istanza:

   Dedica qualche minuto a esplorare i dettagli di configurazione della tua istanza.

   Suggerimento: per trovare rapidamente un campo, premi Ctrl+F o command+F sulla tastiera.

a. AMI: riesci a trovare l'AMI che hai usato per avviare la tua istanza? Puoi trovare le informazioni in ID AMI e Nome AMI nella scheda Dettagli.
b. Tipo di istanza: riesci a trovare il tipo di istanza? Potrebbe essere t3.micro, ad esempio.
c. Coppia di chiavi: riesci a trovare la coppia di chiavi selezionata all'avvio dell'istanza? È specificata per Coppia di chiavi assegnata all'avvio. Se modificherai la coppia di chiavi in futuro, il valore qui non cambierà.
d. VPC: riesci a trovare l'ID del tuo VPC? Troverai tutte le impostazioni di configurazione relative alla rete nella scheda Rete. L'ID VPC è in un formato simile al seguente esempio: vpc-1a2b3c4d
e. Sottorete: riesci a trovare l'ID della sottorete in cui hai avviato l'istanza? È in un formato simile al seguente esempio: subnet-1a2b3c4d
f. Indirizzo IPv4 pubblico: riesci a trovare l'indirizzo IPv4 pubblico che è stato assegnato alla tua istanza? È in un formato simile al seguente esempio: 34.242.148.128.
g. Gruppo di sicurezza: riesci a trovare la regola in entrata che è stata creata per consentire il traffico SSH da qualsiasi luogo (0.0.0.0./0)? Troverai tutte le impostazioni di configurazione relative alla sicurezza nella scheda Sicurezza.
h. Archiviazione: riesci a trovare il volume che è stato creato per questa istanza? Troverai tutte le impostazioni di configurazione relative all'archiviazione nella scheda Archiviazione.
i. Tag dell'istanza: il nome che hai assegnato all'istanza è in realtà un tag. Riesci a trovare i tag della tua istanza? Selezionare la scheda Tag. La chiave è Nome e il valore è il nome che hai fornito.
j. Stato dell'istanza: riesci a verificare lo stato della tua istanza? Dovrebbe essere In esecuzione.

Dedica qualche altro minuto a esplorare gli altri dettagli di configurazione della tua istanza. Quando sei pronto, procedi all'attività successiva.

Attività 7: Acquisisci familiarità con i componenti principali per la connessione a un'istanza

In questa attività, analizzerai i componenti principali necessari per connettersi a un'istanza EC2. Tali componenti sono il protocollo di connessione, il DNS pubblico, il gruppo di sicurezza, la coppia di chiavi e il nome utente dell'istanza.

Per facilitare la visualizzazione di questi componenti, immagina di connetterti a un'istanza come per andare a casa tua:

- Protocollo di connessione – La tua modalità di trasporto: proprio come scegliere come tornare a casa, scegli il protocollo di connessione che ti porterà alla tua istanza. In questo tutorial, useremo SSH (Secure Shell), che crea un tunnel sicuro per connettere il computer all'istanza tramite Internet.
- DNS pubblico – L'indirizzo della casa: proprio come la tua casa ha un indirizzo univoco, l'istanza EC2 ha il proprio nome DNS pubblico (ad esempio, `ec2-18-201-118-201.eu-west-1.compute.amazonaws.com`). Questo nome DNS pubblico consente a SSH di connettersi direttamente all'istanza.
- Gruppo di sicurezza – Il portinaio: Immagina che a casa tua ci sia un portinaio che controlla chi può entrare o uscire. Allo stesso modo, l'istanza EC2 dispone di un gruppo di sicurezza che funge da portinaio, che controlla quali tipi di traffico di rete sono consentiti in entrata o in uscita dall'istanza. È consentito l'ingresso solo del traffico esplicitamente consentito (ad esempio, il traffico SSH proveniente dall'indirizzo IP del computer).
- Chiave privata – La chiave della porta d'ingresso: quando hai avviato l'istanza, hai specificato una coppia di chiavi. La chiave pubblica è stata posizionata nell'istanza e la chiave privata è rimasta nel computer locale. La chiave privata funge da chiave della porta d'ingresso: senza di essa non puoi accedere all'istanza.
- Nome utente dell'istanza – L'inquilino: quando arrivi a casa, devi identificarti per dimostrare di essere l'inquilino. Allo stesso modo, quando ti connetti a un'istanza, fornisci un nome utente. Istanze diverse hanno nomi utente predefiniti diversi, a seconda del sistema operativo. Ad esempio, le istanze Amazon Linux utilizzano `ec2-user` come nome utente predefinito.

Il comando di connessione

Per connetterti all'istanza EC2, usa il seguente comando in una finestra del terminale:

```
ssh -i "test-instance-key-pair.pem" ec2-user@ec2-18-201-118-201.eu-
west-1.compute.amazonaws.com
```

Ecco un'analisi dettagliata di ciò che fa il comando:

- `ssh` – Questo comando specifica il protocollo di connessione, avviando una connessione SSH (Secure Shell) all'istanza.
- `-i "test-instance-key-pair.pem"` –Il flag `-i` indica il file della chiave privata necessario per autenticare la connessione. Questo file della chiave privata deve corrispondere alla coppia di

chiavi specificata all'avvio dell'istanza. Se il file della chiave privata viene salvato in una cartella particolare, specifica il percorso completo per il file.

- `ec2-user` – Questo è il nome utente per accedere all'istanza. Per le istanze Amazon Linux, il nome utente predefinito è `ec2-user`. Altre AMI potrebbero utilizzare nomi utente predefiniti diversi, come `ubuntu` per le istanze Ubuntu.
- `@` – Questo simbolo separa il nome utente dall'indirizzo dell'istanza.
- `ec2-18-201-118-201.eu-west-1.compute.amazonaws.com` – Questo è l'indirizzo pubblico dell'istanza (il DNS pubblico), che include l'indirizzo IPv4 pubblico e la Regione AWS. Identifica l'istanza in modo univoco.

Cosa succede quando esegui il comando

Dopo aver eseguito il comando, SSH stabilisce un tunnel sicuro ed effettua l'autenticazione con la chiave privata. Se il gruppo di sicurezza dell'istanza consente il traffico, ottieni l'accesso alla tua istanza EC2. Ora puoi controllare l'istanza dal tuo computer come se fossi seduto proprio di fronte ad essa. Puoi eseguire i comandi, installare software e gestire file, proprio come faresti sul tuo computer locale.

Attività 8: Connessione all'istanza

In questa attività, ti connetterai alla tua istanza tramite un client SSH sul tuo computer. Nell'attività precedente, abbiamo introdotto i componenti per la connessione a un'istanza utilizzando l'analogia di entrare a casa propria. Ora ci concentreremo sull'effettiva connessione all'istanza EC2.

Vi sono diversi modi per connettersi a un'istanza. Il metodo utilizzato per la connessione dipende dal sistema operativo dell'istanza. Dopo aver avviato un'istanza Linux, utilizzerai un client SSH sul computer locale.

Innanzitutto, controlla se sul tuo computer è installato un client SSH

La maggior parte dei computer include un client SSH preinstallato. Per controllare, apri una finestra del terminale sul tuo computer ed esegui il seguente comando:

```
ssh
```

Se il comando viene riconosciuto, sei pronto per la connessione.

Se il comando non viene riconosciuto, devi installare un client SSH. Le istruzioni per l'installazione di un client SSH non rientrano nell'ambito di questo tutorial. Se hai bisogno di assistenza, consulta

Prerequisiti per la connessione SSH in questa guida per l'utente o cerca online le istruzioni su come installare un client SSH sul tuo sistema operativo.

Segui questi passaggi per connetterti alla tua istanza

1. Inizia la connessione:

   Se ti trovi nella pagina dei dettagli dell'istanza nella console Amazon EC2, scegli il pulsante Connetti (in alto a destra).

   Se hai abbandonato la pagina, scegli Istanze dal pannello di navigazione. Poi, nella pagina Istanze, seleziona la casella di spunta accanto al nome dell'istanza e scegli il pulsante Connetti (in alto a destra).

   Si apre la pagina Connettiti all'istanza.
2. Scegli il metodo di connessione:

   Nella pagina Connettiti all'istanza, scegli la scheda Client SSH.

   Prenditi un momento per esaminare il testo in questa pagina, poiché questi sono i passaggi da rispettare in seguito.
3. Esamina il comando SSH:

   In Esempio, vedrai un comando che viene generato automaticamente e personalizzato con i dettagli della tua istanza. Il nome della chiave privata deriva dal nome della chiave pubblica specificata all'avvio.

   Il comando è simile al seguente:

   ```
   ssh -i "test-instance-key-pair.pem" ec2-user@ec2-18-201-118-201.eu-
   west-1.compute.amazonaws.com
   ```
4. Copia il comando SSH:

   Scegli l'icona di copia accanto al comando SSH di esempio.
5. Apri una finestra del terminale:

   Sul tuo computer locale, apri una finestra del terminale.
6. Incolla ed esegui il comando SSH:

Incolla il comando SSH nella finestra del terminale. Se hai salvato il file della chiave privata in una cartella specifica, modifica il comando per includere il percorso completo per il file.

Premi Invio sulla tastiera.

Noterai una risposta simile alla seguente:

```
The authenticity of host 'ec2-18-201-118-201.eu-west-1.compute.amazonaws.com
 (18-201-118-201)' can't be established.
ED25519 key fingerprint is SHA256:examplehxj9aOr1MogvKOoMNskVVIRBQBoq0example.This
 key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

7. Completa la connessione:

   Inserisci **`yes`** e premi Indietro sulla tastiera.

   La verifica dell'impronta digitale non rientra nell'ambito di questo tutorial. Per ulteriori informazioni, consulta (Opzionale) Ottenimento dell'impronta dell'istanza.

   Dopo una connessione riuscita, il prompt del terminale cambia per visualizzare il DNS pubblico dell'istanza.

Complimenti! Ti sei connesso con successo alla tua istanza!

Attività 9: Arrestare l'istanza

In questa attività, arresterai l'istanza per mantenere i vantaggi del piano gratuito. Quando l'istanza viene arrestata, non dovrai più sostenere i relativi costi. Se hai creato il tuo Account AWS prima del 15 luglio 2025 e sei idoneo per il piano gratuito, continuerai a sostenere i costi per lo storage EBS.

Segui questi passaggi per arrestare la tua istanza

1. Inizia l'arresto:

   Se sei ancora nella pagina Connettiti all'istanza, scegli Istanze dal percorso di navigazione. Se hai abbandonato la pagina, scegli Istanze dal pannello di navigazione.

   Poi, nella pagina Istanze, seleziona la casella di spunta accanto al nome dell'istanza, quindi scegli il menu Stato dell'istanza (in alto a destra) e scegli Arresta istanza. Quando viene richiesto, scegli Arresta.

2. Monitora lo stato dell'istanza:

   Nella pagina Istanze, controlla la colonna Stato dell'istanza. Lo stato dell'istanza cambia a In arresto e poi Arrestata. Se non vedi il testo completo, prova ad allargare la colonna.

   Se ritieni che lo stato dell'istanza sia cambiato da In arresto ad Arrestata, ma ancora non lo vedi, scegli l'icona di aggiornamento (sopra la tabella) per aggiornare la tabella Istanze.

Punti principali

In questo tutorial, abbiamo trattato i seguenti concetti chiave:

- AMI si riferisce a un'Amazon Machine Image, ossia un modello che contiene il sistema operativo e il software necessari per avviare un'istanza.
- Tipo di istanza si riferisce all'hardware del computer host utilizzato per la tua istanza. Determina la quantità di CPU, memoria, archiviazione e capacità di rete dell'istanza.
- Coppia di chiavi si riferisce all'insieme di chiavi pubbliche e private che puoi usare per connetterti in modo sicuro all'istanza.
- Per rete si intendono un VPC (un cloud privato virtuale dedicato al tuo account all'interno del AWS Cloud) e una sottorete (un intervallo di indirizzi IP all'interno del tuo VPC).
- Gruppo di sicurezza si riferisce a un insieme di regole che controllano il traffico che può raggiungere l'istanza.
- Volume EBS si riferisce all'archiviazione di dati per l'istanza. Ogni istanza ha un volume root per l'archiviazione dell'AMI e uno o più volumi di dati opzionali.
- I tag sono metadati che puoi assegnare facoltativamente alla tua istanza. Il nome dell'istanza è un tag, la cui Chiave è il Nome e il Valore è la tua scelta.
- La connessione si riferisce all'accesso all'istanza tramite Internet.
- SSH si riferisce al protocollo di connessione Secure Shell che puoi usare per connetterti alla tua istanza.
- Il DNS pubblico è l'indirizzo pubblico univoco dell'istanza.
- Il nome utente dell'istanza è determinato dal sistema operativo dell'istanza ed è obbligatorio per la connessione.
- L'arresto dell'istanza interrompe i costi per l'istanza, ma i costi di archiviazione EBS rimangono inalterati.

Fasi successive

Per aumentare la sicurezza nell'avvio, nella connessione e nell'arresto delle istanze, prova a ripetere i passaggi di questo tutorial. Assicurati di interrompere tutte le istanze che avvii per mantenere i vantaggi del piano gratuito.

Dopo aver acquisito dimestichezza con queste nozioni di base, puoi esplorare tutorial più avanzati. Per altri tutorial, consulta Cerchi altri tutorial?

Se hai creato il tuo Account AWS prima del 15 luglio 2025, considera la possibilità di guardare il seguente video di 6 minuti: Come posso evitare gli addebiti sul mio account quando utilizzo i servizi Piano gratuito di AWS

Se hai creato il tuo account il Account AWS 15 luglio 2025 o dopo tale data, valuta la possibilità di consultare le seguenti informazioni: Esplora i AWS servizi con il piano AWS gratuito nella Guida per l'utente AWS Billing

Riferimento per i parametri di configurazione delle EC2 istanze Amazon

La procedura guidata di avvio dell'istanza e il modello di avvio nella EC2 console Amazon forniscono tutti i parametri per la configurazione di un'istanza Amazon EC2 .

Ad eccezione della coppia di chiavi, la procedura guidata di avvio dell'istanza fornisce un valore predefinito per ciascun parametro. È possibile accettare uno o tutti i valori predefiniti, o configurare un'istanza i propri valori. Quando crei un modello di avvio, i parametri sono facoltativi. Se utilizzi un modello di avvio per avviare un'istanza, i parametri specificati nel modello di avvio sostituiscono i valori predefiniti nella procedura guidata di avvio dell'istanza. Qualsiasi parametro non specificato nel modello di avvio utilizzerà per impostazione predefinita il valore fornito dalla procedura guidata di avvio dell'istanza.

I parametri sono raggruppati nella procedura guidata di avvio dell'istanza e nel modello di avvio. Le seguenti descrizioni sono presentate in base ai raggruppamenti di parametri nella console.

Parametri per la configurazione di un'istanza

- Nome e tag
- Immagini di applicazioni e sistema operativo (Amazon Machine Image)
- Tipo di istanza
- Coppia di chiavi (login)

- Impostazioni di rete
- Per configurare l'archiviazione
- Dettagli avanzati
- Riepilogo

Nome e tag

Il nome dell'istanza è un tag, dove la chiave è Name (Nome) e il valore è il nome specificato. Puoi applicare tag all'istanza, ai volumi e alle interfacce di rete. Per le istanze spot, è possibile aggiungere un tag solo alla richiesta di istanza spot. Per ulteriori informazioni sui tag, consulta Tagging delle risorse Amazon EC2..

La specifica di un nome di istanza e dei tag aggiuntivi è facoltativa.

- Per Name (Nome), inserire un nome descrittivo per l'istanza. Se non si specifica un nome, l'istanza può essere identificata dal relativo ID, che viene generato automaticamente all'avvio dell'istanza.
- Per aggiungere altri tag, scegliere Add additional tags (Aggiungi altri tag). Scegliere Add tag (Aggiungi tag), quindi immettere una chiave e un valore e selezionare il tipo di risorsa da taggare. Scegliere Add tag (Aggiungi tag) per ogni tag aggiuntivo.

Puoi specificare solo il nome dell'istanza al momento dell'avvio dell'istanza. Non puoi denominare l'istanza quando crei un modello di avvio, ma puoi aggiungere tag per le risorse create all'avvio dell'istanza.

Immagini di applicazioni e sistema operativo (Amazon Machine Image)

Un'Amazon Machine Image (AMI) contiene tutte le informazioni necessarie per creare un'istanza. Ad esempio, un'AMI può contenere il software necessario per fungere da server Web, ad esempio Linux, Apache e il sito Web.

È possibile trovare un'AMI adatta come descritto di seguito: In caso contrario, scegliere Cancel (Annulla) (in alto a destra) per tornare alla procedura guidata di avvio istanza senza scegliere un'AMI.

Barra di ricerca

Per cercare tra tutte le opzioni disponibili AMIs, inserisci una parola chiave nella barra di ricerca AMI e premi Invio. Scegliere Select (Seleziona) per selezionare l'AMI.

Recents (Recenti

Quello AMIs che hai usato di recente.

Scegliere Recently launched (Avviati di recente) o Currently in use (Correntemente in uso) e poi, da Amazon Machine Image (AMI), selezionare un'AMI.

La mia AMIs

I dati privati AMIs che possiedi o quelli privati AMIs che sono stati condivisi con te.

Scegliere Owned by me (Di mia proprietà) o Shared with me (Condiviso con me) e poi, da Amazon Machine Image (AMI), selezionare un'AMI.

Quick Start

AMIs sono raggruppati per sistema operativo (OS) per aiutarti a iniziare rapidamente.

Per prima cosa selezionare il sistema operativo di cui si ha bisogno e quindi da Amazon Machine Image (AMI), selezionare un'AMI. Per selezionare un AMI che può essere utilizzato nel piano AWS gratuito, assicurati che l'AMI sia contrassegnato come idoneo per il livello gratuito.

Sfoglia altro AMIs

Scegli Sfoglia altro AMIs per sfogliare il catalogo AMI completo.

- Per cercare tra tutti quelli disponibili AMIs, inserisci una parola chiave nella barra di ricerca, quindi premi Invio.
- Per trovare un'AMI utilizzando un parametro di Systems Manager, seleziona il pulsante freccia a destra della barra di ricerca, quindi scegli Search by Systems Manager parameter (Cerca per parametro Systems Manager). Per ulteriori informazioni, consulta Fai riferimento alle AMI usando i parametri Systems Manager.
- Per cercare per categoria, scegli Quickstart AMIs AMIs Marketplace AWS AMIs, My o Community AMIs.

  Marketplace AWS È un negozio online in cui è possibile acquistare software funzionanti AWS, tra cui AMIs. Per ulteriori informazioni sull'avvio di un'istanza da Marketplace AWS, consultaAvvia un'istanza Amazon EC2 da un'AMI Marketplace AWS. In Community AMIs, puoi scoprire AMIs che i membri AWS della comunità lo hanno reso disponibile per l'uso da parte di altri. AMIsda Amazon o da un partner verificato sono contrassegnati come fornitore verificato.
- Per filtrare l'elenco di AMIs, seleziona una o più caselle di controllo in Perfeziona i risultati a sinistra dello schermo. Le opzioni di filtro sono diverse a seconda della categoria di ricerca selezionata.

- Controllare le voci per ciascuna AMI nell'elenco Root device type (Tipo dispositivo root). Nota quali AMIs sono i tipi di cui hai bisogno: ebs (supportato da Amazon EBS) o instance-store (supportato da instance store). Per ulteriori informazioni, consulta Tipo di volume root.
- Controllare le voci per ciascuna AMI nell'elenco Virtualization type (Tipo di virtualizzazione). Nota quali AMIs sono i tipi che ti servono: hvm o paravirtual. Ad esempio, alcuni tipi di istanza richiedono HVM. Per ulteriori informazioni sui tipi di virtualizzazione Linux, consulta Tipi di virtualizzazione.
- Controllare la modalità di avvio elencata per ogni AMI. Nota quali AMIs usano la modalità di avvio di cui hai bisogno: legacy-bios, uefi o uefi-preferred. Per ulteriori informazioni, consulta Comportamento di avvio delle istanze con le modalità di avvio di Amazon EC2.
- Scegliere un'AMI conforme alle specifiche esigenze, quindi scegliere Select (Seleziona).

Avviso relativo alle modifiche dell'AMI

All'avvio di un'istanza, se modifichi la configurazione di volumi o gruppi di sicurezza associati all'AMI selezionata e successivamente scegli un'AMI diversa, viene visualizzata una finestra che informa che alcune delle impostazioni correnti verranno modificate o rimosse. Puoi esaminare le modifiche apportate ai gruppi di sicurezza e ai volumi. Inoltre, puoi visualizzare quali volumi verranno aggiunti ed eliminati oppure visualizzare solo i volumi che verranno aggiunti. Questo avviso non viene visualizzato quando si crea un modello di avvio.

Tipo di istanza

Il tipo di istanza definisce la configurazione hardware e le dimensioni dell'istanza. I tipi di istanza più grandi dispongono di una maggiore quantità di CPU e memoria. Per ulteriori informazioni, consulta Tipi di EC2 istanze Amazon.

- Instance type (Tipo di istanza): assicurarsi che il tipo di istanza sia compatibile con l'AMI specificata. Per ulteriori informazioni, consulta Tipi di istanza Amazon EC2.

  Piano gratuito: puoi utilizzare tipi di istanze etichettati come Idoneo per il Piano gratuito gratuitamente nell'ambito del Piano gratuito. I tipi di istanza specifici dipendono da quando hai creato il tuo Account AWS.

  Se l'hai creata Account AWS prima del 15 luglio 2025 e ha meno di 12 mesi, puoi utilizzare Amazon EC2 nel piano gratuito selezionando il tipo di istanza t2.micro o il tipo di istanza t3.micro nelle regioni in cui t2.micro non è disponibile. Tieni presente che quando avvii un'istanza t3.micro,

l'impostazione predefinita è la modalità Illimitata, che potrebbe comportare costi aggiuntivi in base all'utilizzo della CPU.

Se hai creato la tua il Account AWS 15 luglio 2025 o successivamente, puoi utilizzare i tipi di istanza t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large e m7i-flex.large per 6 mesi o fino all'esaurimento dei crediti.

Per ulteriori informazioni, consulta Vantaggi del piano gratuito prima e dopo il 15 luglio 2025.

- Confronta i tipi di istanza: puoi confrontare diversi tipi di istanza in base ai seguenti attributi: numero di vCPUs, architettura, quantità di memoria (GiB), quantità di spazio di archiviazione (GB), tipo di archiviazione e prestazioni di rete.
- Chiedi consigli: puoi ottenere indicazioni e suggerimenti per i tipi di istanza dal Finder dei tipi di EC2 istanza. Per ulteriori informazioni, consulta Ottieni consigli dallo strumento di ricerca del tipo di istanza EC2.
- (Solo modelli di avvio) Avanzato: per specificare gli attributi dell'istanza e consentire ad Amazon di EC2 identificare i tipi di istanza con tali attributi, scegli Avanzato, quindi scegli Specificare gli attributi del tipo di istanza.
  - Numero di v CPUs: inserisci il numero minimo e massimo di v CPUs per i tuoi requisiti di elaborazione. Per indicare nessun limite, inserire un valore minimo **0** e lasciare vuoto il campo del valore massimo.
  - Amount of memory (MiB) (Quantità di memoria [MiB]): inserire la quantità minima e massima di memoria, in MiB, per i propri requisiti di calcolo. Per indicare nessun limite, inserire un valore minimo **0** e lasciare vuoto il campo del valore massimo.
  - Espandere Optional instance type attributes (Attributi facoltativi del tipo di istanza) e scegliere Add attribute (Aggiungi attributo) per esprimere i requisiti di calcolo in modo più dettagliato. Per informazioni su ogni attributo, InstanceRequirementsRequestconsulta Amazon EC2 API Reference.
  - Resulting instance types (Tipi di istanza risultanti): è possibile visualizzare in anteprima i tipi di istanza che corrispondono agli attributi specificati. Per escludere i tipi di istanza, scegliere Add attribute (Aggiungi attributo), quindi dall'elenco Attribute (Attributo), scegliere Excluded instance types (Tipi di istanza escluse). Dall'elenco Attribute value (Valore attributo), selezionare i tipi di istanza da escludere.

Coppia di chiavi (login)

In Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente oppure scegliere Create new key pair (Crea nuova coppia di chiavi) per creane una nuova. Per ulteriori informazioni, consulta Coppie di chiavi Amazon EC2 e istanze Amazon EC2.

> **Important**
>
> Se si sceglie l'opzione Proceed without key pair (Not recommended) (Procedi senza una coppia di chiavi [non consigliato]), non sarà possibile connetterti all'istanza a meno che non si scelga un'AMI configurata per offrire agli utenti un metodo di accesso alternativo.

Impostazioni di rete

Le impostazioni di rete definiscono gli indirizzi IP, i gruppi di sicurezza e le interfacce di rete per le istanze. Puoi utilizzare le impostazioni di rete predefinite o configurarle in base alle esigenze.

- (Solo procedura guidata di avvio dell'istanza) VPC: scegli un VPC esistente per la tua istanza. Il VPC predefinito per la Regione viene selezionato per impostazione predefinita. In alternativa, puoi scegliere un VPC che hai creato o che è stato condiviso con te. Per ulteriori informazioni, consulta Cloud privati virtuali per le istanze EC2.
- Subnet: scegli una sottorete per la tua istanza o scegli Crea nuova sottorete per crearne una nuova utilizzando la console Amazon VPC.
  - Puoi creare una sottorete in qualsiasi zona di disponibilità, Local Zone, Zona Wavelength o Outpost per il VPC selezionato.
  - Per avviare l'istanza in una sottorete IPv6 solo, l'istanza deve essere un'istanza basata su Nitro.
- (Solo procedura guidata di avvio dell'istanza) Assegna automaticamente IP pubblico: abilita o disabilita l'assegnazione automatica degli indirizzi pubblici. IPv4 Quando si esegue l'avvio delle istanze in una sottorete predefinita, il valore predefinito è Abilita. Quando si esegue l'avvio delle istanze in una sottorete non predefinita, il valore predefinito è Disabilita. Per ulteriori informazioni, consulta Indirizzi IPv4 pubblici.

  Non puoi abilitare questa opzione per sottoreti non predefinite se aggiungi un'interfaccia di rete secondaria. Per ulteriori informazioni, consulta the section called "Assegnare un indirizzo IPv4 pubblico all'avvio".

- (Avvia solo la procedura guidata dell'istanza) Assegna automaticamente IPv6 IP: abilita o disabilita l'assegnazione automatica degli indirizzi. IPv6 Per ulteriori informazioni, consulta Indirizzi IPv6.
- Firewall (gruppo di sicurezza): scegli un gruppo di sicurezza esistente o creane uno nuovo. Assicurati che il tuo gruppo di sicurezza disponga di regole che consentano il traffico da e verso le tue istanze. Tutto il traffico rimanente verrà ignorato.

  Se crei un nuovo gruppo di sicurezza, creiamo automaticamente una regola in entrata che consente di connetterti all'istanza da tutti gli indirizzi IP tramite Secure Shell (SSH) (istanze Linux) o Remote Desktop Protocol (RDP) (istanze Windows). Non puoi rimuovere né modificare questa regola. Puoi aggiungere regole in base alle tue esigenze. Per ulteriori informazioni, consulta Configurazione delle regole per i gruppi di sicurezza.

  > **Warning**
  >
  > Le regole che abilitano tutti gli indirizzi IP per accedere all'istanza tramite SSH o RDP sono accettabili se si avvia brevemente un'istanza di test e la si interrompe o termina dopo un breve periodo di tempo. Non sono sicure per gli ambienti di produzione. Dovrai autorizzare solo un determinato intervallo di indirizzi IP per accedere alle istanze.

  Questo gruppo di sicurezza viene aggiunto all'interfaccia di rete principale e a tutte le interfacce di rete secondarie. Puoi selezionare gruppi di sicurezza aggiuntivi per le interfacce di rete, ma non puoi rimuovere quello selezionato qui.
- Configurazione di rete avanzata: puoi configurare l'interfaccia di rete principale in base alle esigenze. Per aggiungere un'interfaccia di rete secondaria, seleziona Aggiungi interfaccia di rete. Il numero di interfacce di rete che puoi aggiungere dipende dal tipo di istanza selezionato. Nota che questa sezione è disponibile solo se scegli una sottorete.
  - Indice del dispositivo: l'indice del dispositivo. L'interfaccia di rete primaria deve essere assegnata all'indice 0.
  - Interfaccia di rete: l'interfaccia di rete. Seleziona Nuova interfaccia per consentire ad Amazon di EC2 creare una nuova interfaccia o seleziona un'interfaccia di rete esistente e disponibile. Se selezioni un'interfaccia di rete esistente come interfaccia di rete primaria, non puoi abilitare Assegna IP pubblico automaticamente per sottoreti non predefinite.
  - Descrizione: una descrizione per la nuova interfaccia di rete.
  - Subnet (Sottorete): la sottorete nella quale creare la nuova interfaccia di rete. L'istanza viene avviata nella stessa sottorete dell'interfaccia di rete principale.

Devi scegliere una sottorete dell'interfaccia di rete secondaria dalla stessa zona di disponibilità della sottorete dell'interfaccia di rete primaria. Se selezioni una sottorete da un altro VPC, viene visualizzata l'etichetta Multi-VPC accanto all'interfaccia di rete. Ciò consente di creare istanze multi-homed VPCs con diverse configurazioni di rete e sicurezza.

Per avviare un' EC2 istanza in una sottorete IPv6 solo, è necessario utilizzare un'istanza basata su Nitro. Quando si avvia un'istanza IPv6 -only, è possibile che DHCPv6 non fornisca immediatamente all'istanza il name server DNS. IPv6 Durante questo ritardo iniziale, l'istanza potrebbe non essere in grado di risolvere i domini pubblici. È possibile modificare il file di configurazione e ridefinire l'immagine dell'AMI in modo che il file abbia l'indirizzo del IPv6 nameserver DNS immediatamente dopo l'avvio.

- Gruppi di sicurezza: i gruppi di sicurezza da associare all'interfaccia di rete. Devi scegliere un gruppo di sicurezza dallo stesso VPC della sottorete dell'interfaccia di rete.
- (Solo modelli di avvio) Assegna automaticamente un IP pubblico: specifica se l'istanza riceve un indirizzo pubblico. IPv4 Per impostazione predefinita, le istanze in una sottorete predefinita ricevono un IPv4 indirizzo pubblico, mentre le istanze in una sottorete non predefinita no. Selezionare Enable (Abilita) o Disable (Disabilita) per sostituire l'impostazione di default della sottorete. Per ulteriori informazioni, consulta Indirizzi IPv4 pubblici.
- IP primario: un IPv4 indirizzo privato compreso nell'intervallo della sottorete. Lascia vuoto per consentire ad Amazon di EC2 scegliere un IPv4 indirizzo privato per te.
- IP secondario: IPv4 indirizzi privati aggiuntivi dall'intervallo della sottorete. Scegli Assegna manualmente e inserisci un IPv4 indirizzo. Scegli Aggiungi IP per aggiungere un altro IPv4 indirizzo. In alternativa, scegli Assegna automaticamente e inserisci un valore per indicare il numero di IPv4 indirizzi che Amazon EC2 sceglie per te.
- (IPv6-only) IPv6 IPs: IPv6 indirizzi dell'intervallo della sottorete. Scegli Assegna manualmente e inserisci un indirizzo. IPv6 Scegli Aggiungi IP per aggiungere un altro IPv6 indirizzo. In alternativa, scegli Assegna automaticamente e inserisci un valore per indicare il numero di IPv6 indirizzi che Amazon EC2 sceglie per te.
- IPv4 Prefissi: i IPv4 prefissi per l'interfaccia di rete. Scegli Assegna manualmente e inserisci un prefisso. IPv4 In alternativa, scegli Assegna automaticamente e inserisci un valore per indicare il numero di IPv4 prefissi che Amazon EC2 sceglie per te.
- IPv6 Prefissi: i prefissi per l' IPv6 interfaccia di rete. Scegli Assegna manualmente e inserisci un prefisso. IPv6 In alternativa, scegli Assegna automaticamente e inserisci un valore per indicare il numero di IPv6 prefissi che Amazon EC2 sceglie per te.

- (Dual-stack e IPv6 solo) Assegna IPv6 IP primario: se selezioni una sottorete dual-stack o -only, assegna un indirizzo principale. IPv6 IPv6 Questo aiuta a evitare interruzioni del traffico verso l'istanza o l'interfaccia di rete. Abilita questa opzione se ti affidi al fatto che l'indirizzo non cambi. IPv6 Non puoi rimuovere l' IPv6 indirizzo principale in un secondo momento. Quando abiliti un indirizzo IPv6 GUA come primario IPv6, il primo IPv6 GUA diventa l' IPv6 indirizzo principale finché l'istanza non viene terminata o l'interfaccia di rete non viene scollegata. Se hai più IPv6 indirizzi associati a un'interfaccia di rete e consenti ad Amazon di EC2 assegnare un IPv6 indirizzo primario, il primo indirizzo IPv6 GUA associato all'interfaccia di rete è l' IPv6 indirizzo primario.
- Elimina al termine: indica se eliminare l'interfaccia di rete quando l'istanza viene eliminata.
- Tipo di interfaccia: il tipo di interfaccia di rete:
  - ENA: un'interfaccia di rete ad alte prestazioni progettata per gestire velocità e packet-per-second velocità elevate per i TCP/IP protocolli, riducendo al minimo l'utilizzo della CPU. Si tratta del valore di default. Per ulteriori informazioni su ENA, consulta Elastic Network Adapter.
  - EFA con ENA: un'interfaccia di rete che supporta sia i dispositivi ENA che EFA per il trasporto tradizionale insieme al trasporto TCP/IP basato su SRD. Per ulteriori informazioni su EFA, consulta Elastic Fabric Adapter.
  - Solo EFA: un'interfaccia di rete ad alte prestazioni progettata per gestire comunicazioni tra nodi con throughput elevato e bassa latenza per il trasporto basato su SRD aggirando lo stack del sistema operativo. Le interfacce di rete solo EFA non supportano gli indirizzi IP. Per ulteriori informazioni su EFA, consulta Elastic Fabric Adapter.
- Elastic Fabric Adapter (EFA): indica se l'interfaccia di rete sia di tipo Elastic Fabric Adapter (EFA). Per ulteriori informazioni, consulta Elastic Fabric Adapter per AI/ML carichi di lavoro HPC su Amazon EC2.
- Indice della scheda di rete: l'indice della scheda di rete. L'interfaccia di rete primaria deve essere assegnata all'indice della scheda di rete 0. Alcuni tipi di istanza supportano più schede di rete.
- ENA Express: ENA Express è alimentato dalla tecnologia AWS Scalable Reliable Datagram (SRD). La tecnologia SRD utilizza un meccanismo di distribuzione dei pacchetti ("packet spraying") per distribuire il carico ed evitare la congestione della rete. L'abilitazione di ENA Express consente alle istanze supportate di comunicare utilizzando SRD in aggiunta al normale traffico TCP, quando possibile. La procedura guidata di avvio dell'istanza o il modello di avvio non include la configurazione ENA Express per l'istanza, a meno che non si selezioni Abilita o Disabilita dall'elenco.

- UDP ENA Express: se hai abilitato ENA Express, puoi facoltativamente utilizzarlo per il traffico UDP. La procedura guidata di avvio dell'istanza o il modello di avvio non include la configurazione ENA Express per l'istanza, a meno che non si selezioni Abilita o Disabilita.

Per configurare l'archiviazione

L'AMI selezionata include uno o più volumi di archiviazione, compreso il volume dispositivo root. È possibile specificare altri volumi da collegare all'istanza.

(Solo procedura guidata di avvio dell'istanza) Puoi utilizzare la visualizzazione Semplice o Avanzata. Con la vista Simple (Semplice), si specificano la dimensione e il tipo di volume. Per specificare tutti i parametri del volume, scegli la vista Advanced (Avanzata) (nella parte superiore destra della scheda).

Con la vista Avanzato, è possibile configurare ciascun volume come segue:

- Storage type (Tipo di archiviazione): selezionare volumi Amazon EBS o dell'archivio istanza da associare alla propria istanza. I tipi di volume disponibili nell'elenco dipendono dal tipo di istanza scelta. Per ulteriori informazioni , consulta Archivio dell'istanza archiviazione a blocchi temporanea per le istanze EC2 e Volumi Amazon EBS.
- Device (Dispositivo): selezionare dall'elenco di nomi dei dispositivi disponibili per il volume.
- Snapshot: selezionare lo snapshot da cui ripristinare il volume. È inoltre possibile cercare snapshot pubblici e condivisi disponibili digitando il testo nel campo Snapshot.
- Dimensioni: per i volumi EBS, è possibile specificare una dimensione di archiviazione.
- Volume Type (Tipo di volume): per i volumi EBS, selezionare un tipo di volume. Per ulteriori informazioni, consulta Tipi di volumi di Amazon EBS nella Guida per l'utente di Amazon EBS.
- IOPS: se hai selezionato il tipo di volume io1, io2 o gp3, puoi inserire il numero di I/O operazioni al secondo (IOPS) che il volume può supportare. Obbligatorio per i volumi io1, io2 e gp3. Non supportato per i volumi gp2, st1, sc1 o standard. Se si omette questo parametro per il modello di avvio, è necessario specificare un valore quando si avvia un'istanza dal modello di avvio.
- Delete on termination (Elimina alla terminazione): per i volumi Amazon EBS, scegliere Yes (Sì) per eliminare il volume quando l'istanza viene terminata oppure No per conservare il volume. Per ulteriori informazioni, consulta Conservare i dati quando un'istanza viene terminata.
- Encrypted (Crittografato): se il tipo di istanza supporta la crittografia EBS, scegliere Yes (Sì) per abilitare la crittografia per il volume. Se hai abilitato la crittografia per impostazione predefinita in questa regione allora la crittografia è abilitata. Per ulteriori informazioni, consulta Crittografia Amazon EBS nella Guida per l'utente di Amazon EBS.

- KMS key (Chiave KMS): se si è selezionato Yes (Sì) per Encrypted (Crittografato), allora è necessario selezionare una chiave gestita dal cliente da utilizzare per crittografare il volume. Se hai abilitato la crittografia per impostazione predefinita in questa Regione, viene selezionata automaticamente la chiave gestita dal cliente predefinita. È possibile selezionare una chiave diversa o specificare l'ARN di qualsiasi chiave gestita dal cliente creata.
- Throughput: se hai selezionato il tipo di volume `gp3`, puoi inserire il throughput supportato dal volume, in MiB/s.
- Velocità di inizializzazione del volume: se hai selezionato uno snapshot, puoi facoltativamente specificare la velocità di inizializzazione del volume, in MiB/s, alla quale i blocchi di snapshot devono essere scaricati da Amazon S3 sul volume. Per ulteriori informazioni, consulta Use an Amazon EBS Provisioned Rate for Volume Initialization. Per utilizzare la velocità di inizializzazione predefinita o il ripristino rapido degli snapshot (se abilitato per lo snapshot selezionato), non specificare una velocità.
- File system: monta un FSx file system Amazon EFS o Amazon sull'istanza. Per ulteriori informazioni su come montare un file system Amazon EFS, consulta Utilizzo di Amazon EFS con le istanze Linux Amazon EC2. Per ulteriori informazioni sul montaggio di un FSx file system Amazon, consulta Utilizzo di Amazon FSx con istanze Amazon EC2

Dettagli avanzati

Per Advanced Details (Dettagli avanzati), espandi la sezione per visualizzare i campi e specifica eventuali parametri aggiuntivi per l'istanza.

- (Solo procedura guidata di avvio dell'istanza) Directory di aggiunta al dominio: seleziona la Directory Service directory (dominio) a cui viene aggiunta l'istanza dopo il lancio. Se si seleziona un dominio, è necessario selezionare un ruolo IAM con le autorizzazioni necessarie. Per ulteriori informazioni sull'aggiunta al dominio, consulta Aggiungere senza problemi un'istanza Amazon EC2 Linux alla directory Microsoft AD AWS gestita (istanze Linux) e Unire senza problemi un'istanza Amazon EC2 Windows alla directory gestita di AWS Microsoft AD (istanze Windows).
- Profilo dell'istanza IAM: Seleziona un profilo dell'istanza IAM da associare all'istanza. Questo è un container per un ruolo IAM. Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.
- Hostname type (Tipo di nome host): selezionare se il nome host del sistema operativo guest dell'istanza deve includere il nome della risorsa o il nome IP. Per ulteriori informazioni, consulta Hostname e domini delle istanze EC2.
- Nome host DNS: determina se le interrogazioni DNS sul nome della risorsa o sul nome IP (a seconda del tipo di nome host selezionato) risponderanno con l' IPv4 indirizzo (record A), l' IPv6

indirizzo (record AAAA) o entrambi. Per ulteriori informazioni, consulta Hostname e domini delle istanze EC2.

- Ripristino automatico dell'istanza: se abilitato, ripristina l'istanza se le verifiche dello stato del sistema hanno esito negativo. Questa impostazione è abilitata per impostazione predefinita all'avvio per i tipi di istanza supportati. Per ulteriori informazioni, consulta Configurare il ripristino automatico semplificato su un'istanza Amazon EC2.
- Shutdown behavior (Comportamento di arresto): selezionare se l'istanza deve interrompersi o terminare all'arresto. Per ulteriori informazioni, consulta Modificare il comportamento di arresto avviato dall'istanza.
- Stop - Hibernate behavior (Comportamento di interruzione/ibernazione): per abilitare l'ibernazione, scegliere Enable (Abilita). Questa opzione è disponibile solo se l'istanza soddisfa i prerequisiti di ibernazione. Per ulteriori informazioni, consulta Metti in ibernazione la tua istanza Amazon EC2.
- Termination protection (Protezione da terminazione): per impedire la terminazione accidentale, scegliere Enable (Abilita). Per ulteriori informazioni, consulta Modifica della protezione da terminazione dell'istanza.
- Protezione da arresto: per evitare l'arresto accidentale, scegli Enable (Abilita). Per ulteriori informazioni, consulta Abilitare la protezione da arresto.
- CloudWatch Monitoraggio dettagliato: scegli Abilita per attivare il monitoraggio dettagliato della tua istanza tramite Amazon CloudWatch. Si applicano costi aggiuntivi. Per ulteriori informazioni, consulta Monitora le tue istanze utilizzando CloudWatch.
- Credit specification (Specifica credito): scegliere Unlimited (Illimitato) per consentire l'espansione delle applicazioni oltre la baseline per tutto il periodo necessario. Questo campo è valido solo per le istanze T. Potrebbero essere applicati costi aggiuntivi. Per ulteriori informazioni, consulta Istanze a prestazioni espandibili.
- Nome del gruppo di posizionamento: specifica un gruppo di posizionamento in cui avviare l'istanza. È possibile selezionare un gruppo di collocamento esistente o crearne uno nuovo. Non tutti i tipi di istanza supportano l'avvio di una istanza in un gruppo di collocazione. Per ulteriori informazioni, consulta Gruppi di collocamento per le tue istanze Amazon EC2.
- EBS-optimized instance (Istanza ottimizzata per EBS): un'istanza ottimizzata per Amazon EBS usa uno stack di configurazione ottimizzato e offre una capacità aggiuntiva dedicata per l'I/O Amazon EBS. Se il tipo di istanza supporta questa caratteristica, scegliere Enable (Abilita) per abilitarla. Si applicano costi aggiuntivi. Per ulteriori informazioni, consulta the section called "Ottimizzazione EBS".

- Configurazione della larghezza di banda dell'istanza: puoi aumentare la larghezza di banda della rete o la larghezza di banda EBS. Solo per i tipi di istanza supportati. Per ulteriori informazioni, consulta Configurazione della ponderazione della larghezza di banda dell'istanza EC2.
- Opzione di acquisto: scegliere Istanze spot per richiedere le istanze spot al prezzo spot, limitato al prezzo on demand, e scegliere Personalizza per modificare le impostazioni dell'istanza spot di default. Puoi impostare il prezzo massimo (sconsigliato) e modificare il tipo di richiesta, la durata della richiesta e il comportamento di interruzione. Se non richiedi un'istanza Spot, Amazon EC2 avvia un'istanza On-Demand per impostazione predefinita. Per ulteriori informazioni, consulta Gestione delle istanze spot.
- Capacity Reservation (Prenotazione di capacità): specificare se avviare l'istanza in una qualsiasi prenotazione della capacità aperta (Open), una prenotazione della capacità specificare (Target by ID) o in un gruppo di prenotazione della capacità (Target by group). Per specificare che non deve essere utilizzata una prenotazione della capacità, selezionare None (Nessuno). Per ulteriori informazioni, consulta Avvio di istanze in una Prenotazione della capacità esistente.
- Tenancy: seleziona se eseguire l'istanza su hardware condiviso (Shared [Condiviso]), isolato, hardware dedicato (Dedicated [Dedicato]) o su un Host dedicato (Dedicated host [Host dedicato]). Se decidi di avviare l'istanza su un Host dedicato, puoi specificare se avviare l'istanza in un gruppo di risorse host o usare uno specifico Host dedicato come target. Potrebbero essere applicati costi aggiuntivi. Per ulteriori informazioni, consultare Istanze dedicate Amazon EC2 e Host dedicati di Amazon EC2.
- ID disco RAM: (Valido solo per paravirtual (PV) AMIs) Seleziona un disco RAM per l'istanza. Se avete selezionato un kernel, potrebbe essere necessario selezionare un disco RAM specifico con i driver che lo supportano.
- ID kernel: (Valido solo per paravirtual (PV) AMIs) Seleziona un kernel per l'istanza.
- Nitro Enclave: consente di creare ambienti di esecuzione isolati, chiamati enclavi, da istanze Amazon. EC2 Seleziona Abilita per abilitare l'istanza per Nitro Enclaves. AWS Per ulteriori informazioni, consulta Che cos'è AWS Nitro Enclaves? nella Guida per l'utente di AWS Nitro Enclaves.
- Configurazioni licenza: è possibile avviare istanze con la configurazione di licenza specificata per tenere traccia dell'utilizzo della licenza. Per ulteriori informazioni, consulta Creazione di una configurazione di licenza nella Guida per l'utente di AWS License Manager.
- Specificare le opzioni della CPU: nella procedura guidata di avvio dell'istanza, questo campo è visibile solo se il tipo di istanza selezionato supporta la specifica delle opzioni della CPU. Scegli Specificare le opzioni della CPU per specificare un numero personalizzato di v CPUs durante

l'avvio. Imposta il numero di thread per core e di core CPU. Per ulteriori informazioni, consulta Opzioni della CPU per le istanze Amazon EC2.

- Metadati accessibili: puoi abilitare o disabilitare l'accesso al Servizio di metadati dell'istanza (IMDS). Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.
- IPv6 Endpoint di metadati: è possibile consentire all'istanza di utilizzare l' IPv6 indirizzo `[fd00:ec2::254]` IMDS per recuperare i metadati dell'istanza. Questa opzione è disponibile solo se si avviano istanze basate su Nitro in una sottorete supportata (dual stack o solo IPv6). IPv6 Per ulteriori informazioni su come recuperare i metadati dell'istanza, consulta Accesso ai metadati dell'istanza per un'istanza EC2.
- Versione dei metadati: se abiliti l'accesso a IMDS, puoi scegliere di richiedere l'utilizzo di Servizio di metadati dell'istanza Versione 2 quando si richiedono i metadati dell'istanza. Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.
- Limite di hop della risposta dei metadati: se abiliti l'accesso a IMDS, puoi impostare il numero consentito di hop di rete per il token dei metadati. Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.
- Allow tags in metadata (Consenti tag nei metadati): se selezioni Enable (Abilita), l'istanza consentirà l'accesso a tutti i suoi tag dai metadati. Se non viene specificato alcun valore, l'accesso ai tag nei metadati dell'istanza non è permesso di default. Per ulteriori informazioni, consulta Abilita l'accesso ai tag nei metadati dell'istanza.
- User data (Dati utente): è possibile specificare i dati utente per configurare un'istanza durante l'avvio o per eseguire uno script di configurazione. Per ulteriori informazioni sui dati utente per istanze Linux, consulta Esegui i comandi quando avvii un'istanza EC2 con l'input dei dati utente. Per ulteriori informazioni sui dati utente per istanze Windows, consulta In che modo Amazon EC2 gestisce i dati utente per le istanze Windows.

Riepilogo

Utilizzare il pannello Summary (Riepilogo) per specificare il numero di istanze da avviare , esaminare la configurazione dell'istanza e avviare le istanze.

- Number of instances (Numero di istanze): immettere il numero di istanze da avviare. Tutte le istanze verranno avviate con la stessa configurazione.

> **Tip**
>
> Per garantire avvii di istanza più veloci, suddividi le richieste di grandi dimensioni in batch più piccoli. Ad esempio, crea cinque richieste di avvio distinte per 100 istanze invece di un'unica richiesta di avvio per 500 istanze.

- (Facoltativo) Se specificate più di un'istanza, per assicurarvi di mantenere il numero corretto di istanze per gestire la domanda sulla vostra applicazione, potete scegliere di prendere in considerazione EC2 Auto Scaling per creare un modello di avvio e un gruppo di Auto Scaling. La funzionalità Auto Scaling dimensiona il numero di istanze nel gruppo in base alle specifiche. Per ulteriori informazioni, consulta la Amazon EC2 Auto Scaling User Guide.

> **Note**
>
> Se Amazon EC2 Auto Scaling contrassegna un'istanza che fa parte di un gruppo di Auto Scaling come non integra, l'istanza viene automaticamente pianificata per la sostituzione, viene interrotta e ne viene avviata un'altra e si perdono i dati sull'istanza originale. Un'istanza è contrassegnata come non integra se arresti o riavvii l'istanza o se un altro evento contrassegna l'istanza come non integra. Per ulteriori informazioni, consulta la sezione Health checks for Instances in an Auto Scaling Group nella Amazon Auto EC2 Scaling User Guide.

- Esaminare i dettagli dell'istanza e apportare eventuali modifiche necessarie. È possibile passare direttamente a una sezione scegliendo il relativo collegamento nel pannello Summary (Riepilogo).
- Quando si è pronti per avviare l'istanza, scegliere Launch instance (Avvia istanza).

Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console

È possibile avviare un'istanza Amazon EC2 tramite la procedura guidata di avvio dell'istanza nella console Amazon EC2. La procedura guidata fornisce valori predefiniti per i parametri di avvio, che è possibile accettare o modificare in base alle proprie esigenze. L'unico parametro non specificato è la coppia di chiavi. Se si accettano i valori di default, è possibile avviare un'istanza selezionando solo una coppia di chiavi.

> **Important**
>
> Vengono addebitati dei costi per l'istanza mentre è nello stato `running`, anche se rimane inattiva. Tuttavia, se si è idonei per il piano gratuito, potrebbero non essere emessi addebiti. Per ulteriori informazioni, consulta Monitorare l'utilizzo del piano gratuito per Amazon EC2.

Per la descrizione di ciascun parametro della procedura guidata di avvio dell'istanza, consultare Riferimento per i parametri di configurazione delle EC2 istanze Amazon.

Argomenti

- Avvio rapido di un'istanza
- Avvio di un'istanza utilizzando parametri definiti

Avvio rapido di un'istanza

Per configurare rapidamente un'istanza a scopo di test, completare la seguente procedura per avviare rapidamente un'istanza. Verrà selezionato il sistema operativo e la coppia di chiavi e accettati i valori di default. Ad eccezione della coppia di chiavi, la procedura guidata di avvio istanza fornisce i valori di default per tutti i parametri. È possibile accettare uno o tutti i valori predefiniti o configurare un'istanza specificando i propri valori per ciascun parametro.

Per la descrizione di ciascun parametro della procedura guidata di avvio dell'istanza, consultare Riferimento per i parametri di configurazione delle EC2 istanze Amazon.

Avvio rapido di un'istanza tramite la procedura guidata di avvio dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore dello schermo, viene visualizzata la AWS regione corrente (ad esempio, Stati Uniti orientali (Ohio)). Se necessario, selezionare una regione diversa in cui avviare l'istanza.
3. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).
4. (Facoltativo) in Name and tags (Nome e tag), per Name (Nome), inserire un nome descrittivo per la propria istanza.
5. In Application and OS Images (Amazon machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), scegli Quick Start (Avvio rapido), quindi scegli il sistema operativo (SO) per la tua istanza.

6. In Key pair (login) (Coppia di chiavi (login), per Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente o creane una nuova.
7. Nel pannello Summary (Riepilogo), scegliere Launch instance (Avvia istanza).

Avvio di un'istanza utilizzando parametri definiti

Se stai lanciando un'istanza da utilizzare in produzione, dovrai configurare l'istanza in base alle tue esigenze. Per la descrizione di ciascun parametro della procedura guidata di avvio dell'istanza, consultare Riferimento per i parametri di configurazione delle EC2 istanze Amazon.

Avvio di un'istanza tramite la definizione di tutti i parametri di lancio tramite la procedura guidata di avvio dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore dello schermo, viene visualizzata la AWS regione corrente (ad esempio, Stati Uniti orientali (Ohio)). Se necessario, selezionare una regione diversa in cui avviare l'istanza.
3. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).
4. (Facoltativo) In Nome e tag, in Nome, specifica un nome descrittivo per l'istanza in modo da poterne tenere traccia.

   Il nome dell'istanza è un tag, dove la chiave è Name (Nome) e il valore è il nome specificato.
5. In Immagini di applicazioni e sistema operativo (Amazon Machine Image), scegli il sistema operativo (SO) per la tua istanza, quindi seleziona un'AMI.

   Un'AMI è un modello che contiene il sistema operativo e il software necessari per avviare l'istanza.
6. In Tipo di istanza, seleziona un tipo di istanza.

   Il tipo di istanza determina la configurazione hardware (capacità in termini di CPU, memoria, storage e rete) e le dimensioni del computer host utilizzato per l'istanza.

   Se hai dei dubbi sul tipo di istanza da scegliere, puoi effettuare le seguenti operazioni:

   - Scegli Confronta tipi di istanze per confrontare diversi tipi di istanza in base ai seguenti attributi: numero di vCPUs, architettura, quantità di memoria (GiB), quantità di spazio di archiviazione (GB), tipo di archiviazione e prestazioni di rete.

- Scegli Fatti consigliare per ottenere indicazioni e suggerimenti per i tipi di istanza dal selettore dei tipi di istanza EC2. Per ulteriori informazioni, consulta Ottieni consigli dallo strumento di ricerca del tipo di istanza EC2.

> **Note**
>
> A seconda di quando hai creato l'account, potresti essere in grado di utilizzare i tipi di istanza gratuitamente nell'ambito del Piano gratuito. Questi tipi di istanze sono etichettati come Idoneo per il Piano gratuito.
> Se l'hai creato Account AWS prima del 15 luglio 2025 e ha meno di 12 mesi, puoi utilizzare Amazon EC2 nel piano gratuito selezionando il tipo di istanza t2.micro o il tipo di istanza t3.micro nelle regioni in cui t2.micro non è disponibile. Tieni presente che quando avvii un'istanza t3.micro, l'impostazione predefinita è la modalità Illimitata, che potrebbe comportare costi aggiuntivi in base all'utilizzo della CPU.
> Se hai creato la tua il Account AWS 15 luglio 2025 o successivamente, puoi utilizzare i tipi di istanza t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large e m7i-flex.large per 6 mesi o fino all'esaurimento dei crediti.
> Per ulteriori informazioni, consulta Vantaggi del piano gratuito prima e dopo il 15 luglio 2025.

7. In Key pair (login) (Coppia di chiavi (login), per Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente o creane una nuova. Se non hai bisogno di una coppia di chiavi per connetterti alla tua istanza, puoi scegliere Procedi senza una coppia di chiavi (scelta non consigliata).
8. In Impostazioni di rete puoi mantenere le impostazioni predefinite se stai avviando un'istanza di prova. Se stai lanciando un'istanza di produzione, è consigliabile controllare il traffico in entrata e in uscita dall'istanza utilizzando le impostazioni di rete e i gruppi di sicurezza da te definiti.
9. In Configura archiviazione puoi mantenere le impostazioni predefinite o specificare uno spazio di archiviazione aggiuntivo. L'AMI selezionata include uno o più volumi di archiviazione, compreso il volume dispositivo root. È possibile specificare altri volumi da collegare all'istanza.

   È possibile utilizzare la vista Semplice o Avanzato. Con la vista Simple (Semplice), si specificano la dimensione e il tipo di volume. Per specificare tutti i parametri del volume, scegli la vista Advanced (Avanzata) (nella parte superiore destra della scheda).
10. Per Dettagli avanzati, espandi la sezione per visualizzare i campi e specifica eventuali parametri aggiuntivi per l'istanza.

11. Nel pannello Riepilogo puoi eseguire le seguenti operazioni:

    a. Specificare il numero di istanze da avviare.

    b. Controllare la configurazione dell'istanza e accedere direttamente a una sezione scegliendo il collegamento.

    c. Quando si è pronti per avviare l'istanza, scegliere Launch instance (Avvia istanza).

    Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio dell'istanza Amazon EC2.

12. (Facoltativo) È possibile creare un avviso di fatturazione per l'istanza. Nella schermata di conferma, in Next Steps (Fasi successive), scegli Create billing alerts (Crea avvisi di fatturazione) e segui le istruzioni. Gli avvisi di fatturazione possono essere creati anche dopo l'avvio dell'istanza. Per ulteriori informazioni, consulta Creazione di un allarme di fatturazione per monitorare gli AWS addebiti stimati nella Amazon CloudWatch User Guide.

Avvio di istanze EC2 usando un modello di avvio

Un modello di avvio di Amazon EC2 archivia i parametri di avvio di istanze in modo da non doverli specificare ogni volta che si avvia un'istanza.

Diversi servizi di avvio di istanze possono opzionalmente utilizzare modelli di avvio per avviare le istanze, mentre per altri servizi, come il parco istanze EC2, le istanze non possono essere avviate a meno che non venga utilizzato un modello di avvio. Questo argomento descrive come utilizzare un modello di avvio quando si avvia un'istanza utilizzando la procedura guidata di avvio dell'istanza EC2, Amazon EC2 Auto Scaling, parco istanze EC2 e parco istanze spot.

Per ulteriori informazioni sui modelli di avvio, fra cui come creare un modello di avvio, consulta Archivia i parametri di avvio dell'istanza nei modelli di avvio di Amazon EC2.

Argomenti

- Avvia un'istanza Amazon EC2 usando un modello di avvio
- Avvia istanze in un gruppo Amazon EC2 Auto Scaling utilizzando un modello di avvio
- Avvia un parco istanze EC2 usando un modello di avvio
- Avvia un parco istanze spot usando un modello di avvio

Avvia un'istanza Amazon EC2 usando un modello di avvio

È possibile utilizzare i parametri contenuti in un modello di avvio per avviare un'istanza Amazon EC2. Dopo aver selezionato il modello di avvio, ma prima di avviare l'istanza, puoi modificare i parametri di avvio.

Alle istanze che vengono avviate tramite un modello di avvio vengono automaticamente assegnati due tag con le chiavi `aws:ec2launchtemplate:id` e `aws:ec2launchtemplate:version`. Non è possibile rimuovere o modificare questi tag.

Console

Per avviare un'istanza usando un modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Utilizzare una delle seguenti opzioni per selezionare il modello di avvio:
   - Dalla dashboard della console Amazon EC2, scegli la freccia in basso accanto ad Avvia istanza, scegli Avvia istanza dal modello, quindi per Modello di origine, seleziona un modello di avvio.
   - Nel riquadro di navigazione, scegli Modelli di avvio, seleziona il modello di avvio e scegli Operazioni, Avvia istanza dal modello.
3. Per Source template version (Versione modello origine), selezionare la versione del modello di avvio da utilizzare.
4. (Facoltativo) Puoi modificare i valori per qualsiasi parametro di avvio. Se un valore non viene modificato, viene utilizzato il valore definito dal modello di avvio. Se non è stato specificato alcun valore nel modello di avvio, viene utilizzato il valore predefinito per il parametro.
5. Nel pannello Riepilogo, per Numero di istanze, specifica il numero di istanze da avviare.
6. Scegliere Launch Instance (Avvia istanza).

   Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio dell'istanza Amazon EC2.

AWS CLI

Per avviare un'istanza da un modello di avvio

- Utilizzare il comando run-instances e specificare il parametro `--launch-template`. Facoltativamente, specificare la versione del modello di avvio da utilizzare. Se non specifichi la versione, viene utilizzata la versione predefinita.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- Per sovrascrivere un parametro del modello di avvio, specificare il parametro nel comando run-instances. L'esempio seguente sovrascrive il tipo di istanza specificato nel modello di avvio (se presente).

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --instance-type t2.small
```

- Se specifichi un parametro nidificato che fa parte di una struttura complessa, l'istanza viene avviata utilizzando la struttura complessa come specificato nel modello di avvio, oltre a eventuali parametri nidificati aggiuntivi specificati.

  Nell'esempio seguente, l'istanza viene avviata con il tag *Owner*=*TeamA*, oltre a qualsiasi altro tag specificato nel modello di avvio. Se il modello di avvio ha un tag esistente con una chiave di *Owner*, il valore viene sostituito con *TeamA*.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
```

  Nell'esempio seguente, l'istanza viene avviata con un volume con il nome del dispositivo */dev/xvdb*, oltre a qualsiasi altra mappatura dei dispositivi a blocchi specificata nel modello di avvio. Se il modello di avvio ha un volume esistente definito per */dev/xvdb*, i suoi valori vengono sostituiti con i valori specificati.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --block-device-mappings "DeviceName=/dev/
xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
```

Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio dell'istanza Amazon EC2.

PowerShell

Per avviare un'istanza da un modello di avvio utilizzando AWS Strumenti per PowerShell

- Utilizza il comando New-EC2Instance e specifica il parametro `-LaunchTemplate`. Facoltativamente, specificare la versione del modello di avvio da utilizzare. Se non specifichi la versione, viene utilizzata la versione predefinita.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Per sovrascrivere un parametro del modello di avvio, specificate il parametro nel New-EC2Instance comando. L'esempio seguente sovrascrive il tipo di istanza specificato nel modello di avvio (se presente).

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Se specifichi un parametro nidificato che fa parte di una struttura complessa, l'istanza viene avviata utilizzando la struttura complessa come specificato nel modello di avvio, oltre a eventuali parametri nidificati aggiuntivi specificati.

Nell'esempio seguente, l'istanza viene avviata con il tag *Owner*=*TeamA*, oltre a qualsiasi altro tag specificato nel modello di avvio. Se il modello di avvio ha un tag esistente con una chiave di *Owner*, il valore viene sostituito con *TeamA*.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
        }
) `
    -TagSpecification (
        New-Object -TypeName Amazon.EC2.Model.TagSpecification -Property @{
            ResourceType = 'instance';
            Tags         = @(
                @{key = "Owner"; value = "TeamA" },
                @{key = "Department"; value = "Operations" }
            )
        }
)
```

Nell'esempio seguente, l'istanza viene avviata con un volume con il nome del dispositivo */dev/xvdb*, oltre a qualsiasi altra mappatura dei dispositivi a blocchi specificata nel modello di avvio. Se il modello di avvio ha un volume esistente definito per */dev/xvdb*, i suoi valori vengono sostituiti con i valori specificati.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
) `
    -BlockDeviceMapping  (
        New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping -Property @{
```

```
            DeviceName = '/dev/xvdb';
            EBS        = (
                New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property @{
                    VolumeSize = 25;
                    VolumeType = 'gp3'
                }
            )
        }
)
```

Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio dell'istanza Amazon EC2.

Avvia istanze in un gruppo Amazon EC2 Auto Scaling utilizzando un modello di avvio

È possibile creare un gruppo Auto Scaling e specificare un modello di avvio da utilizzare per il gruppo. Quando Amazon EC2 Auto Scaling avvia le istanze nel gruppo Auto Scaling, utilizza i parametri di lancio definiti nel modello di avvio associato.

Prima di poter creare un gruppo Auto Scaling utilizzando un modello di avvio, devi prima creare un modello di avvio che includa i parametri necessari per avviare un'istanza in un gruppo Auto Scaling. Alcuni parametri sono obbligatori, come l'ID dell'AMI, e alcuni parametri non sono disponibili per l'uso con un gruppo Auto Scaling. La console fornisce indicazioni per aiutarti a creare un modello da utilizzare con Amazon EC2 Auto Scaling.

Per creare un gruppo Auto Scaling con un modello di avvio usando la console

- Per le istruzioni, consulta Creare un gruppo Auto Scaling utilizzando un modello di avvio nella Guida per l'utente di Amazon EC2 Auto Scaling.

Per creare o aggiornare un gruppo Auto Scaling con un modello di avvio utilizzando AWS CLI

- Utilizzare il comando create-auto-scaling-group o update-auto-scaling-group e specificare il parametro `--launch-template`.

Per ulteriori informazioni, consulta i seguenti argomenti nella Guida per l'utente di Amazon EC2 Auto Scaling:

- Crea un modello di avvio per un gruppo Auto Scaling
- Crea un modello di avvio utilizzando le impostazioni avanzate
- Esempi per la creazione e la gestione di modelli di avvio con l' AWS Command Line Interface (AWS CLI): fornisce esempi che mostrano come creare modelli di avvio con varie combinazioni di parametri.
- Creare gruppi Auto Scaling utilizzando modelli di avvio
- Aggiornamento di un gruppo Auto Scaling

Avvia un parco istanze EC2 usando un modello di avvio

Un modello di avvio è un requisito per creare una richiesta di parco istanze EC2. Quando Amazon EC2 soddisfa la richiesta Parco istanze EC2, utilizza i parametri di lancio definiti nel modello di avvio associato. È possibile sovrascrivere alcuni dei parametri specificati nel modello di avvio. Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.

Per creare una flotta EC2 con un modello di lancio utilizzando AWS CLI

- Utilizzare il comando create-fleet. Utilizzare il parametro `--launch-template-configs` per specificare il modello di avvio ed eventuali sostituzioni per il modello di avvio.

Avvia un parco istanze spot usando un modello di avvio

> **Important**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Un modello di avvio è facoltativo quando si crea una richiesta di parco istanze spot. Se non utilizzi un modello di avvio, puoi specificare manualmente i parametri di avvio. Se utilizzi un modello di avvio, quando Amazon EC2 soddisfa la richiesta di parco istanze spot, utilizza i parametri di avvio definiti nel modello di avvio associato. È possibile sovrascrivere alcuni dei parametri specificati nel modello di avvio. Per ulteriori informazioni, consulta Creazione di un parco istanze Spot.

Per creare una richiesta di parco istanze spot usando un modello di avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Selezionare Request Spot Instances (Richiedi istanze Spot).
4. In Launch parameters (Parametri di avvio), scegli Use a launch template (Utilizza un modello di avvio).
5. Per Modello di avvio, scegli un modello di avvio, quindi, dal campo a destra scegli la versione del modello di avvio.
6. Configura il parco istanze spot selezionando diverse opzioni su questa schermata. Per ulteriori informazioni su queste opzioni, consulta Crea una richiesta di parco istanze spot utilizzando parametri definiti.
7. Quando è tutto pronto per la creazione del parco istanze spot, scegli Launch (Avvia).

Per creare una richiesta di parco istanze spot usando un modello di avvio

- Utilizzare il comando request-spot-fleet. Utilizzare il parametro `LaunchTemplateConfigs` per specificare il modello di avvio ed eventuali sostituzioni per il modello di avvio.

Avvia un'istanza EC2 usando i dettagli da un'istanza esistente

Nella console Amazon EC2 è disponibile l'opzione Launch more like this (Avvia altre come questa) che ti consente di utilizzare l'istanza corrente come base per l'avvio di altre istanze. Questa opzione popola automaticamente la procedura guidata di avvio dell'istanza Amazon EC2 con specifici dettagli di configurazione derivati dall'istanza selezionata.

Considerazioni

- Non cloniamo le istanze, ma replichiamo solamente alcuni dei dettagli di configurazione. Per creare una copia dell'istanza, devi innanzitutto creare un'AMI da tale istanza, quindi avviare altre istanze da tale AMI. Crea un modello di avvio per assicurarti di avviare le istanze utilizzando gli stessi dettagli di avvio.
- L'istanza attuale deve essere nello stato `running`.

Dettagli copiati

I seguenti dettagli di configurazione vengono copiati dall'istanza selezionata alla procedura guidata di avvio dell'istanza:

- ID AMI
- Tipo di istanza
- Zona di disponibilità o VPC e sottorete in cui si trova l'istanza selezionata
- Indirizzo IPv4 pubblico. Se l'istanza selezionata attualmente dispone di un indirizzo IPv4 pubblico, la nuova istanza riceve un indirizzo IPv4 pubblico, indipendentemente dall'impostazione di default dell'indirizzo IPv4 pubblico dell'istanza selezionata. Per ulteriori informazioni sugli indirizzi IPv4 pubblici, consulta Indirizzi IPv4 pubblici.
- Gruppo di collocamento, se applicabile
- Ruolo IAM associato all'istanza, se applicabile
- Impostazione relativa al comportamento dell'arresto (arresto o interruzione)
- Impostazione relativa alla protezione per l'interruzione (true o false)
- CloudWatch monitoraggio (abilitato o disabilitato)
- EBS-optimization impostazione Amazon (vera o falsa)
- Impostazione relativa alla tenancy, in caso di avvio in un VPC (condiviso o dedicato)
- ID kernel e ID disco RAM, se applicabili
- Dati utente, se specificati
- Tag associati all'istanza, se applicabili
- Gruppi di sicurezza associati all'istanza
- [Istanze Windows] Informazioni sull'associazione. Se l'istanza selezionata è associata a un file di configurazione, tale file viene automaticamente associato alla nuova istanza. Se il file di configurazione include una configurazione di aggiunta al dominio, la nuova istanza viene aggiunta a tale dominio. Per ulteriori informazioni sull'adesione a un dominio, consulta Unire senza problemi un'istanza Windows EC2 alla tua Active Directory Microsoft AD AWS gestita nella Guida all'Servizio di directory AWS amministrazione.

Dettagli non copiati

I seguenti dettagli di configurazione non vengono copiati dall'istanza selezionata. La procedura guidata applica invece le impostazioni o il comportamento predefiniti:

- Numero di interfacce di rete: il valore predefinito prevede un'interfaccia di rete, ovvero l'interfaccia di rete primaria (eth0).
- Archiviazione: la configurazione di archiviazione di default è determinata dall'AMI e dal tipo di istanza.

Per avviare più istanze come un'istanza esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona un'istanza, quindi scegli Operazioni, Immagini e modelli, Avvia altre come questa.
4. Si apre la procedura guidata dell'istanza di avvio. Puoi apportare le modifiche necessarie alla configurazione dell'istanza selezionando diverse opzioni in questa schermata.

   Quando sei pronto ad avviare l'istanza, scegli Launch instance (Avvia istanza).
5. Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio dell'istanza Amazon EC2.

Avvia un'istanza Amazon EC2 da un'AMI Marketplace AWS

Puoi abbonarti a un' Marketplace AWS AMI e avviare un'istanza da essa utilizzando la console Amazon EC2 o uno strumento a riga di comando. Per ulteriori informazioni su Marketplace AWS AMIs, consultaAMI a pagamento in Marketplace AWS per istanze Amazon EC2.

Per annullare l'abbonamento all'AMI dopo il lancio, devi prima terminare tutte le istanze che sono state lanciate dall'AMI. Per ulteriori informazioni, consulta Gestisci il tuo Marketplace AWS sottoscrizioni.

Per avviare un'istanza da un' Marketplace AWS AMI utilizzando la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).
3. (Facoltativo) in Name and tags (Nome e tag), per Name (Nome), inserire un nome descrittivo per la propria istanza.
4. In Immagini dell'applicazione e del sistema operativo (Amazon Machine Image), scegli Sfoglia altro AMIs, quindi scegli la Marketplace AWS AMIsscheda. Individua un'AMI idonea sfogliando le

categorie oppure utilizzando la funzionalità di ricerca. Scegli Select (Seleziona) per scegliere un prodotto.

5. Viene visualizzata una finestra di dialogo con la panoramica del prodotto selezionato. È possibile visualizzare le informazioni sui prezzi, nonché alte informazioni specificate dal fornitore. Quando sei pronto, scegli Abbonati e avvia. In questo modo il tuo abbonamento inizierà immediatamente. Mentre l'abbonamento è in corso, puoi configurare l'istanza continuando con i passaggi di questa procedura. Se sono presenti problemi con i dettagli della carta di credito, verrà richiesto di aggiornare i dettagli dell'account.

   > **Note**
   >
   > Non è previsto alcun addebito per l'utilizzo del prodotto finché non viene avviata un'istanza mediante l'AMI. Presta attenzione ai prezzi per ogni tipo di istanza supportata quando selezioni un tipo di istanza. Al prodotto potrebbero essere applicate anche tasse aggiuntive.

6. Per Instance type (Tipo di istanza), seleziona un tipo di istanza. Il tipo di istanza definisce la configurazione hardware e le dimensioni dell'istanza da avviare.
7. In Key pair (login) (Coppia di chiavi (login), per Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente o creane una nuova.
8. In Impostazioni di rete, per Firewall (gruppi di sicurezza) prendi nota del nuovo gruppo di sicurezza creato in base alle specifiche definite dal fornitore per il prodotto. Il gruppo di sicurezza potrebbe includere regole che consentono l'accesso a tutti IPv4 gli indirizzi (`0.0.0.0/0`) su SSH (porta 22) su Linux o RDP (porta 3389) su Windows. Consigliamo di modificare queste regole per consentire solo a un indirizzo specifico o a uno specifico intervallo di indirizzi di accedere all'istanza tramite queste porte.
9. Puoi utilizzare gli altri campi sullo schermo per configurare l'istanza e aggiungere storage e tag. Per ulteriori informazioni sulle diverse opzioni configurabili, consulta Riferimento per i parametri di configurazione delle EC2 istanze Amazon.
10. Nel pannello Summary (Riepilogo), in Software Image (AMI) (Immagine software [AMI]), verifica dettagli dell'AMI da cui si sta avviando l'istanza. Verifica anche gli altri dettagli di configurazione che hai specificato. Quando si è pronti per avviare l'istanza, scegliere Launch instance (Avvia istanza).
11. A seconda del prodotto a cui è stata eseguita la sottoscrizione, l'avvio dell'istanza può richiedere alcuni minuti. Se sono presenti problemi con i dettagli della carta di credito, verrà richiesto di

aggiornare i dettagli dell'account. Quando viene visualizzata la pagina di conferma dell'avvio, scegli View all instances (Visualizza tutte le istanze) per passare alla pagina Instances (Istanze).

> **Note**
>
> Verrà addebitato il prezzo della sottoscrizione a condizione che l'istanza sia nello stato `running`, anche se inattiva. Se l'istanza viene arrestata, potrebbe continuare a venire addebitato il costo dell'archiviazione.

12. Quando lo stato dell'istanza è `running`, sarà possibile connettersi a tale istanza. A tale scopo, seleziona l'istanza nell'elenco, scegli Connect (Connetti), quindi scegli un'opzione di connessione. Per ulteriori informazioni sulla connessione all'istanza, consulta Connettiti all'istanza EC2.

> **Important**
>
> Controlla attentamente le istruzioni del fornitore relative all'utilizzo perché potrebbe essere necessario utilizzare un nome utente specifico per connettersi all'istanza. Per ulteriori informazioni sull'accesso ai dettagli della sottoscrizione, consulta Gestisci il tuo Marketplace AWS sottoscrizioni.

13. Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio dell'istanza Amazon EC2.

Per avviare un'istanza da un' Marketplace AWS AMI utilizzando uno strumento da riga di comando

Per avviare istanze da Marketplace AWS prodotti utilizzando uno strumento da riga di comando, assicurati innanzitutto di essere abbonato al prodotto. Puoi quindi avviare un'istanza con l'ID AMI del prodotto utilizzando i seguenti metodi:

Metodo	Documentazione
AWS CLI	Utilizza il comando run-instances o consulta l'articolo Launch your instance nella Guida per l'utente di AWS Command Line Interface .

Metodo	Documentazione
AWS Tools for Windows PowerShell	Usa il New-EC2Instancecomando o consulta il seguente argomento per ulteriori informazioni: Avvio di un'istanza Amazon EC2 tramite Windows PowerShell
API della query	Usa la RunInstancesrichiesta.

Connettiti all'istanza EC2

La tua istanza Amazon EC2 è un server virtuale in Cloud AWS. Per accedere alla tua istanza, devi stabilire una connessione all'istanza. La modalità di connessione all'istanza dipende dal sistema operativo dell'istanza e dal sistema operativo del computer utilizzato per connettersi all'istanza. Nella tabella seguente, vengono descritti in dettaglio i requisiti per ciascun metodo di connessione.

Opzione di connessione	Sistema operativo dell'istanza.	Regola del traffico in entrata	autorizzazioni IAM	Ruolo del profilo dell'istanza	Software sull'istanza	Software sul sistema di connessione	Coppia di chiavi
Client SSH	Linux	Sì	No	No	No	Sì	Sì
EC2 Instance Connect	Linux	Sì	Sì	No	Sì [1]	No	No
PuTTY	Linux	Sì	No	No	No	Sì	Sì
Client RDP	Windows	Sì	No	No	No	Sì	Sì [2]
Fleet Manager	Windows	No	Sì	Sì	Sì [1]	No	Sì

Opzione di connessione	Sistema operativo dell'istanza.	Regola del traffico in entrata	autorizzazioni IAM	Ruolo del profilo dell'istanza	Software sull'istanza	Software sul sistema di connessione	Coppia di chiavi
Session Manager	Linux, Windows	No	Sì	Sì	Sì [1]	No	No
Endpoint EC2 Instance Connect	Linux, Windows	Sì	Sì	No	No	No	No [3]

[1] Il software richiesto è preinstallato solo su alcune AMI. Puoi installare manualmente il software richiesto, se necessario, sui sistemi operativi supportati.

[2] La coppia di chiavi è obbligatoria solo se si utilizza la password generata casualmente per l'account utente dell'amministratore locale.

[3] È necessaria una coppia di chiavi se utilizzi il metodo di connessione SSH.

Per ulteriori informazioni, consulta la documentazione relativa all'opzione di connessione che intendi usare.

Opzioni di connessione

- Connessione all'istanza Linux tramite un client SSH
- Connessione a un'istanza Linux tramite PuTTY
- Connettiti alla tua istanza Windows utilizzando un client RDP
- Connessione a un'istanza Windows utilizzando Fleet Manager
- Connessione tramite Session Manager
- Connettiti tramite un IP pubblico ed EC2 Instance Connect
- Connessione usando un IP privato e l'endpoint EC2 Instance Connect

Prerequisiti generali per la connessione

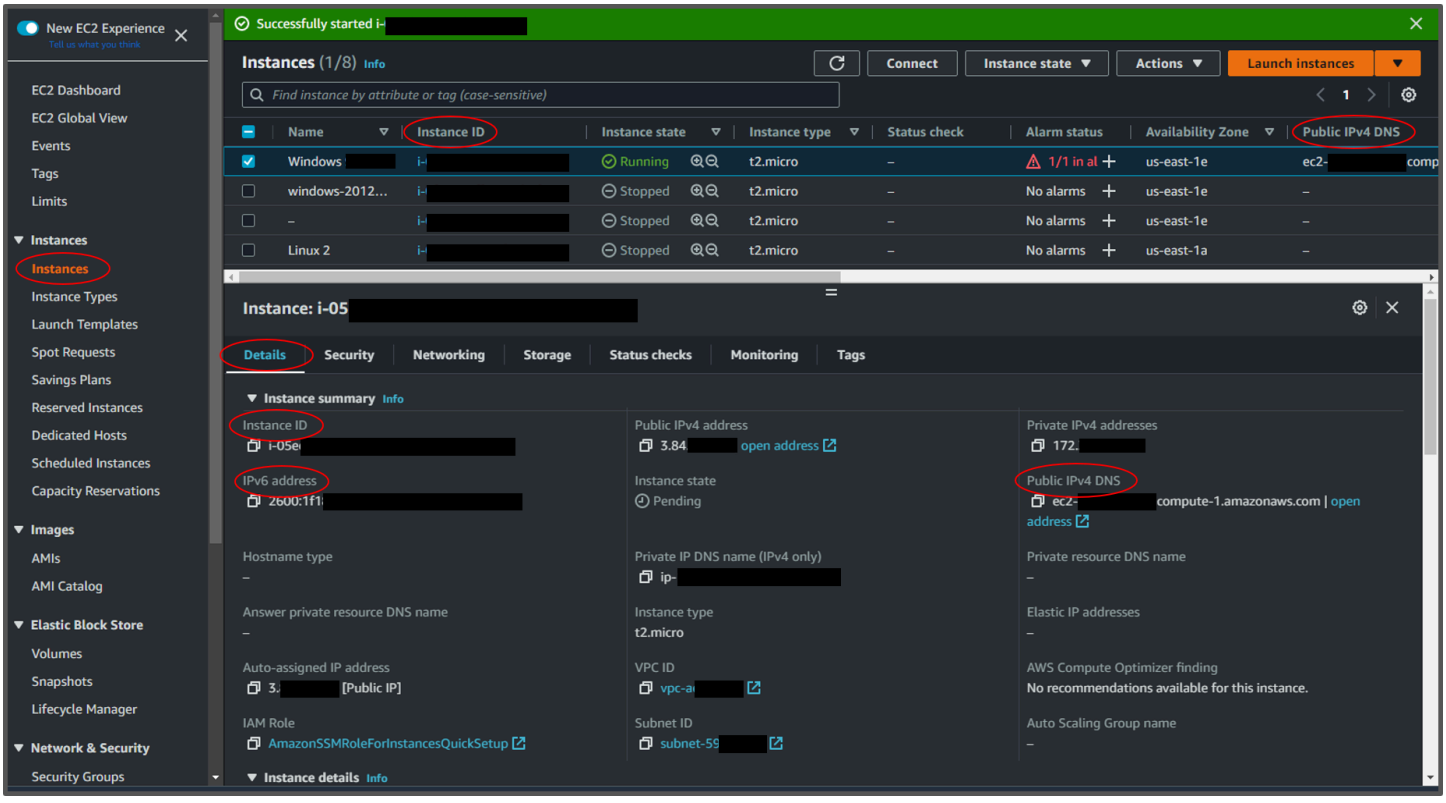
Di seguito sono riportati i prerequisiti generali per connettersi a un'istanza. Potrebbero esserci prerequisiti aggiuntivi specifici per l'opzione di connessione scelta.

Prerequisiti generali

- Verifica che l'istanza abbia superato i controlli dello stato. Possono essere necessari alcuni minuti affinché un'istanza sia pronta ad accettare richieste di connessione. Per ulteriori informazioni, consulta Visualizzazione dei controlli di stato.
- Ottieni i dettagli richiesti sull'istanza.
- Individuazione della chiave privata e impostazione delle autorizzazioni.
- (Opzionale) Ottenimento dell'impronta dell'istanza.

Ottieni i dettagli richiesti sull'istanza

Per prepararti a connetterti alla tua istanza, ottieni le seguenti informazioni dalla console Amazon EC2 o utilizzando la riga di comando.



- Ottieni il nome DNS pubblico dell'istanza.

Puoi ottenere il DNS pubblico dell'istanza dalla console Amazon EC2. Controlla la colonna DNS IPv4 pubblico del riquadro Istanze. Se questa colonna è nascosta, scegli l'icona delle impostazioni ( ) nell'angolo superiore destro della schermata e seleziona DNS pubblico IPv4. Puoi anche trovare il DNS pubblico nella sezione delle informazioni sull'istanza del riquadro Istanze. Quando selezioni l'istanza nel riquadro Istanze della console Amazon EC2, le informazioni su quell'istanza verranno visualizzate nella metà inferiore della pagina. Nella scheda Dettagli, cerca DNS IPv4 pubblico.

Se preferisci, puoi usare i comandi describe-instances (AWS CLI) o Get-EC2Instance ().AWS Tools for Windows PowerShell

Se non viene visualizzato alcun DNS IPv4 pubblico, verifica che lo Stato dell'istanza sia In esecuzione e che non sia stata avviata l'istanza in una sottorete privata. Se hai avviato l'istanza utilizzando la procedura guidata di avvio dell'istanza, potresti aver modificato il campo IP Auto-assign pubblico in Impostazioni di rete e cambiato il valore in Disabilita. Se disabiliti l'opzione IP Auto-assign pubblico, all'istanza non viene assegnato un indirizzo IP pubblico all'avvio.

- (Solo istanze IPv6) Ottieni l'indirizzo IPv6 dell'istanza.

  Se hai assegnato un indirizzo IPv6 all'istanza, puoi facoltativamente connetterti all'istanza utilizzando il relativo indirizzo IPv6 anziché un indirizzo IPv4 pubblico o un nome host DNS IPv4 pubblico. Il tuo computer locale deve avere un indirizzo IPv6 ed essere configurato per utilizzare IPv6. Puoi ottenere l'indirizzo IPv6 dell'istanza dalla console Amazon EC2. Controlla la colonna IP IPv6 del riquadro Istanze. In alternativa, puoi trovare l'indirizzo IPv6 nella sezione delle informazioni sull'istanza. Quando selezioni l'istanza nel riquadro Istanze della console Amazon EC2, le informazioni su quell'istanza verranno visualizzate nella metà inferiore della pagina. Nella scheda Dettagli, cerca l'indirizzo IPv6.

  Se preferisci, puoi usare i comandi describe-instances (AWS CLI) o Get-EC2Instance ().AWS Tools for Windows PowerShell Per ulteriori informazioni su IPv6, consulta Indirizzi IPv6.

- (Istanze Linux) Ottieni il nome utente per la tua istanza.

  È possibile connettersi all'istanza utilizzando il nome utente dell'account utente o il nome utente predefinito per l'AMI utilizzato per avviare l'istanza.

  - Ottenere il nome utente per il proprio account utente.

    Per ulteriori informazioni su come creare un account utente, consulta Gestione degli utenti del sistema sull'istanza Amazon EC2 Linux.

- Ottieni il nome utente predefinito per l'AMI che hai utilizzato per avviare l'istanza.
  - Amazon Linux – `ec2-user`
  - CentOS – `centos` oppure `ec2-user`
  - Debian – `admin`
  - Fedora – `fedora` oppure `ec2-user`
  - FreeBSD – `ec2-user`
  - RHEL – `ec2-user` oppure `root`
  - SUSE – `ec2-user` oppure `root`
  - Ubuntu – `ubuntu`
  - Oracle: `ec2-user`
  - Bitnami – `bitnami`
  - Rocky Linux – `rocky`
  - Altro – Verifica con il provider dell'AMI

Individuazione della chiave privata e impostazione delle autorizzazioni

Per effettuare la connessione iniziale a un'istanza Linux tramite SSH o a istanze Windows tramite RDP, devi conoscere la posizione del file della chiave privata. Per le connessioni SSH, devi impostare le autorizzazioni dei file in modo che tu sia l'unico a poter leggere la chiave privata.

Per informazioni su come funzionano le coppie di chiavi quando si utilizza Amazon EC2, consulta Coppie di chiavi Amazon EC2 e istanze Amazon EC2.

- Individuazione della chiave privata.

  Ottieni il percorso pienamente qualificato alla posizione nel tuo computer del file `.pem` per una coppia di chiavi che hai specificato quando hai avviato l'istanza. Per ulteriori informazioni, consulta the section called "Identificazione della chiave pubblica specificata al momento dell'avvio".

  Se non riesci a trovare il file della chiave privata, consulta Ho perso la mia chiave privata. Come posso connettermi alla mia istanza?

  (Istanze Linux) Se ti stai connettendo alla tua istanza usando PuTTY e devi convertire il file `.pem` in `.ppk`, consulta Convertire la chiave privata tramite PuTTYgen.

- (Istanze Linux) Imposta le autorizzazioni della tua chiave privata in modo che solo tu possa leggerla.
  - Connessione da macOS o Linux

    Se prevedi di utilizzare un client SSH su un computer macOS o Linux per connetterti all'istanza Linux, utilizza il comando seguente per impostare le autorizzazioni del file della chiave privata per essere l'unico a poterlo leggere.

    ```
    chmod 400 key-pair-name.pem
    ```

    Se non imposti queste autorizzazioni, allora non puoi connetterti alle tue istanze usando questa coppia di chiavi. Per ulteriori informazioni, consulta Errore: Unprotected Private Key File (File della chiave privata non protetto).
  - Connessione da Windows

    Apri File Explorer e apri il menu contestuale (clic con il pulsante destro del mouse) per il file. `.pem` Seleziona la scheda Proprietà > Sicurezza e scegli Avanzate. Scegli Disabilita l'ereditarietà. Rimuovi l'accesso a tutti gli utenti tranne l'utente corrente.

(Opzionale) Ottenimento dell'impronta dell'istanza

Per proteggerti dagli attacchi man-in-the-middle, puoi verificare l'autenticità dell'istanza a cui stai per connetterti verificando l'impronta visualizzata. La verifica dell'impronta risulta utile se hai avviato l'istanza da un'AMI pubblica fornita da terzi.

Panoramica delle attività

In primo luogo, ottieni l'impronta dell'istanza basandoti sull'istanza. Successivamente, quando ti connetti all'istanza e ti viene richiesta la verifica dell'impronta digitale, confronta l'impronta digitale ottenuta in questa procedura con l'impronta digitale visualizzata. Se le impronte digitali non corrispondono, qualcuno potrebbe tentare un attacco man-in-the-middle. Se tali impronte corrispondono, puoi collegarti in modo sicuro alla tua istanza.

Prerequisiti per ottenere l'impronta dell'istanza

- L'istanza non deve essere nello stato `pending`. L'impronta è disponibile solo al termine del primo avvio dell'istanza.
- Per ottenere l'output della console, devi essere il proprietario dell'istanza.

- Vi sono vari metodi per ottenere l'impronta digitale dell'istanza. Se vuoi utilizzare AWS CLI, deve essere installato sul computer locale. Per informazioni sull'installazione di AWS CLI, consulta Getting started with the AWS CLI nella Guida per l'AWS Command Line Interface utente.

Per ottenere l'impronta dell'istanza

Nella fase 1, viene visualizzato l'output della console, che include l'impronta digitale dell'istanza. Nella fase 2, individui l'impronta digitale dell'istanza nell'output della console.

1. Ottieni l'output della console usando uno dei seguenti metodi.

   Console

   1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
   2. Nel riquadro di navigazione sinistro, scegli Istanze.
   3. Seleziona l'istanza e poi scegli Operazioni, Monitoraggio e risoluzione dei problemi, Ottieni il log di sistema.

   AWS CLI

   Sul tuo computer locale (non sull'istanza alla quale ti stai connettendo), utilizza il comando get-console-output. Se l'output è grande, puoi reindirizzarlo a un file di testo per agevolarne la lettura.

   ```
   aws ec2 get-console-output \
       --instance-id i-1234567890abcdef0 \
       --query Output \
       --output text > temp.txt
   ```

   PowerShell

   Sul computer locale, utilizzare il seguente Get-EC2ConsoleOutput cmdlet.

   ```
   $encodedOutput = (Get-EC2ConsoleOutput -InstanceId i-1234567890abcdef0).Output
   [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($encodedOutput
   ```

2. Nell'output della console, individua l'impronta digitale dell'istanza (host), che si trova in `BEGIN SSH HOST KEY FINGERPRINTS`. Potrebbero esserci diverse impronte digitali dell'istanza. Quando effettui la connessione all'istanza, questa visualizzerà solo una delle impronte digitali.

L'output esatto può variare in base al sistema operativo, alla versione AMI e al fatto che AWS crei o meno la coppia di chiavi. Di seguito è riportato un output di esempio.

```
ec2:#############################################################
ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
ec2: 256 SHA256:l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY no comment (ECDSA)
ec2: 256 SHA256:kpEa+rw/Uq3zxaYZN8KT501iBtJOIdHG52dFi66EEfQ no comment (ED25519)
ec2: 2048 SHA256:L8l6pepcA7iqW/jBecQjVZClUrKY+o2cHLI0iHerbVc no comment (RSA)
ec2: -----END SSH HOST KEY FINGERPRINTS-----
ec2: #############################################################
```

> **Note**
>
> Farai riferimento a questa impronta digitale quando ti connetti all'istanza.

Connessione a un'istanza Linux tramite SSH

Ci sono tanti modi per connettersi alla propria istanza Linux tramite SSH. Alcuni modi dipendono dal sistema operativo del computer locale da cui ti connetti. Altri metodi sono basati su browser, come EC2 Instance Connect o AWS Systems Manager Session Manager, e possono essere utilizzati da qualsiasi computer. Puoi usare SSH per connetterti alla tua istanza Linux ed eseguire comandi, oppure utilizzare SSH per trasferire file tra il tuo computer locale e l'istanza.

Prima di connetterti a un'istanza Linux tramite SSH, è necessario soddisfare i prerequisiti seguenti:

- Verifica che l'istanza abbia superato i controlli dello stato. Possono essere necessari alcuni minuti affinché un'istanza sia pronta ad accettare richieste di connessione. Per ulteriori informazioni, consulta Visualizzazione dei controlli di stato.
- Verificare che il gruppo di sicurezza associato alla tua istanza consenta il traffico SSH in entrata dal tuo indirizzo IP. Per ulteriori informazioni, consulta Regole per la connessione alle istanze dal computer in uso.
- Ottieni i dettagli richiesti sull'istanza.
- Individuazione della chiave privata e impostazione delle autorizzazioni.
- (Opzionale) Ottenimento dell'impronta dell'istanza.

Quindi, scegli una delle seguenti opzioni per connetterti alla tua istanza Linux tramite SSH.

- Connettiti utilizzando un client SSH
- Collegamento tramite PuTTY
- Trasferisci file tramite SCP

Se non riesci a collegarti all'istanza e hai bisogno di assistenza per la risoluzione dei problemi, consulta Risoluzione dei problemi di connessione all'istanza Linux di Amazon EC2.

Connessione all'istanza Linux tramite un client SSH

Puoi usare Secure Shell (SSH) per connetterti all'istanza Linux dal tuo computer locale. Per ulteriori informazioni su altre opzioni, consulta Connettiti all'istanza EC2.

> **Note**
>
> Se compare un errore mentre tenti di connetterti alla tua istanza, assicurati che l'istanza soddisfi tutti i Prerequisiti per la connessione SSH. Se soddisfa tutti i prerequisiti e non riesci ancora a connetterti alla tua istanza Linux, consulta Risoluzione dei problemi di connessione all'istanza Linux di Amazon EC2.

Indice

- Prerequisiti per la connessione SSH
- Connessione all'istanza Linux tramite un client SSH

Prerequisiti per la connessione SSH

Prima di poterti connettere a un'istanza Linux tramite SSH, completa le seguenti attività.

Completa i prerequisiti generali.

- Verifica che l'istanza abbia superato i controlli dello stato. Possono essere necessari alcuni minuti affinché un'istanza sia pronta ad accettare richieste di connessione. Per ulteriori informazioni, consulta Visualizzazione dei controlli di stato.
- Ottieni i dettagli richiesti sull'istanza.
- Individuazione della chiave privata e impostazione delle autorizzazioni.
- (Opzionale) Ottenimento dell'impronta dell'istanza.

Consenti il traffico SSH in entrata dall'indirizzo IP.

Verificare che il gruppo di sicurezza associato alla tua istanza consenta il traffico SSH in entrata dal tuo indirizzo IP. Per ulteriori informazioni, consulta Regole per la connessione alle istanze dal computer in uso.

Installare un client SSH sul computer locale, se necessario.

Il computer locale potrebbe avere un client SSH installato per impostazione predefinita. Puoi verificarlo immettendo il seguente comando in una finestra del terminale. Se il computer non riconosce il comando, devi installare un client SSH.

```
ssh
```

Di seguito sono riportate alcune delle possibili opzioni per Windows. Se il computer è dotato di un sistema operativo diverso, consulta la documentazione relativa a quel sistema operativo per le opzioni del client SSH.

Installare OpenSSH su Windows

Dopo aver installato OpenSSH su Windows, puoi connetterti all'istanza Linux dal tuo computer Windows tramite SSH. Prima di iniziare, assicurati che siano soddisfatti i seguenti requisiti.

Versione Windows

La versione di Windows sul tuo computer deve essere Windows Server 2019 o successiva.

Per le versioni precedenti di Windows, scarica e installa Win32-OpenSSH invece.

PowerShell requisiti

Per installare OpenSSH sul tuo sistema operativo Windows utilizzando PowerShell, devi eseguire la PowerShell versione 5.1 o successiva e il tuo account deve essere membro del gruppo Administrators integrato. Esegui `$PSVersionTable.PSVersion` da PowerShell per verificare la tua versione. PowerShell

Per verificare se sei un membro del gruppo Administrators integrato, esegui il PowerShell comando seguente:

```
(New-Object
 Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).Is
```

Se sei un membro del gruppo Amministratori integrato, l'output è `True`.

Per installare OpenSSH per Windows utilizzando PowerShell, esegui il comando seguente. PowerShell

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Di seguito è riportato un output di esempio.

```
Path          :
Online        : True
RestartNeeded : False
```

Per disinstallare OpenSSH da Windows utilizzando PowerShell, esegui il seguente comando. PowerShell

```
Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Di seguito è riportato un output di esempio.

```
Path          :
Online        : True
RestartNeeded : True
```

Installare il Sottosistema Windows per Linux (WSL)

Dopo aver installato WSL su Windows, puoi connetterti all'istanza Linux dal tuo computer Windows tramite gli strumenti a riga di comando di Linux, come un client SSH.

Segui le istruzioni in Installazione del sottosistema Windows per Linux sulla tua istanza EC2 Windows. Se segui le istruzioni nella guida all'installazione di Microsoft, viene installata la distribuzione Ubuntu di Linux. Se preferisci, puoi installare una distribuzione Linux diversa.

In una finestra del terminale WSL, copia il file `.pem` (per la coppia di chiavi da te specificata per l'istanza all'avvio) da Windows a WSL. Prendi nota del percorso completo al file `.pem` su WSL da utilizzare nella connessione all'istanza. Per informazioni su come specificare il percorso al disco rigido Windows, consultare Come faccio ad accedere alla mia unità C?.

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

Per informazioni su come disinstallare Windows Subsystem per Linux, consultare Come faccio a disinstallare una distribuzione WSL?.

Connessione all'istanza Linux tramite un client SSH

Utilizza la seguente procedura per stabilire una connessione a un'istanza Linux tramite un client SSH.

Per connettersi all'istanza tramite un client SSH

1. Apri una finestra del terminale sul tuo computer.
2. Per connetterti all'istanza, utilizza il comando ssh. Ti servono i dettagli sull'istanza che hai raccolto come parte dei prerequisiti. Ad esempio, ti serve la posizione della chiave privata (file `.pem`), il nome utente e il nome DNS pubblico o l'indirizzo IPv6. Di seguito sono riportati comandi di esempio.
   - (DNS pubblico) Per utilizzare il nome DNS pubblico, inserisci il seguente comando.

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
     ```
   - (IPv6) In alternativa, se l'istanza dispone di un indirizzo IPv6, inserisci il seguente comando per utilizzare l'indirizzo IPv6.

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@2001:db8::1234:5678:1.2.3.4
     ```

   Di seguito è riportata una risposta di esempio.

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
    can't be established.
   ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
   Are you sure you want to continue connecting (yes/no)?
   ```
3. (Opzionale) Verificare che l'impronta riportata nell'avviso di sicurezza corrisponda all'impronta. Se queste impronte digitali non corrispondono, qualcuno potrebbe tentare un attacco man-in-the-middle. Se invece corrispondono, passare alla fase successiva. Per ulteriori informazioni, consulta Ottieni l'impronta dell'istanza.
4. Specificare (sì **`yes`**.

   La risposta visualizzata sarà simile alla seguente:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
 the list of known hosts.
```

Connessione a un'istanza Linux tramite PuTTY

Puoi connetterti all'istanza Linux tramite PuTTY, un client SSH gratuito per Windows.

Se utilizzi Windows Server 2019 o versione successiva, ti consigliamo di utilizzare OpenSSH, uno strumento di connettività open source per l'accesso remoto con il protocollo SSH.

> **Note**
>
> Se compare un errore mentre tenti di connetterti alla tua istanza, assicurati che l'istanza soddisfi tutti i Prerequisiti per la connessione SSH. Se soddisfa tutti i prerequisiti e non riesci ancora a connetterti alla tua istanza Linux, consulta Risoluzione dei problemi di connessione all'istanza Linux di Amazon EC2.

Indice

- Prerequisiti
- (Opzionale) Convertire la chiave privata tramite PuTTYgen
- Connessione all'istanza di Linux

Prerequisiti

Prima di connetterti a un'istanza Linux tramite PuTTY, completa le seguenti attività.

Completa i prerequisiti generali.

- Verifica che l'istanza abbia superato i controlli dello stato. Possono essere necessari alcuni minuti affinché un'istanza sia pronta ad accettare richieste di connessione. Per ulteriori informazioni, consulta Visualizzazione dei controlli di stato.
- Ottieni i dettagli richiesti sull'istanza.
- Individuazione della chiave privata e impostazione delle autorizzazioni.
- (Opzionale) Ottenimento dell'impronta dell'istanza.

Consenti il traffico SSH in entrata dall'indirizzo IP.

Verificare che il gruppo di sicurezza associato alla tua istanza consenta il traffico SSH in entrata dal tuo indirizzo IP. Per ulteriori informazioni, consulta Regole per la connessione alle istanze dal computer in uso.

Installare PuTTY sul computer locale (se necessario).

Scarica e installa PuTTY dalla pagina di download di PuTTY. Se è già installata una versione precedente di PuTTY, ti consigliamo di scaricare la versione più aggiornata. Assicurarsi di installare l'intera suite.

Converti la chiave privata in formato PPK tramite PuTTYgen.

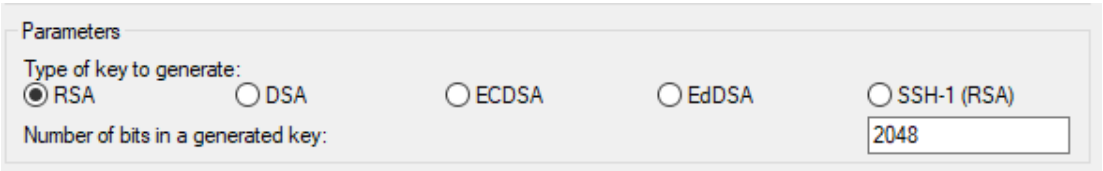
Devi specificare la chiave privata per la coppia di chiavi specificata al momento dell'avvio dell'istanza. Se hai creato la chiave privata in formato .pem, devi convertirla in un file PPK per utilizzarla con PuTTY. Individua la chiave privata (file .pem), poi segui i passaggi in Convertire la chiave privata tramite PuTTYgen.

(Opzionale) Convertire la chiave privata tramite PuTTYgen

PuTTY non supporta a livello nativo il formato PEM per le chiavi SSH. PuTTY fornisce uno strumento denominato PuTTYgen, che converte le chiavi PEM nel formato PPK richiesto per PuTTY. Se hai creato la chiave utilizzando il formato PEM anziché il formato PPK, devi convertire la chiave privata (file .pem) in questo formato (file .ppk) per l'utilizzo con PuTTY.

Per convertire la chiave privata dal formato PEM a PPK

1. Dal menu Start, scegliere All Programs (Tutti i programmi), PuTTY, PuTTYgen.
2. In Type of key to generate (Tipo di chiave da generare) scegliere RSA. Se la tua versione di PuTTYgen non include questa opzione, scegli RSA. SSH-2



3. Scegliere Load (Carica). Di default, PuTTYgen visualizza solo i file con estensione `.ppk`. Per individuare il file `.pem`, scegli l'opzione per visualizzare tutti i tipi di file.



4. Selezionare il file `.pem` per la coppia di chiavi specificata all'avvio dell'istanza, quindi scegliere Open (Apri). PuTTYgen visualizza un avviso che il file `.pem` è stato importato correttamente. Seleziona OK.
5. Per salvare la chiave privata in un formato che può essere utilizzato con PuTTY, scegliere Save private key (Salva chiave privata). PuTTYgen visualizza un avviso relativo al salvataggio della chiave senza passphrase. Scegliere Yes (Sì).

   > **Note**
   >
   > Le chiavi private con passphrase dispongono di un ulteriore livello di sicurezza. Anche se la chiave privata dovesse venire scoperta, non sarebbe possibile utilizzarla senza la passphrase. L'unico inconveniente dell'utilizzo di una passphrase è che complica l'automazione, in quanto è necessario l'intervento dell'utente per eseguire l'accesso all'istanza o per copiare i file in un'istanza.

6. Specificare per la chiave lo stesso nome usato per la coppia di chiavi (ad esempio, `key-pair-name`) e selezionare Save (Salva). PuTTY; aggiunge automaticamente l'estensione di file `.ppk`.

La chiave privata ora ha il formato corretto per l'utilizzo con PuTTY. A questo punto è possibile connettersi all'istanza utilizzando il client SSH di PuTTY.

Connessione all'istanza di Linux

Utilizza la seguente procedura per stabilire una connessione a un'istanza Linux tramite PuTTY. Devi disporre del file `.ppk` creato per la chiave privata. Per maggiori informazioni, consulta (Opzionale) Convertire la chiave privata tramite PuTTYgen nella sezione precedente. Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta Risoluzione dei problemi di connessione all'istanza Linux di Amazon EC2.

Ultima versione testata – PuTTY .78

Per connettersi all'istanza tramite PuTTY

1. Avvia PuTTY (dal menu Start, cerca PuTTY e scegli Apri).
2. Nel riquadro Category (Categoria), scegliere Session (Sessione) e completare i seguenti campi:

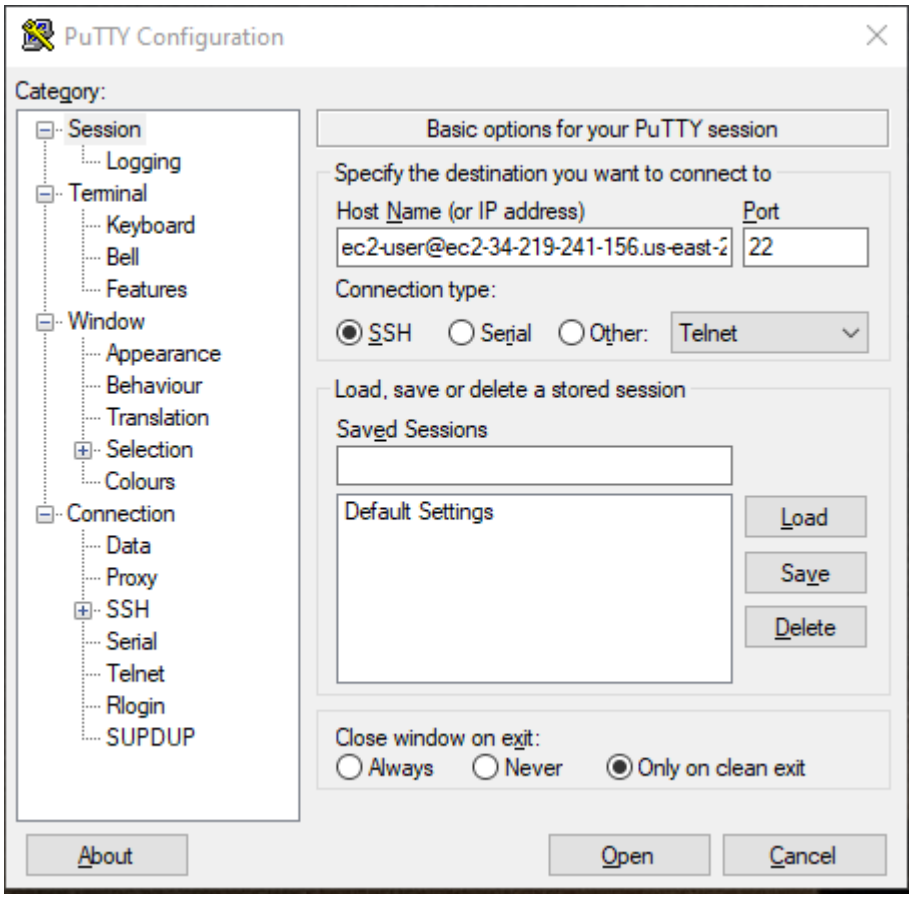
   a. Nella casella Host Name (Nome host) eseguire una delle operazioni seguenti:

- Per connettersi utilizzando il nome DNS pubblico dell'istanza, immettere *instance-user-name*@*instance-public-dns-name*.
- (IPv6) In alternativa, se l'istanza dispone di un indirizzo IPv6, per connettersi utilizzando l'indirizzo IPv6 dell'istanza, immettere *instance-user-name*@*2001:db8::1234:5678:1.2.3.4*.

Per ulteriori informazioni su come ottenere il nome utente per l'istanza e il nome DNS pubblico o l'indirizzo IPv6 dell'istanza, consulta Ottieni i dettagli richiesti sull'istanza.

b. Assicurarsi che il valore specificato per la Porta sia 22.

c. In Connection type (Tipo di connessione), selezionare SSH.



3. (Opzionale) È possibile configurare PuTTY in modo che invii automaticamente dati 'keepalive' a intervalli regolari per mantenere attiva la sessione. Ciò risulta utile per evitare la disconnessione dall'istanza a causa dell'inattività della sessione. Nel riquadro Categoria, scegli Connessione, quindi immettere l'intervallo richiesto nel campo Secondi tra dati keepalive. Ad esempio, se la

sessione si disconnette dopo 10 minuti di inattività, immettere 180 per configurare PuTTY per l'invio di dati keepalive ogni 3 minuti.

4. Nel riquadro Categoria, espandere Connessione, SSH e Autenticazione. Scegli Credenziali.
5. Accanto a File della chiave privata per l'autenticazione, scegli Sfoglia. Nella finestra di dialogo Seleziona file chiave privata, seleziona il file `.ppk` che hai generato per la tua coppia di chiavi. È possibile aprire il file o scegliere Apri nella finestra di dialogo Seleziona file con chiave privata.
6. (Opzionale) Se si prevede di connetterti di nuovo dopo questa sessione, puoi salvare le informazioni sulla sessione per uso futuro. Nel riquadro Categoria, scegli Sessione. Immetti un nome per la sessione in Sessioni salvate e quindi scegli Salva.
7. Per connetterti all'istanza, scegli Apri.
8. Se è la prima volta che si stabilisce una connessione a questa istanza, PuTTY visualizza una finestra di dialogo contenente un avviso di sicurezza che richiede di confermare l'affidabilità dell'host a cui ci si sta connettendo.

    a. (Opzionale) Verificare che l'impronta riportata nella finestra di dialogo dell'avviso di sicurezza corrisponda all'impronta precedentemente ottenuta in (Opzionale) Ottenimento dell'impronta dell'istanza. Se le impronte non corrispondono, è possibile che un utente non autorizzato stia cercando di eseguire un attacco di tipo "man-in-the-middle". Se invece corrispondono, passare alla fase successiva.

    b. Scegliere Accept (Accetta). Viene visualizzata una finestra e a questo punto si è connessi all'istanza.

> **Note**
>
> Se hai specificato una passphrase quando hai convertito la chiave privata nel formato PuTTY, devi specificare tale passphrase quando accedi all'istanza.

Se si verifica un errore mentre tenti di connetterti alla tua istanza, consulta Risoluzione dei problemi di connessione all'istanza Linux di Amazon EC2.

Trasferimento di file a un'istanza Linux tramite SCP

Un modo per trasferire file tra il computer locale e un'istanza Linux è utilizzare il protocollo secure copy (SCP). La policy di controllo dei servizi (SCP) è una buona opzione per operazioni semplici, ad esempio copie di file una tantum. L'SCP protegge i trasferimenti di file utilizzando lo stesso file .pem utilizzato per connetterti a un'istanza tramite SSH. Se devi mantenere i file sincronizzati o

se i file sono di grandi dimensioni, rsync è più veloce ed efficiente di SCP. Per motivi di sicurezza, utilizza rsync tramite SSH, poiché rsync trasferisce i dati utilizzando testo semplice per impostazione predefinita.

Prima di connetterti a un'istanza Linux tramite SCP, completa le seguenti attività:

- Completa i prerequisiti generali.
  - Verifica che l'istanza abbia superato i controlli dello stato. Possono essere necessari alcuni minuti affinché un'istanza sia pronta ad accettare richieste di connessione. Per ulteriori informazioni, consulta Visualizzazione dei controlli di stato.
  - Ottieni i dettagli richiesti sull'istanza.
  - Individuazione della chiave privata e impostazione delle autorizzazioni.
  - (Opzionale) Ottenimento dell'impronta dell'istanza.
- Consenti il traffico SSH in entrata dall'indirizzo IP.

  Verificare che il gruppo di sicurezza associato alla tua istanza consenta il traffico SSH in entrata dal tuo indirizzo IP. Per ulteriori informazioni, consulta Regole per la connessione alle istanze dal computer in uso.
- Installare un client SCP.

  La maggior parte dei computer Linux, Unix e Apple includono un client SCP per impostazione di default. Se il computer in uso non dispone di questo client, il progetto OpenSSH fornisce un'implementazione gratuita della suite completa di strumenti SSH, incluso un client SCP. Per ulteriori informazioni, consulta https://www.openssh.com.

La seguente procedura in fasi consente di utilizzare SCP per trasferire un file mediante il nome DNS pubblico dell'istanza o l'indirizzo IPv6, se l'istanza ne ha uno.

Per utilizzare SCP per trasferire file tra il computer e l'istanza

1. Determina la posizione del file di origine nel computer e il percorso di destinazione nell'istanza. Negli esempi seguenti, il nome del file della chiave privata è `key-pair-name.pem`, il file da trasferire è `my-file.txt`, il nome utente per l'istanza è ec2-user, il nome DNS pubblico dell'istanza è `instance-public-dns-name` e l'indirizzo IPv6 dell'istanza è `2001:db8::1234:5678:1.2.3.4`.
   - (DNS pubblico) Per trasferire un file nella destinazione sull'istanza, immetti il seguente comando dal computer.

```
scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@instance-public-dns-name:path/
```

- (IPv6) Per trasferire un file nella destinazione sull'istanza se l'istanza dispone di un indirizzo IPv6, immetti il seguente comando dal computer. L'indirizzo IPv6 deve essere racchiuso tra parentesi quadrate (`[ ]`), che devono essere inserite dopo un carattere di escape (\).

```
scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@
\[2001:db8::1234:5678:1.2.3.4\]:path/
```

2. Se non hai già effettuato la connessione all'istanza utilizzando SSH, viene visualizzata una risposta simile alla seguente:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

(Facoltativo) È possibile verificare se l'impronta nell'avviso di sicurezza corrisponde all'impronta dell'istanza. Per ulteriori informazioni, consulta (Opzionale) Ottenimento dell'impronta dell'istanza.

Specificare **`yes`**.

3. Se il trasferimento ha esito positivo, la risposta è simile alla seguente:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
my-file.txt                                   100%   480     24.4KB/s   00:00
```

4. Per trasferire un file nell'altra direzione, ovvero dall'istanza Amazon EC2 al computer, inverti l'ordine dei parametri host. Ad esempio, puoi trasferire `my-file.txt` dall'istanza EC2 a una destinazione nel computer locale come `my-file2.txt`, come illustrato negli esempi seguenti.

- (DNS pubblico) Per trasferire un file a una destinazione del computer, immetti il seguente comando dal computer.

```
scp -i /path/key-pair-name.pem ec2-user@instance-public-dns-name:path/my-file.txt path/my-file2.txt
```

- (IPv6) Per trasferire un file a una destinazione del computer se l'istanza ha un indirizzo IPv6, immetti il seguente comando dal computer. L'indirizzo IPv6 deve essere racchiuso tra parentesi quadrate ([ ]), che devono essere inserite dopo un carattere di escape (\).

```
scp -i /path/key-pair-name.pem ec2-user@\[2001:db8::1234:5678:1.2.3.4\]:path/
my-file.txt path/my-file2.txt
```

Gestione degli utenti del sistema sull'istanza Amazon EC2 Linux

Ogni istanza Linux viene avviata con un utente predefinito del sistema Linux. Puoi aggiungere utenti alla tua istanza ed eliminare utenti.

Per l'utente predefinito, il nome utente predefinito viene determinato dall'AMI specificata all'avvio dell'istanza.

> **Note**
>
> Per impostazione predefinita, l'autenticazione tramite password e l'accesso root sono disabilitati e sudo è abilitato. Per accedere alla tua istanza, devi usare una coppia di chiavi. Per ulteriori informazioni sull'accesso, consulta Connessione a un'istanza Linux tramite SSH. Puoi consentire l'autenticazione tramite password e l'accesso root per la tua istanza. Per ulteriori informazioni, consulta la documentazione relativa al sistema operativo in uso.

> **Note**
>
> Gli utenti del sistema Linux non devono essere confusi con gli utenti IAM. Per ulteriori informazioni, consulta Utenti IAM nella Guida per l'utente di IAM.

Indice

- Nomi utente predefiniti
- Considerazioni
- Creazione di un utente
- Rimuovere un utente

Nomi utente predefiniti

Il nome utente predefinito per un'istanza EC2 viene determinato dall'AMI specificata all'avvio dell'istanza.

I nomi utente predefiniti sono:

- Per un'AMI Amazon Linux, il nome utente è `ec2-user`.
- Per un'AMI CentOS, il nome utente è `centos` o `ec2-user`.
- Per un'AMI Debian, il nome utente è `admin`.
- Per un'AMI Fedora, il nome utente è `fedora` o `ec2-user`.
- Per un'AMI FreeBSD, il nome utente è `ec2-user`.
- Per un'AMI RHEL, il nome utente è `ec2-user` o `root`.
- Per un'AMI SUSE, il nome utente è `ec2-user` o `root`.
- Per un'AMI Ubuntu, il nome utente è `ubuntu`.
- Per un'AMI Oracle, il nome utente è `ec2-user`.
- Per un'AMI Bitnami, il nome utente è `bitnami`.

> **Note**
>
> Per trovare il nome utente predefinito per altre distribuzioni Linux, contattare il fornitore di AMI.

Considerazioni

L'utilizzo dell'utente di default è adeguato per numerose applicazioni, ma puoi aggiungere altri utenti in modo tale che possano disporre di propri file e WorkSpace. Inoltre, la creazione di utenti per i nuovi utenti è una procedura più sicura rispetto alla concessione a più utenti (spesso inesperti) dell'accesso all'utente predefinito, dal momento che tale utente può causare seri problemi al sistema se viene utilizzato in modo inappropriato.

Per abilitare l'accesso SSH agli utenti per l'istanza EC2 utilizzando un utente del sistema Linux, devi condividere la chiave SSH con l'utente. In alternativa, puoi utilizzare EC2 Instance Connect per fornire accesso agli utenti senza necessità di condividere e gestire le chiavi SSH. Per ulteriori informazioni, consulta Connettiti all'istanza Linux usando un indirizzo IP pubblico ed EC2 Instance Connect.

Creazione di un utente

Prima crea l'utente e in seguito aggiungi la chiave pubblica SSH che permette all'utente di connettersi e accedere all'istanza.

> **Important**
>
> Nella fase 1 di questa procedura, viene creata una nuova coppia di chiavi. Una coppia di chiavi funziona come una password, perciò è fondamentale gestirla in modo sicuro. Se si crea una coppia di chiavi per un utente, è necessario assicurarsi che l'invio della chiave privata venga effettuato in modo sicuro. In alternativa, l'utente può completare le fasi 1 e 2 creando la propria coppia di chiavi, mantenendo la propria chiave privata al sicuro sulla macchina, e poi inviare la chiave pubblica per completare la procedura dalla Fase 3.

Come creare un utente

1. Creazione di una nuova coppia di chiavi. È necessario fornire il file `.pem` all'utente per il quale si sta creando l'utente. Gli utenti devono utilizzare questo file per connettersi all'istanza.
2. Recuperare la chiave pubblica dalla coppia di chiavi creata nella fase precedente.

   ```
   $ ssh-keygen -y -f /path_to_key_pair/key-pair-name.pem
   ```

   Il comando restituisce la chiave pubblica, come illustrato nell'esempio seguente.

   ```
   ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6Vhz2ItxCih
   +PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/
   d6RJhJOI0iBXrlsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/
   i8SeJtjnV3iAoG/cQk+0FzZqaeJAAHco
   +CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi
   +z7wB3RbBQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
   ```

3. Collegati all'istanza.
4. Utilizzare il comando adduser per creare l'utente e aggiungerlo al sistema (con una voce nel file `/etc/passwd`). Il comando crea anche un gruppo e una home directory per l'utente. In questo esempio, l'utente viene chiamato *`newuser`*.

   - AL2023 e Amazon Linux 2

Con AL2023 e Amazon Linux 2, l'utente viene creato con l'autenticazione tramite password disabilitata per impostazione predefinita.

```
[ec2-user ~]$ sudo adduser newuser
```

- Ubuntu

  Includi il parametro `--disabled-password` per creare l'utente con l'autenticazione tramite password disabilitata.

```
[ubuntu ~]$ sudo adduser newuser --disabled-password
```

5. Passare al nuovo utente in modo che la directory e il file che verranno creati siano associati a una proprietà idonea.

```
[ec2-user ~]$ sudo su - newuser
```

   Il prompt cambia da `ec2-user` in *`newuser`* per indicare che si è passati dalla sessione di shell (interprete dei comandi) al nuovo utente.

6. Aggiungi la chiave pubblica SSH all'utente. Creare prima una directory nella home directory dell'utente per il file della chiave SSH, in seguito creare il file della chiave e infine incollare la chiave pubblica nel file della chiave, come descritto nelle seguenti fasi secondarie.

   a. Creare una directory `.ssh` nella home directory *`newuser`* e modificare le relative autorizzazioni file in `700` (solo il proprietario può leggere, scrivere o aprire la directory).

```
[newuser ~]$ mkdir .ssh
```

```
[newuser ~]$ chmod 700 .ssh
```

> **Important**
>
> Senza queste precise autorizzazioni file l'utente non sarà in grado di eseguire l'accesso.

   b. Creare un file denominato `authorized_keys` nella home directory `.ssh` e modificare le relative autorizzazioni file in `600` (solo il proprietario può leggere o scrivere nel file).

```
[newuser ~]$ touch .ssh/authorized_keys
```

```
[newuser ~]$ chmod 600 .ssh/authorized_keys
```

> **Important**
>
> Senza queste precise autorizzazioni file l'utente non sarà in grado di eseguire l'accesso.

c. Aprire il file `authorized_keys` con l'editor di testo preferito (ad esempio vim o nano).

```
[newuser ~]$ nano .ssh/authorized_keys
```

Incollare la chiave pubblica recuperata nella fase 2 nel file e salvare le modifiche.

> **Important**
>
> Assicurarsi di incollare la chiave pubblica in una riga continua. La chiave pubblica non deve essere divisa su più righe.

L'utente ora dovrebbe essere in grado di eseguire l'accesso all'istanza tramite l'utente *`newuser`* utilizzando la chiave privata corrispondente alla chiave pubblica aggiunta al file `authorized_keys`. Per ulteriori informazioni sui diversi metodi di connessione a un'istanza Linux, vedere Connessione a un'istanza Linux tramite SSH.

Rimuovere un utente

Se un utente non è più necessario, puoi rimuoverlo in modo che non possa più essere utilizzato.

Utilizza il comando userdel per rimuovere l'utente dal sistema. Quando si specifica il parametro `-r`, la home directory e lo spool di posta dell'utente vengono eliminati. Per conservare la home directory e lo spool di posta dell'utente, omettere il parametro `-r`.

```
[ec2-user ~]$ sudo userdel -r olduser
```

Connessione all'istanza Windows con il protocollo RDP

È possibile connettersi alle istanze Amazon EC2 create dalla maggior parte delle Amazon Machine Image (AMI) per Windows tramite Desktop remoto. Desktop remoto utilizza il protocollo RDP (Remote Desktop Protocol) per connettersi e utilizzare l'istanza con le stesse procedure usate per un computer vero e proprio. È disponibile per la maggior parte delle versioni di Windows e anche per Mac OS.

La licenza per il sistema operativo di Windows Server consente due connessioni remote simultanee per attività amministrative. Il costo della licenza per Windows Server è incluso nel costo della tua istanza Windows. Se servono più di due connessioni remote simultanee, devi acquistare una licenza di Remote Desktop Services (RDS). Se tenti di stabilire una terza connessione, si verifica un errore.

> **Tip**
>
> Se hai bisogno di connetterti alla tua istanza per risolvere problemi di avvio, configurazione di rete e altri problemi per le istanze basate sul sistema AWS Nitro, puoi utilizzare il. Console seriale EC2 per istanze

Indice

- Connettiti alla tua istanza Windows utilizzando un client RDP
- Connessione a un'istanza Windows utilizzando Fleet Manager
- Trasferire file a un'istanza Windows tramite RDP

Connettiti alla tua istanza Windows utilizzando un client RDP

Puoi connetterti alla tua istanza Windows utilizzando un client RDP nel modo seguente.

> **Tip**
>
> In alternativa, puoi connetterti alla tua istanza Windows con Systems Manager Fleet Manager o Endpoint EC2 Instance Connect.

Prerequisiti

Devi soddisfare i seguenti prerequisiti per connetterti all'istanza Windows utilizzando un client RDP.

- Completa i prerequisiti generali.
  - Verifica che l'istanza abbia superato i controlli dello stato. Possono essere necessari alcuni minuti affinché un'istanza sia pronta ad accettare richieste di connessione. Per ulteriori informazioni, consulta Visualizzazione dei controlli di stato.
  - Ottieni i dettagli richiesti sull'istanza.
  - Individuazione della chiave privata e impostazione delle autorizzazioni.
  - (Opzionale) Ottenimento dell'impronta dell'istanza.
- Installare un client RDP.
  - (Windows) Windows include un client RDP per default. Per verificare, digitare mstsc nella finestra del prompt dei comandi. Se il tuo computer non riconosce questo comando, scarica l'app Desktop remoto Microsoft da Microsoft Store.
  - (macOS X) Scarica l'app Windows per Mac (precedentemente denominata Desktop remoto di Microsoft) dal Mac App Store.
  - (Linux) Usare Remmina.
- Consenti il traffico RDP in entrata dall'indirizzo IP.

  Verifica che il gruppo di sicurezza associato alla tua istanza consenta il traffico RDP in entrata dal tuo indirizzo IP. Per ulteriori informazioni, consulta Regole per la connessione alle istanze dal computer in uso.

Recuperare la password amministratore

Se hai aggiunto la tua istanza a un dominio, puoi connetterti alla tua istanza utilizzando le credenziali di dominio di. Directory Service Nella schermata di accesso a Desktop remoto, anziché utilizzare il nome del computer locale e la password generata, utilizzare il nome utente completo per l'amministratore (ad esempio, **`corp.example.com\Admin`**) e la password per questo account.

Per connettersi a un'istanza di Windows usando RDP, è necessario recuperare la password iniziale dell'amministratore e immetterla quando ci si connette all'istanza. Dopo l'avvio dell'istanza, dovrai attendere alcuni minuti prima che la password sia disponibile. Il tuo account deve disporre dell'autorizzazione per avviare l'GetPasswordDataazione. Per ulteriori informazioni, consulta Policy di esempio da utilizzare all'API Amazon EC2.

Il nome utente predefinito per l'account amministratore dipende dalla lingua del sistema operativo (OS) contenuto nell'AMI. Per verificare il nome utente corretto, identifica la lingua del sistema operativo, poi scegli il nome utente corrispondente. Ad esempio, per un sistema operativo in inglese,

il nome utente è `Administrator`, per un sistema operativo in francese è `Administrateur` e per un sistema operativo portoghese è `Administrador`. Se una versione di lingua del sistema operativo non ha un nome utente nella stessa lingua, scegli il nome utente `Administrator (Other)`. Per ulteriori informazioni, consulta Nomi localizzati dell'account amministratore in Windows nel sito Web di Microsoft.

Per recuperare la password dell'amministratore iniziale

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza quindi scegli Connect (Connetti).
4. Nella pagina Connettiti all'istanza, scegli la scheda Client RDP.
5. Per Nome utente, scegli il nome utente predefinito per l'account amministratore. Il nome utente scelto deve corrispondere alla lingua del sistema operativo (OS) contenuto nell'AMI utilizzata per avviare l'istanza. Se non esiste un nome utente nella stessa lingua del sistema operativo, scegli Amministratore (Altro).
6. Scegliere Ottieni password.
7. Nella pagina Ottieni password di Windows, procedi nel modo seguente:

   a. Scegli Carica file della chiave privata e individua il file della chiave privata (`.pem`) da te specificato al momento dell'avvio dell'istanza. Selezionare il file e scegliere Open (Apri) per copiare l'intero contenuto del file in questa finestra.

   b. Selezionare Decifra password. La pagina Ottieni password Windows si chiude e la password di amministratore predefinita per l'istanza viene visualizzata in Password, sostituendo il link Ottieni password mostrato in precedenza.

   c. Copia la password e salvala in un luogo sicuro. Questa password ti servirà per connetterti all'istanza.

Connessione all'istanza Windows

La procedura seguente utilizza il client Remote Desktop Connection per Windows (MSTSC). Se utilizzi un client RDP diverso, scarica il file RDP e consulta la documentazione per il client RDP per i passaggi necessari per stabilire la connessione RDP.

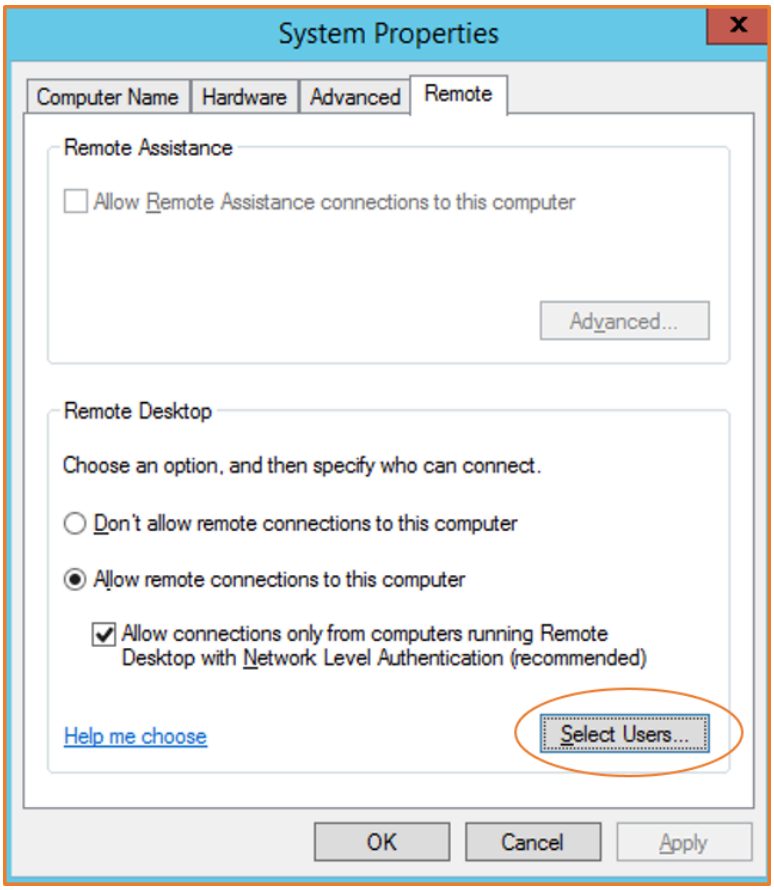
Per connetterti a un'istanza Windows utilizzando un client RDP

1. Nella pagina Connettiti all'istanza, scegli Scarica file desktop remoto. Al termine del download del file, scegli Annulla per tornare alla pagina Istanze. Il file RDP viene scaricato nella tua cartella `Downloads`.
2. Esegui `mstsc.exe` per aprire il client RDP.
3. Espandi Mostra opzioni, scegli Apri e seleziona il file.rdp dalla cartella `Downloads`.
4. Per impostazione predefinita, Computer è il nome DNS IPv4 pubblico dell'istanza e Nome utente è l'account amministratore. Per connetterti all'istanza utilizzando invece IPv6, sostituisci il nome DNS IPv4 pubblico dell'istanza con il relativo indirizzo IPv6. Rivedi le impostazioni predefinite e modificale come necessario.
5. Scegli Connetti. Se ricevi un avviso che il publisher della connessione remota non è noto, scegli Connetti per continuare.
6. Inserisci la password salvata in precedenza, poi scegli OK.
7. Data la natura dei certificati autofirmati, è possibile che venga visualizzato un avviso relativo all'impossibilità di autenticare il certificato di sicurezza. Esegui una delle seguenti operazioni:
   - Se consideri attendibile il certificato, scegli Sì per connetterti all'istanza.
   - [Windows] Prima di procedere, confronta l'impronta digitale del certificato con il valore nel log di sistema per confermare l'identità del computer remoto. Scegli Visualizza certificato e poi seleziona Identificazione personale dalla scheda Dettagli. Confronta questo valore con il valore di `RDPCERTIFICATE-THUMBPRINT` in Operazioni, Monitoraggio e risoluzione dei problemi, Ottieni log di sistema.
   - [Mac OS X] Prima di procedere, confronta l'impronta del certificato con il valore nel log di sistema per confermare l'identità del computer remoto. Scegli Mostra certificato, espandi Dettagli e seleziona Impronte digitali SHA1. Confronta questo valore con il valore di `RDPCERTIFICATE-THUMBPRINT` in Operazioni, Monitoraggio e risoluzione dei problemi, Ottieni log di sistema.
8. Se la connessione RDP ha esito positivo, il client RDP visualizza la schermata di accesso di Windows e poi il desktop di Windows. Se invece ricevi un messaggio di errore, consulta the section called "Il desktop remoto non può connettersi al computer remoto". Quando hai completato la connessione RDP, puoi chiudere il client RDP.

Configurazione degli account utente

Dopo aver stabilito la connessione all'istanza tramite RDP, ti consigliamo di svolgere le seguenti attività:

- Modificare la password dell'amministratore rispetto al valore di default. Modificare la password mentre si è connessi all'istanza, usando le stesse procedure valide per qualsiasi computer che esegua Windows Server.
- Crea un altro utente con privilegi di amministratore sull'istanza. Questo rappresenta una garanzia se ci si dimentica la password dell'amministratore o se si verifica un problema a livello di account dell'amministratore. Il nuovo account deve essere autorizzato ad accedere all'istanza da remoto. Aprire System Properties (Proprietà di sistema) facendo clic con il tasto destro sull'icona Questo PC sul desktop Windows o su File Explorer e selezionare Properties (Proprietà). Scegliere Remote settings (Impostazioni remote), quindi Select Users (Seleziona utenti) per aggiungere l'utente al gruppo Utenti desktop remoti.



Connessione a un'istanza Windows utilizzando Fleet Manager

Puoi utilizzare Fleet Manager, una funzionalità di AWS Systems Manager, per connetterti alle istanze Windows utilizzando il Remote Desktop Protocol (RDP) e visualizzare fino a quattro istanze Windows sulla stessa pagina nel. Console di gestione AWS Puoi connetterti alla prima istanza nel desktop remoto della Gestione dei gruppi di nodi direttamente dalla pagina Istanze nella console Amazon EC2. Per ulteriori informazioni su Fleet Manager, consulta Connect to a managed instance using Remote Desktop nella Guida per l'utente di AWS Systems Manager .

Nello specifico, non è necessario che tu consenta il traffico RDP in entrata dal tuo indirizzo IP, se utilizzi Fleet Manager per la connessione. Fleet Manager lo gestisce al posto tuo.

Prerequisiti

Prima di tentare di connetterti a un'istanza tramite Fleet Manager, devi configurare l'ambiente. Per ulteriori informazioni, consulta Configurare l'ambiente nella Guida per l'utente di AWS Systems Manager .

Per connettersi a un'istanza Windows tramite Fleet Manager

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Instances (Istanze).
3. Seleziona l'istanza quindi scegli Connect (Connetti).
4. Nella scheda Client RDP, per Tipo di connessione, scegli Connettiti tramite Fleet Manager.
5. Scegliere Desktop remoto di Fleet Manager. Si apre la pagina Fleet Manager Remote Desktop nella console AWS Systems Manager .
6. Inserisci le credenziali e poi scegli Connettiti.
7. Se la connessione RDP ha esito positivo, Fleet Manager visualizza il desktop di Windows. Al termine della sessione, scegli Operazioni, Termina sessione.

Per ulteriori informazioni, consulta Connessione a un'istanza gestita da Windows Server tramite Desktop remoto nella Guida per l'utente di AWS Systems Manager .

Trasferire file a un'istanza Windows tramite RDP

Puoi usare l'istanza Windows con le stesse procedure valide per qualsiasi server Windows. Ad esempio, puoi trasferire file tra un'istanza Windows e il computer locale tramite la caratteristica di

condivisione di file locale del software Connessione desktop remoto (RDP) Microsoft. Puoi accedere ai file locali su unità disco rigido (HDD), unità DVD, unità audio/video portatili e unità di rete mappate.

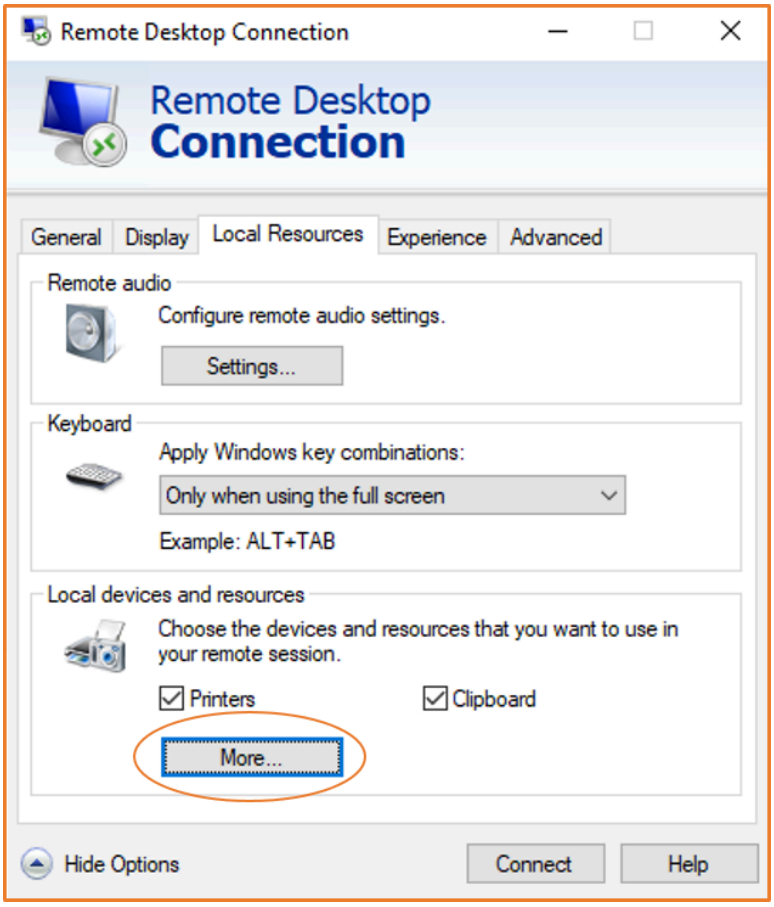
Per accedere ai file locali dalle istanze di Windows, devi abilitare la caratteristica di condivisione file locale mappando l'unità di sessione remota sull'unità locale. I passaggi sono leggermente diversi, a seconda che il sistema operativo del computer locale sia Windows o macOS X.

Per ulteriori informazioni sui prerequisiti per connettersi tramite RDP, consulta Prerequisiti.

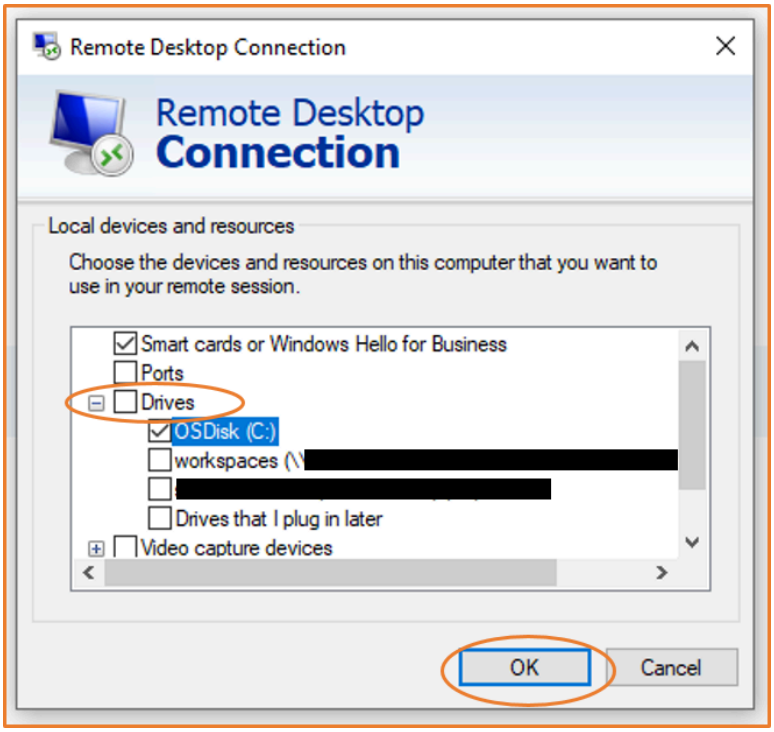
Windows

Per mappare l'unità di sessione remota all'unità locale sul computer Windows locale

1. Apri il client di connessione remota desktop.
2. Scegliere Show options (Mostra opzioni).
3. Aggiungi il nome host dell'istanza al campo Computer e il nome utente al campo Nome utente, come riportato di seguito:
    a. Nella sezione Connection settings (Impostazioni connessione), scegli Open... (Apri...) e passa al file di collegamento RDP scaricato dalla console Amazon EC2. Il file contiene il nome host DNS IPv4 pubblico, che identifica l'istanza e il nome utente dell'amministratore.
    b. Scegli il file e seleziona Open (Apri). I campi Computer e User name (Nome utente) vengono compilati con i valori del file di collegamento RDP.
    c. Scegli Save (Salva).
4. Scegliere la scheda Local Resources (Risorse locali).
5. In Local Devices and resources (Dispositivi e risorse locali), scegli More... (Altro...).



6. Apri Drives (Unità) e seleziona l'unità locale per mappare la tua istanza di Windows.
7. Seleziona OK.

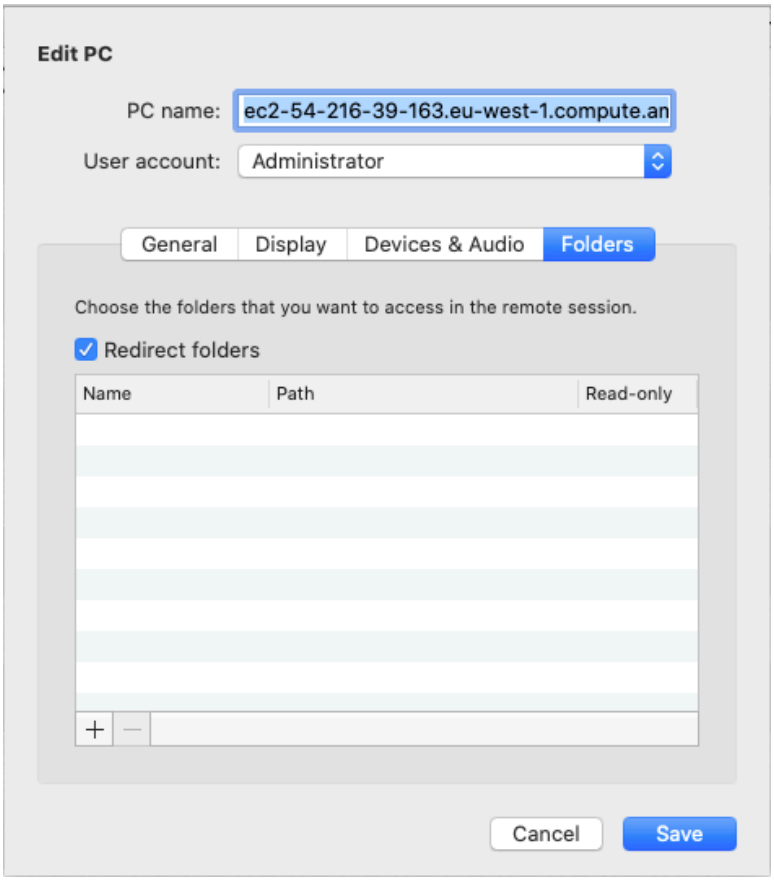


8. Scegli Connect (Connetti) per collegarti all'istanza di Windows.

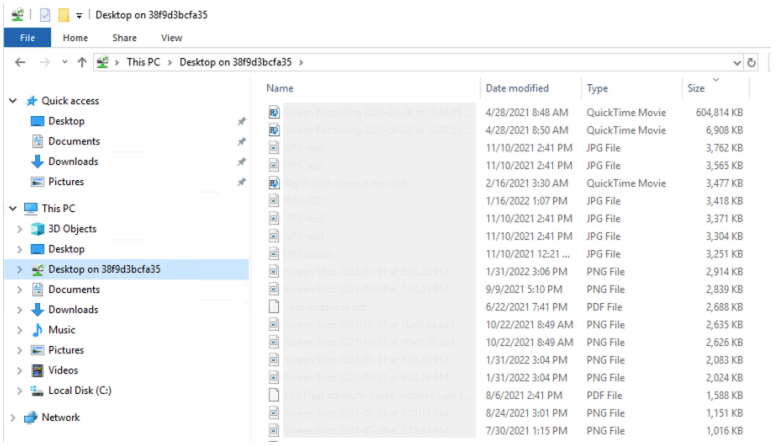
macOS X

Per mappare l'unità di sessione remota alla cartella locale sul computer macOS X locale

1. Apri il client di connessione remota desktop.
2. Individua il file RDP scaricato dalla console Amazon EC2 (quando ti sei connesso inizialmente all'istanza) e trascinalo sul client di Connessione Desktop remoto.
3. Apri il menu contestuale (clic con il pulsante destro del mouse) per il file RDP e scegli Modifica.
4. Seleziona la scheda Cartelle e poi la casella di spunta Reindirizza cartelle.



5. Seleziona l'icona + in basso a sinistra, vai alla cartella da mappare e scegli Open (Apri). Ripeti questo passaggio per eseguire la mappatura di ogni cartella da mappare.
6. Scegli Save (Salva).
7. Scegli Connect (Connetti) per collegarti all'istanza di Windows. Ti verrà richiesta la password.
8. Nell'istanza, in Esplora file espandi This PC (Questo PC) e cerca la cartella condivisa da cui puoi accedere ai file locali. Nello screenshot seguente, la cartella Desktop del computer locale è stata mappata all'unità di sessione remota sull'istanza.



Per ulteriori informazioni su come rendere disponibili i dispositivi locali per una sessione remota su un computer Mac, consulta Get started with the macOS client (Nozioni di base sul client macOS).

Connettersi all'istanza Amazon EC2 utilizzando Session Manager

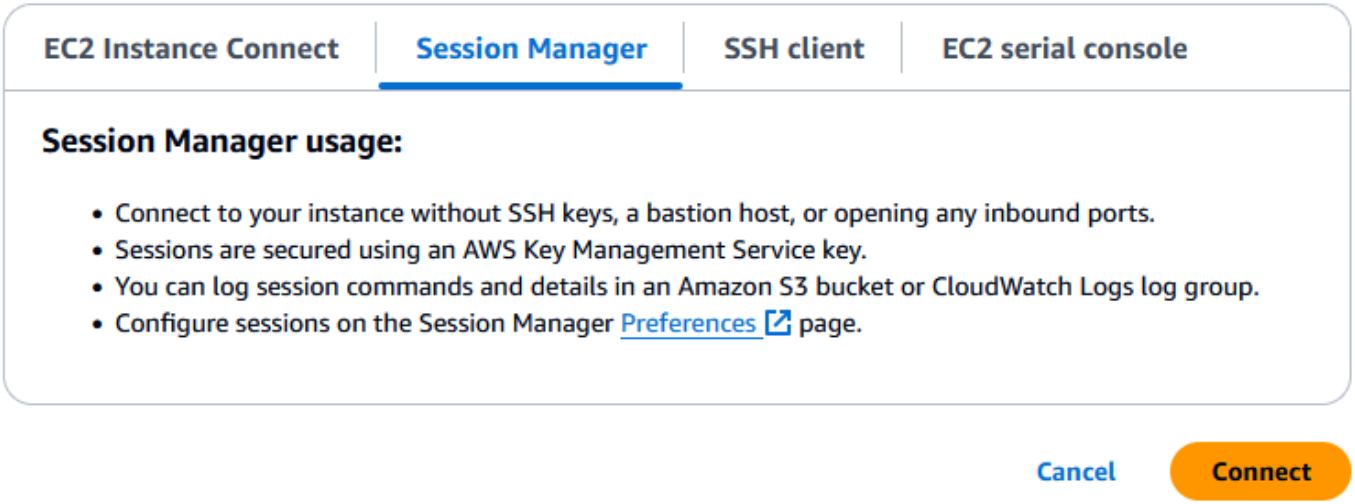
Session Manager è una AWS Systems Manager funzionalità completamente gestita per la gestione delle istanze Amazon EC2 tramite una shell interattiva basata su browser o tramite. AWS CLI Puoi utilizzare Session Manager per avviare una sessione con un'istanza nel tuo account. Dopo l'avvio della sessione, puoi eseguire comandi interattivi sull'istanza come faresti con qualsiasi altro tipo di connessione. Per ulteriori informazioni su Session Manager, consulta AWS Systems Manager Session Manager nella Guida per l'utente di AWS Systems Manager .

Prerequisiti

Prima di tentare di connetterti a un'istanza utilizzando Session Manager, devi completare le fasi di installazione richieste. Ad esempio, l'istanza deve essere gestita da SSM e deve avere un ruolo IAM associato alla policy. AmazonSSMManagedInstanceCore Per ulteriori informazioni e istruzioni, consulta Setting up Session Manager (Impostazione di Session Manager).

Per connetterti a un'istanza Amazon EC2 che utilizza Session Manager tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza, quindi scegliere Collegarsi.
4. Per il metodo di connessione, seleziona Session Manager.
5. Scegli Connetti per iniziare la sessione.



Risoluzione dei problemi

Se viene visualizzato un errore che non si è autorizzati a eseguire una o più operazioni Systems Manager (`ssm:command-name`), è necessario aggiornare le policy per consentire l'avvio delle sessioni dalla console Amazon EC2. Per ulteriori informazioni e istruzioni, consulta Guida rapida sulle policy IAM predefinite per Session Manager nella Guida per l'utente di AWS Systems Manager .

Connettiti all'istanza Linux usando un indirizzo IP pubblico ed EC2 Instance Connect

Con Amazon EC2 Instance Connect, puoi connetterti in modo sicuro alle istanze Linux con Secure Shell (SSH). Con EC2 Instance Connect, utilizzi policy e principi AWS Identity and Access Management (IAM) per controllare l'accesso SSH alle tue istanze, eliminando la necessità di condividere e gestire le chiavi SSH. Tutte le richieste di connessione effettuate tramite EC2 Instance Connect vengono registrate su AWS CloudTrail per consentirti di verificarle.

Puoi utilizzare EC2 Instance Connect per collegarti alle istanze Linux tramite la console Amazon EC2 o il client SSH di tua scelta.

Quando ti connetti a un'istanza tramite EC2 Instance Connect, l'API di EC2 Instance Connect invia una chiave pubblica SSH ai metadati dell'istanza, dove rimane per 60 secondi. Una policy IAM collegata al tuo utente autorizza quest'ultimo a inserire la chiave pubblica tra i metadati dell'istanza. Il daemon SSH utilizza `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, configurati al momento dell'installazione di EC2 Instance Connect, per recuperare la chiave pubblica dai metadati dell'istanza al fine effettuare l'autenticazione e ti permette di collegarti all'istanza.

> **Tip**
>
> EC2 Instance Connect è una delle opzioni per la connessione all'istanza Linux. Per altre opzioni, vedi Connessione a un'istanza Linux tramite SSH Per effettuare la connessione a un'istanza Windows, consulta Connessione all'istanza Windows con il protocollo RDP.

Prezzi

EC2 Instance Connect è disponibile senza costi aggiuntivi.

Disponibilità nelle regioni

EC2 Instance Connect è disponibile in tutte le versioni tranne. Regioni AWS AWS European Sovereign Cloud (Germany) Non è supportato nelle zone locali.

Indice

- Tutorial: Completa la configurazione richiesta per connettersi all'istanza tramite EC2 Instance Connect
- Prerequisiti per EC2 Instance Connect
- Concessione di un'autorizzazione IAM per EC2 Instance Connect
- Installazione di EC2 Instance Connect sulle istanze EC2
- Connessione alla tua istanza Linux tramite EC2 Instance Connect
- Disinstallazione di EC2 Instance Connect

Per un post del blog che illustra come migliorare la sicurezza degli host bastione utilizzando EC2 Instance Connect, consulta Securing your bastion hosts with Amazon EC2 Instance Connect.

Tutorial: Completa la configurazione richiesta per connettersi all'istanza tramite EC2 Instance Connect

Per connetterti alla tua istanza tramite EC2 Instance Connect nella console Amazon EC2, devi prima completare la configurazione dei prerequisiti che ti consentirà di connetterti con successo all'istanza. Lo scopo di questo tutorial è di guidarti attraverso le attività per completare la configurazione dei prerequisiti.

Panoramica del tutorial

In questo tutorial, completerai le quattro seguenti attività:

- Attività 1: Concessione delle autorizzazioni necessarie per utilizzare EC2 Instance Connect

  Per prima cosa, creerai una policy IAM che contenga le autorizzazioni IAM che ti consentono di inviare una chiave pubblica ai metadati dell'istanza. Collegherai questa policy alla tua identità IAM (utente, gruppo di utenti o ruolo) in modo tale che la tua identità IAM ottenga tali autorizzazioni.
- Attività 2: Consenti il traffico in entrata dal servizio EC2 Instance Connect all'istanza in uso

  Creerai un gruppo di sicurezza che consenta il traffico dal servizio EC2 Instance Connect verso la tua istanza. Questa funzionalità è obbligatoria quando utilizzi EC2 Instance Connect nella console Amazon EC2 per collegarti all'istanza.
- Attività 3: Avvia la tua istanza

  Avvierai un'istanza EC2 utilizzando un'AMI preinstallata con EC2 Instance Connect e aggiungerai il gruppo di sicurezza da te creato nella fase precedente.
- Attività 4: Connessione all'istanza

  Infine, utilizzerai EC2 Instance Connect nella console Amazon EC2 per collegarti all'istanza. Se riesci a connetterti, puoi essere certo che la configurazione dei prerequisiti da te completata nelle Attività 1, 2 e 3 ha avuto successo.

Attività 1: Concessione delle autorizzazioni necessarie per utilizzare EC2 Instance Connect

Quando ti connetti a un'istanza tramite EC2 Instance Connect, l'API di EC2 Instance Connect invia una chiave pubblica SSH ai metadati dell'istanza, dove rimane per 60 secondi. Hai bisogno di una policy IAM collegata alla tua identità IAM (utente, gruppo di utenti o ruolo) per concederti l'autorizzazione richiesta per inviare la chiave pubblica ai metadati dell'istanza.

Obiettivo dell'attività

Creerai la policy IAM che concede l'autorizzazione per inviare la chiave pubblica all'istanza. L'azione specifica da consentire è `ec2-instance-connect:SendSSHPublicKey`. Devi anche consentire l'azione `ec2:DescribeInstances` in modo da poter visualizzare e selezionare l'istanza nella console Amazon EC2.

Dopo aver creato la policy, la collegherai alla tua identità IAM (utente, gruppo di utenti o ruolo) in modo tale che la tua identità IAM ottenga le autorizzazioni.

Creerai una policy configurata come indicato di seguito:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
}
```

> **Important**
>
> La policy IAM creata in questo tutorial è una politica altamente permissiva; consente di connettersi a qualsiasi istanza utilizzando qualsiasi nome utente dell'AMI. Questo tutorial utilizza questa politica altamente permissiva per mantenere il tutorial semplice e focalizzato sulle configurazioni specifiche che questo tutorial sta insegnando. Tuttavia, in un ambiente di produzione, consigliamo di configurare la policy IAM in modo da fornire autorizzazioni con privilegi minimi. Per esempi di policy IAM, consulta Concessione di un'autorizzazione IAM per EC2 Instance Connect.

Per creare e collegare una policy IAM che consenta di utilizzare EC2 Instance Connect per connetterti alle istanze

1. Innanzitutto, crea la policy IAM
   a. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
   b. Nel riquadro di navigazione, scegli Policy.
   c. Scegli Create Policy (Crea policy).
   d. Nella pagina Specifica autorizzazione, procedi nel modo seguente:

i. Per Servizio, scegli EC2 Instance Connect.

ii. In Azioni consentite, nel campo di ricerca inizia a digitare **`send`** per mostrare le azioni pertinenti, quindi seleziona. SendSSHPublicKey

iii. In Risorse, scegli Tutte. Per un ambiente di produzione, consigliamo di specificare l'istanza tramite il relativo ARN, ma per questo tutorial, consentirai tutte le istanze.

iv. Scegli Aggiungere più autorizzazioni.

v. Per Servizio, scegli EC2.

vi. In Azioni consentite, nel campo di ricerca inizia **`describein`** a digitare per mostrare le azioni pertinenti, quindi seleziona. DescribeInstances

vii. Scegli Avanti.

e. Nella pagina Rivedi e crea, effettua le operazioni seguenti:

i. In Policy name (Nome policy), immettere un nome per la policy.

ii. Scegli Crea policy.

2. Poi collega la policy alla tua identità

a. Nel pannello di navigazione della console IAM seleziona Policy.

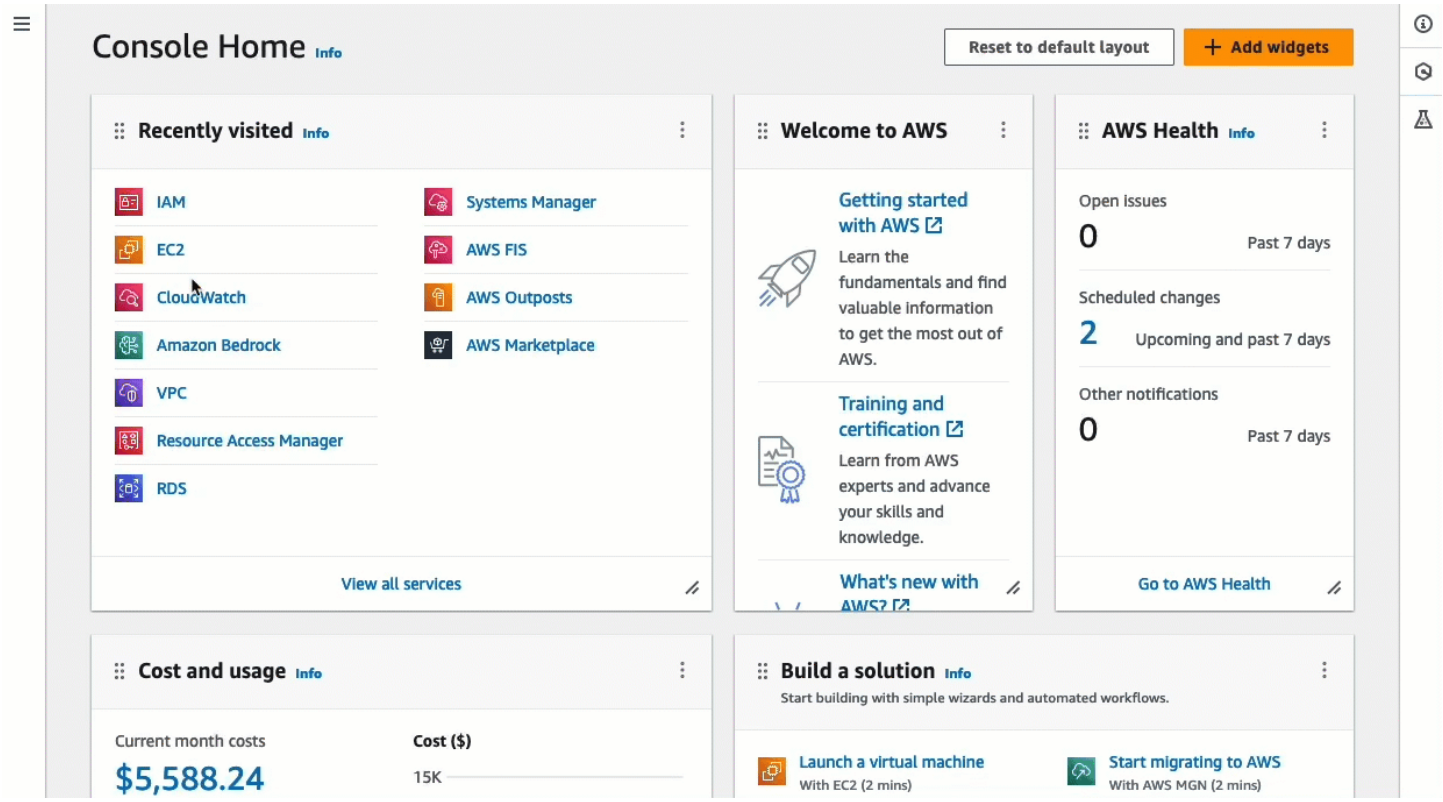
b. Nell'elenco di policy, seleziona il pulsante di opzione accanto al nome della policy da te creata. Puoi utilizzare la casella di ricerca per filtrare l'elenco di policy.

c. Seleziona Operazioni, Collega.

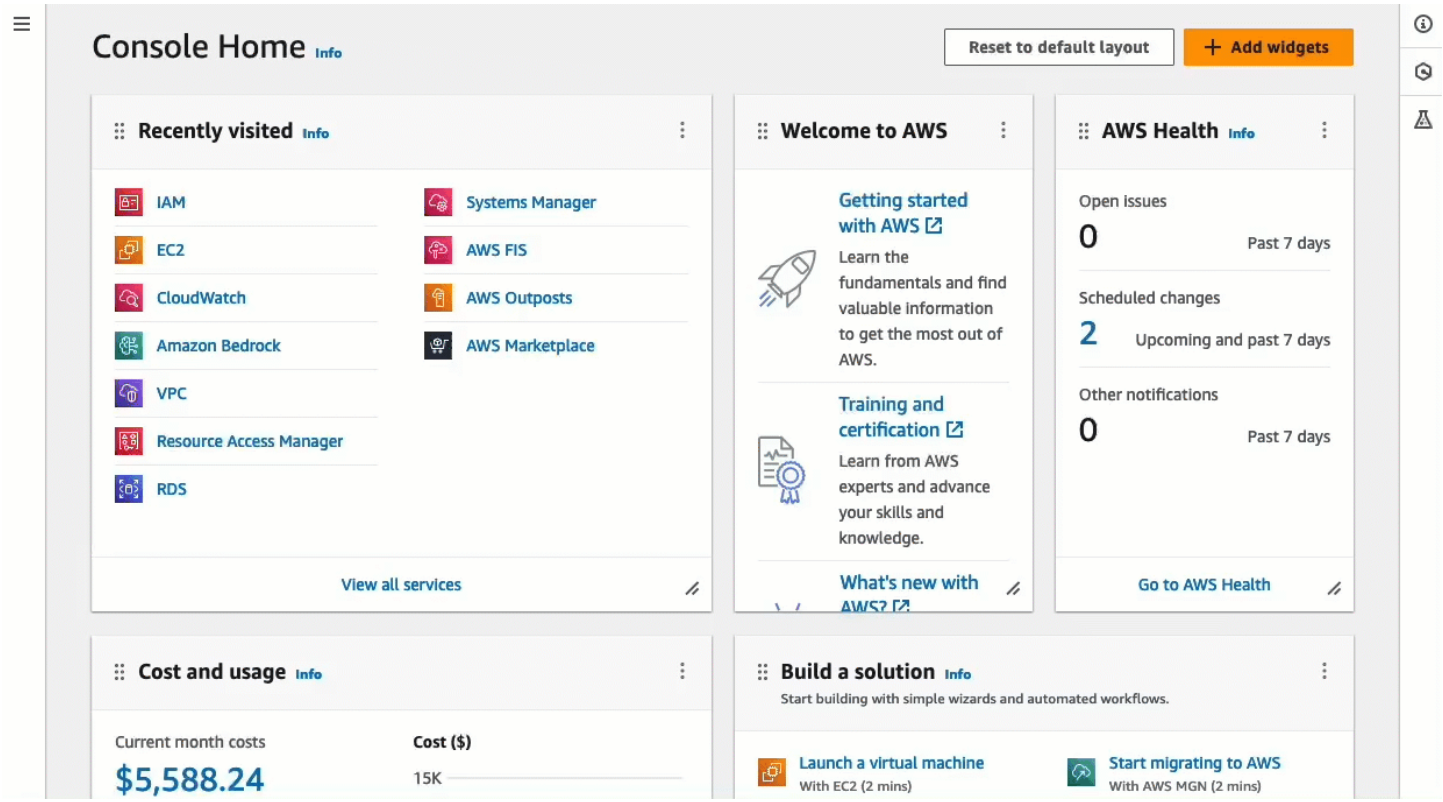
d. In Entità IAM, seleziona la casella di spunta accanto alla tua identità (utente, gruppo di utenti o ruolo). Puoi utilizzare la casella di ricerca per filtrare l'elenco di entità.

e. Scegli Collega policy.

Visualizzazione di un'animazione: Crea una policy IAM



Visualizzazione di un'animazione: Collega una policy IAM



Attività 2: Consenti il traffico in entrata dal servizio EC2 Instance Connect all'istanza in uso

Quando utilizzi EC2 Instance Connect nella console Amazon EC2 per connetterti a un'istanza, il traffico a cui deve essere consentito di raggiungere l'istanza è il traffico proveniente dal servizio EC2 Instance Connect. Questa operazione è diversa dalla connessione dal computer locale a un'istanza; in quel caso, devi consentire il traffico dal computer locale all'istanza. Per consentire il traffico dal servizio EC2 Instance Connect, devi creare un gruppo di sicurezza che consenta il traffico SSH in entrata dall'intervallo di indirizzi IP per il servizio EC2 Instance Connect.

AWS utilizza elenchi di prefissi per gestire gli intervalli di indirizzi IP. I nomi degli elenchi di prefissi di EC2 Instance Connect sono i seguenti, *`region`* sostituiti dal codice regionale:

- Nome dell'elenco di prefissi IPv4: `com.amazonaws.`*`region`*`.ec2-instance-connect`
- Nome dell'elenco di prefissi IPv6: `com.amazonaws.`*`region`*`.ipv6.ec2-instance-connect`

Obiettivo dell'attività

Creerai un gruppo di sicurezza che consente il traffico SSH in entrata sulla porta 22 dall'elenco dei prefissi IPv4 nella regione in cui si trova l'istanza.

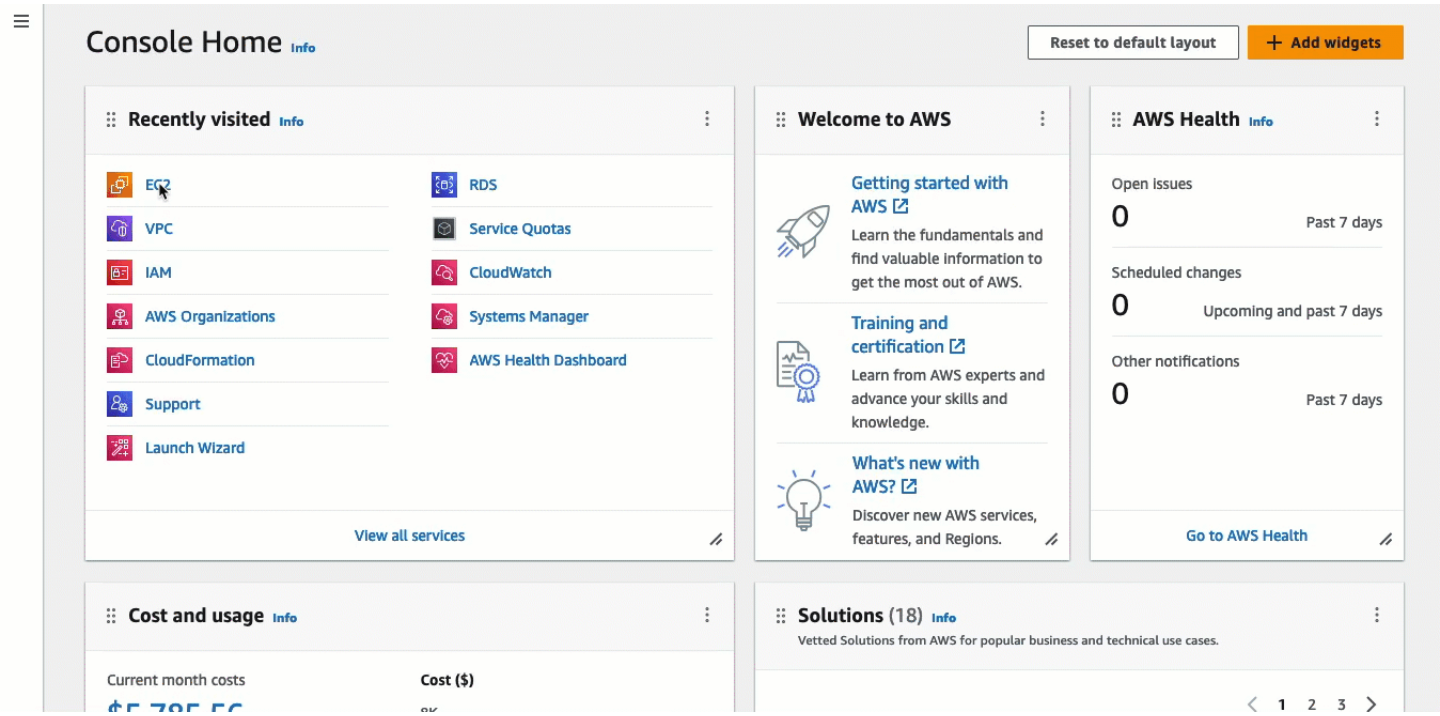
Per creare un gruppo di sicurezza che consenta il traffico in entrata dal servizio EC2 Instance Connect verso la tua istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fare clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
3. Scegliere Create Security Group (Crea gruppo di sicurezza).
4. In Basic details (Dettagli di base), eseguire le operazioni seguenti:
   a. In Nome gruppo di sicurezza, inserisci un nome significativo per il tuo gruppo di sicurezza.
   b. In Descrizione, inserisci una descrizione significativa per il tuo gruppo di sicurezza.
5. In Regole in entrata, effettua le operazioni seguenti:
   a. Scegli Aggiungi regola.
   b. Per Type (Tipo) scegli SSH.
   c. Per Origine, lascia Personalizzata.
   d. Nel campo accanto a Origine, seleziona l'elenco dei prefissi per EC2 Instance Connect.

Ad esempio, se la tua istanza si trova nella regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`) e gli utenti si connetteranno al relativo indirizzo IPv4 pubblico, scegli il seguente elenco di prefissi: com.amazonaws.us-east-1.ec2-instance-connect

6. Scegliere Create Security Group (Crea gruppo di sicurezza).

Visualizzazione di un'animazione: Crea il gruppo di sicurezza



Attività 3: Avvia la tua istanza

Quando avvii un'istanza, devi specificare un'AMI contenente le informazioni richieste per avviare l'istanza. Puoi scegliere di avviare un'istanza con o senza EC2 Instance Connect preinstallato. In questa attività, si specifica un'AMI preinstallata con EC2 Instance Connect.

Se avvii l'istanza senza EC2 Instance Connect preinstallato, e desideri utilizzare EC2 Instance Connect per connetterti alla tua istanza, dovrai svolgere alcuni passaggi di configurazione aggiuntivi. Tali passaggi non rientrano nell'ambito di questo tutorial.

Obiettivo dell'attività

Avvierai un'istanza con l'AMI di Amazon Linux 2023, preinstallata con EC2 Instance Connect. Specificherai anche il gruppo di sicurezza da te creato in precedenza in modo tale da poter utilizzare EC2 Instance Connect nella console Amazon EC2 per connetterti all'istanza. Poiché utilizzerai

EC2 Instance Connect per connetterti alla tua istanza, che invia una chiave pubblica ai metadati dell'istanza, non dovrai necessariamente specificare una chiave SSH all'avvio dell'istanza.

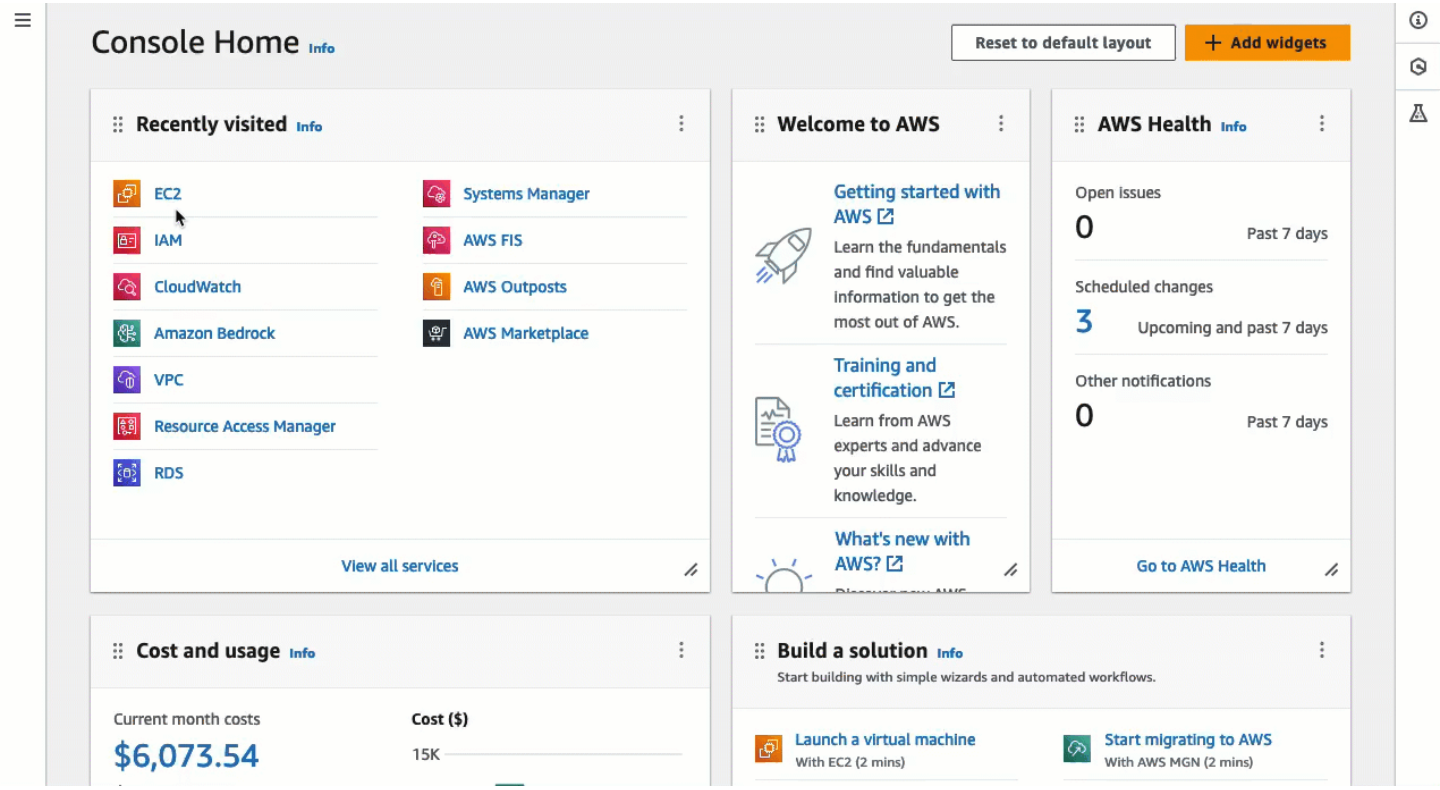
Per avviare un'istanza in grado di utilizzare EC2 Instance Connect nella console Amazon EC2 per la connessione:

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione nella parte superiore dello schermo, viene visualizzata la AWS regione corrente (ad esempio, Irlanda). Seleziona una regione in cui avviare l'istanza. Questa scelta è importante perché hai creato un gruppo di sicurezza che consente il traffico per una regione specifica, quindi devi selezionare la stessa regione in cui avviare l'istanza.
3. Dal pannello di controllo della console Amazon EC2, scegli Launch Instance (Avvia istanza).
4. (Facoltativo) in Name and tags (Nome e tag), per Name (Nome), inserire un nome descrittivo per la propria istanza.
5. In Applicazioni e immagini SO (Amazon Machine Image), scegli Avvio rapido. Amazon Linux è selezionato per impostazione predefinita. In Amazon Machine Image (AMI) è selezionato AMI Amazon Linux 2023 per impostazione predefinita. Mantieni la selezione predefinita per questa attività.
6. In Tipo di istanza, per Tipo di istanza, mantieni la selezione predefinita, oppure scegli un diverso tipo di istanza.
7. In Coppia di chiavi (login), per Nome della coppia di chiavi, scegli Procedi senza una coppia di chiavi (non consigliato). Quando utilizzi EC2 Instance Connect per connetterti a un'istanza, EC2 Instance Connect invia una coppia di chiavi ai metadati dell'istanza, e questa coppia di chiavi viene utilizzata per la connessione.
8. Sotto Network settings (Impostazioni di rete) effettua le seguenti operazioni:
   a. Per l'IP Auto-assign pubblico, lascia Abilita.

      > **Note**
      >
      > Per utilizzare EC2 Instance Connect nella console Amazon EC2 per connettersi a un'istanza, l'istanza deve disporre di un indirizzo IPv4 o IPv6 pubblico.

   b. Per Firewall (gruppi di sicurezza), scegli Seleziona un gruppo di sicurezza esistente.
   c. In Gruppi di sicurezza comuni, scegli il gruppo di sicurezza da te creato in precedenza.
9. Nel pannello Summary (Riepilogo), scegliere Launch instance (Avvia istanza).

Visualizzazione di un'animazione: Avvio di un'istanza



Attività 4: Connessione all'istanza

Quando ti connetti a un'istanza tramite EC2 Instance Connect, l'API di EC2 Instance Connect invia una chiave pubblica SSH ai metadati dell'istanza, dove rimane per 60 secondi. Il daemon SSH utilizza `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` per recuperare la chiave pubblica dai metadati dell'istanza al fine effettuare l'autenticazione e ti permette di collegarti all'istanza.

Obiettivo dell'attività

In questa attività, ti connetterai alla tua istanza usando EC2 Instance Connect nella console Amazon EC2. Se hai completato le Attività preliminari 1, 2 e 3, la connessione dovrebbe avere successo.

Passaggi per connetterti alla tua istanza

Segui questi passaggi per connetterti alla tua istanza. Per visualizzare un'animazione di questi passaggi, consulta Visualizzazione di un'animazione: Connessione a un'istanza.

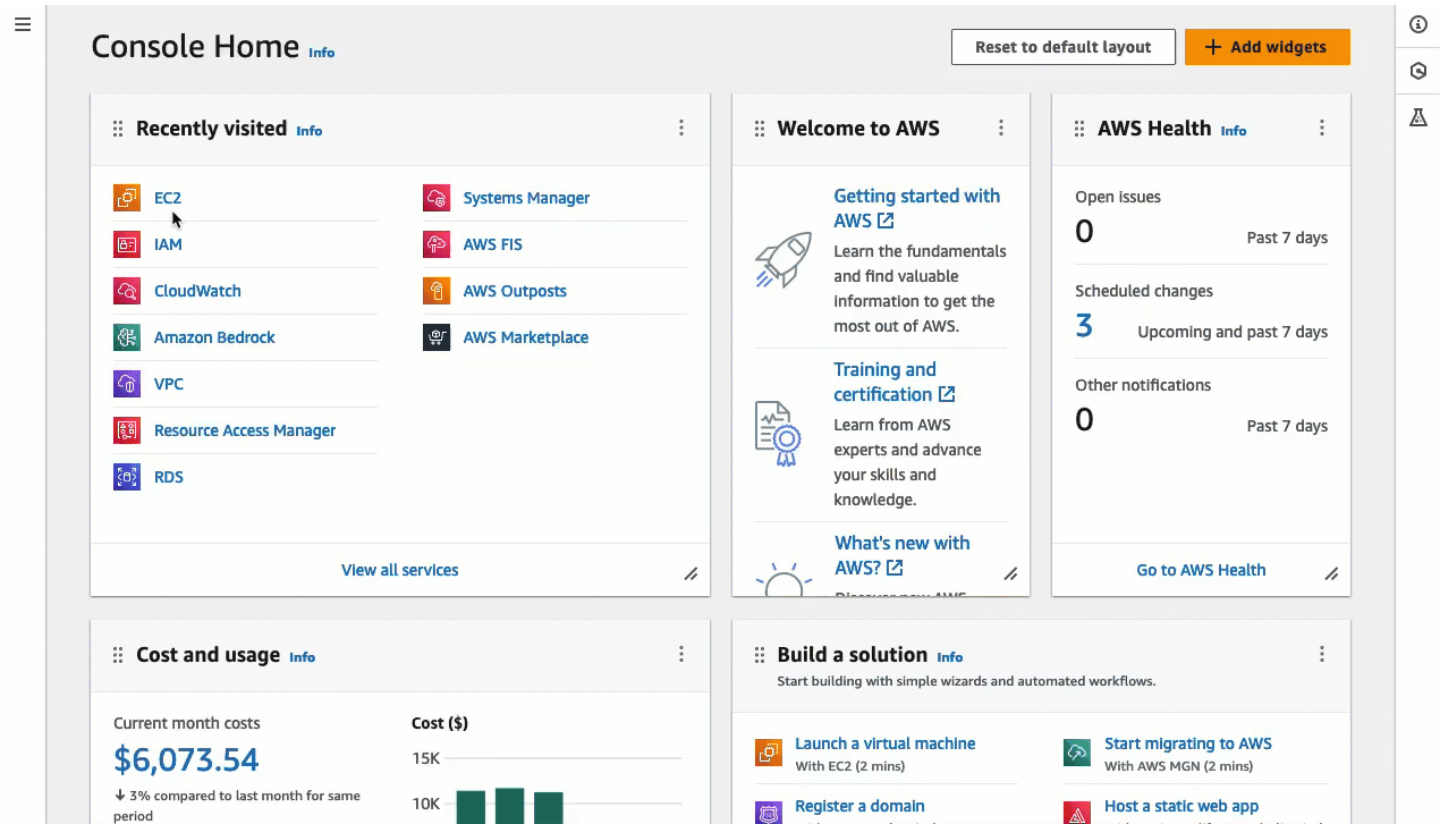
Per connetterti a un'istanza usando EC2 Instance Connect nella console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nella barra di navigazione nella parte superiore dello schermo, viene visualizzata la AWS regione corrente (ad esempio, Irlanda). Seleziona la regione in cui si trova l'istanza.
3. Nel riquadro di navigazione, scegliere Instances (Istanze).
4. Seleziona l'istanza e scegli Connetti.
5. Scegli la scheda EC2 Instance Connect.
6. Scegli Connettiti usando un IP pubblico.
7. Scegli Connetti.

   Si apre una finestra del terminale nel browser e viene stabilita la connessione all'istanza.

Visualizzazione di un'animazione: Connessione a un'istanza



Prerequisiti per EC2 Instance Connect

Di seguito sono riportati i prerequisiti per l'installazione e l'utilizzo di EC2 Instance Connect:

- Installazione di EC2 Instance Connect
- Assicurare la connettività di rete
- Consenti il traffico in uscita verso il proxy EC2 Instance Connect

- Consenti il traffico SSH in entrata
- Concessione delle autorizzazioni
- Installare un client SSH sul computer locale
- Soddisfa i requisiti del nome utente

Installazione di EC2 Instance Connect

Per utilizzare EC2 Instance Connect per connettersi a un'istanza, è necessario che EC2 Instance Connect sia installato sull'istanza. Puoi avviare l'istanza utilizzando un'AMI preinstallata con EC2 Instance Connect oppure puoi installare EC2 Instance Connect su istanze avviate con AMI supportate. Per ulteriori informazioni, consulta Installazione di EC2 Instance Connect sulle istanze EC2.

Assicurare la connettività di rete

Le istanze possono essere configurate per consentire agli utenti di connettersi all'istanza tramite Internet o tramite l'indirizzo IP privato dell'istanza. A seconda del modo in cui gli utenti si connettono all'istanza tramite EC2 Instance Connect, devi configurare il seguente accesso alla rete:

- Se gli utenti si connettono all'istanza tramite Internet, l'istanza deve avere un indirizzo IPv4 o IPv6 pubblico e trovarsi in una sottorete pubblica con una route a Internet. Se non hai modificato la sottorete pubblica predefinita, questa contiene una route a Internet solo per IPv4 e non per IPv6. Per ulteriori informazioni, consulta Permetti l'accesso a Internet VPC tramite gateway Internet nella Guida per l'utente di Amazon VPC.
- Se gli utenti si connetteranno alla tua istanza tramite l'indirizzo IPv4 privato dell'istanza, devi stabilire una connettività di rete privata al tuo VPC, ad esempio utilizzando, o il peering VPC AWS Direct Connect AWS Site-to-Site VPN, in modo che gli utenti possano raggiungere l'indirizzo IP privato dell'istanza.

Se la tua istanza non dispone di un indirizzo IPv4 o IPv6 pubblico e preferisci non configurare l'accesso alla rete come descritto sopra, puoi considerare l'endpoint EC2 Instance Connect come alternativa a EC2 Instance Connect. Con EC2 Instance Connect Endpoint, puoi connetterti a un'istanza tramite SSH o RDP anche se l'istanza non dispone di un indirizzo IPv4 o IPv6 pubblico. Per ulteriori informazioni, consulta Connessione a un'istanza Linux tramite la console Amazon EC2.

Consenti il traffico in uscita verso il proxy EC2 Instance Connect

Quando ti connetti a un'istanza utilizzando la console Amazon EC2, il browser stabilisce una WebSocket connessione sulla porta 443 al servizio proxy EC2 Instance Connect su un endpoint. Region-specific

Il formato dell'endpoint dipende dalla partizione: https://docs.aws.amazon.com/glossary/latest/reference/glos-chap.html#partition

- Le regioni AWS commerciali e le regioni AWS GovCloud (Stati Uniti) utilizzano il formato degli endpoint:. `prod.region.oneclickv2-proxy.ec2.aws.dev`
- Le regioni cinesi utilizzano il formato degli endpoint:. `prod.region.oneclickv2-proxy.ec2.a2z.org.cn`

Gli esempi seguenti mostrano l'endpoint per ogni partizione:

- Per la regione Stati Uniti orientali (Virginia settentrionale), l'endpoint è. `prod.us-east-1.oneclickv2-proxy.ec2.aws.dev`
- Per la regione Cina (Pechino), l'endpoint è. `prod.cn-north-1.oneclickv2-proxy.ec2.a2z.org.cn`

> **Note**
>
> Il browser deve essere in grado di raggiungere questo endpoint. Se un firewall o una VPN bloccano la connessione, la connessione fallisce.

Consenti il traffico SSH in entrata

Quando utilizzi una console Amazon EC2 per connetterti a un'istanza

Quando gli utenti si connettono a un'istanza usando la console Amazon EC2, il traffico a cui deve essere consentito di raggiungere l'istanza è il traffico proveniente dal servizio EC2 Instance Connect. Il servizio è identificato da intervalli di indirizzi IP specifici, AWS gestiti tramite elenchi di prefissi. Devi creare un gruppo di sicurezza che consenta il traffico SSH in entrata dal servizio EC2 Instance Connect. Per configurarlo, per la regola in entrata, nel campo accanto a Origine, seleziona l'elenco dei prefissi per EC2 Instance Connect.

AWS fornisce diversi elenchi di prefissi gestiti per gli indirizzi IPv4 e IPv6 per ciascuna regione. I nomi degli elenchi di prefissi di EC2 Instance Connect sono i seguenti, sostituiti dal codice regionale: *region*

- Nome dell'elenco di prefissi IPv4: `com.amazonaws.region.ec2-instance-connect`
- Nome dell'elenco di prefissi IPv6: `com.amazonaws.region.ipv6.ec2-instance-connect`

Per le istruzioni per la creazione del gruppo di sicurezza, consulta Attività 2: Consenti il traffico in entrata dal servizio EC2 Instance Connect all'istanza in uso. Per ulteriori informazioni, consulta gli elenchi di prefissi AWS gestiti disponibili nella Amazon VPC User Guide.

Quando utilizzi la CLI o SSH per connetterti a un'istanza

Verificare che il gruppo di sicurezza associato all'istanza consenta il traffico SSH in entrata dalla porta 22 dell'indirizzo IP o dalla rete. Per impostazione predefinita, il gruppo di sicurezza predefinito per il VPC non consente il traffico SSH in entrata. Per impostazione predefinita, il gruppo di sicurezza creato dalla procedura guidata di avvio dell'istanza abilita il traffico SSH. Per ulteriori informazioni, consulta Regole per la connessione alle istanze dal computer in uso.

Concessione delle autorizzazioni

Devi concedere le autorizzazioni richieste a tutti gli utenti IAM che utilizzano EC2 Instance Connect per connettersi a un'istanza. Per ulteriori informazioni, consulta Concessione di un'autorizzazione IAM per EC2 Instance Connect.

Installare un client SSH sul computer locale

Se gli utenti si connettono tramite SSH, devono assicurarsi che il loro computer locale disponga di un client SSH.

Il computer locale di un utente probabilmente include un client SSH installato per impostazione predefinita. Possono verificare la presenza di un client SSH digitando ssh nella linea di comando. Se il computer locale non riconosce il comando, possono installare un client SSH. Per informazioni sull'installazione di un client SSH su Linux o macOS X, consulta. http://www.openssh.com Per informazioni sull'installazione di un client SSH in Windows 10, consulta OpenSSH in Windows.

Non è necessario installare un client SSH sul computer locale se gli utenti utilizzano la console Amazon EC2 per la connessione a un'istanza.

Soddisfa i requisiti del nome utente

Quando si utilizza EC2 Instance Connect per connettersi a un'istanza, il nome utente deve soddisfare i seguenti requisiti:

- Primo carattere: deve essere una lettera (`A-Z`, `a-z`), una cifra (`0-9`) o un carattere di sottolineatura (`_`)
- Caratteri successivi: possono essere lettere (`A-Z`, `a-z`), cifre (`0-9`) o i seguenti caratteri: `@ . _ -`
- Lunghezza minima: 1 carattere
- Lunghezza massima: 31 caratteri

Concessione di un'autorizzazione IAM per EC2 Instance Connect

Per connetterti all'istanza tramite EC2 Instance Connect, devi creare una policy IAM che concede agli utenti le autorizzazioni per le seguenti operazioni e condizioni:

- Operazione `ec2-instance-connect:SendSSHPublicKey`: concede l'autorizzazione per inviare la chiave pubblica a un'istanza.
- Condizione `ec2:osuser`: specifica il nome dell'utente del sistema operativo che può inviare la chiave pubblica a un'istanza. Utilizza il nome utente predefinito per l'AMI che è stata utilizzata per avviare l'istanza. Il nome utente predefinito per AL2023 e Amazon Linux 2 è `ec2-user` e `ubuntu` per Ubuntu.
- Operazione `ec2:DescribeInstances`: obbligatoria quando si utilizza la console EC2 perché il wrapper richiama questa operazione. Gli utenti potrebbero già disporre dell'autorizzazione per richiamare questa operazione da un'altra policy.
- Operazione `ec2:DescribeVpcs` – Obbligatoria per la connessione a un indirizzo IPv6.

Considera la possibilità di limitare l'accesso a specifiche istanze EC2. In caso contrario, tutti i principali IAM con l'autorizzazione per l'operazione `ec2-instance-connect:SendSSHPublicKey` possono connettersi a tutte le istanze EC2. Puoi limitare l'accesso specificando gli ARN delle risorse o utilizzando i tag risorsa come chiavi di condizione.

Per ulteriori informazioni, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2 Instance Connect.

Per informazioni sulla creazione di una policy IAM, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Consentire agli utenti di connettersi a istanze specifiche

La seguente policy IAM concede l'autorizzazione per connettersi a istanze specifiche, identificate dai relativi ARN delle risorse.

Nel seguente esempio di policy IAM, vengono specificate le operazioni e le condizioni seguenti:

- L'operazione `ec2-instance-connect:SendSSHPublicKey` concede agli utenti l'autorizzazione per connettersi a due istanze, specificate dagli ARN delle risorse. Per concedere agli utenti l'autorizzazione per connettersi a tutte le istanze EC2, sostituisci gli ARN della risorsa con il carattere jolly `*`.
- La `ec2:osuser` condizione concede l'autorizzazione alla connessione alle istanze solo se *`ami-username`* viene specificata al momento della connessione.
- L'operazione `ec2:DescribeInstances` è specificata per concedere l'autorizzazione agli utenti che utilizzano la console per connettersi alle tue istanze. Se gli utenti utilizzano solo un client SSH per connettersi alle istanze, puoi omettere `ec2:DescribeInstances`. Le operazioni API `ec2:Describe*` non supportano le autorizzazioni a livello di risorsa. Il carattere jolly `*` è quindi necessario nell'elemento `Resource`.
- L'operazione `ec2:DescribeVpcs` è specificata per concedere l'autorizzazione agli utenti che utilizzano la console per connettersi alle tue istanze con un indirizzo IPv6. Se i tuoi utenti utilizzeranno solo un indirizzo IPv4, puoi ometterlo `ec2:DescribeVpcs`. Le operazioni API `ec2:Describe*` non supportano le autorizzazioni a livello di risorsa. Il carattere jolly `*` è quindi necessario nell'elemento `Resource`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": [
                "arn:aws:ec2:us-
east-1:111122223333:instance/i-1234567890abcdef0",
                "arn:aws:ec2:us-east-1:111122223333:instance/i-0598c7d356eba48d7"
            ],
            "Condition": {
                "StringEquals": {
```

```
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}
```

Consentire agli utenti di connettersi alle istanze con tag specifici

Attribute-based il controllo degli accessi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base a tag che possono essere allegati a utenti e risorse. AWS Puoi utilizzare i tag delle risorse per controllare l'accesso a un'istanza. Per ulteriori informazioni sull'uso dei tag per controllare l'accesso alle AWS risorse, consulta Controlling access to AWS resources nella IAM User Guide.

Nel seguente esempio di policy IAM, l'operazione `ec2-instance-connect:SendSSHPublicKey` concede agli utenti l'autorizzazione per connettersi a qualsiasi istanza (indicata dal carattere jolly `*` nell'ARN della risorsa) a condizione che l'istanza abbia un tag di risorsa con key=`tag-key` e value=`tag-value`.

L'operazione `ec2:DescribeInstances` è specificata per concedere l'autorizzazione agli utenti che utilizzano la console per connettersi alle tue istanze. Se gli utenti utilizzano solo un client SSH per connettersi alle istanze, puoi omettere `ec2:DescribeInstances`. Le operazioni API `ec2:Describe*` non supportano le autorizzazioni a livello di risorsa. Il carattere jolly `*` è quindi necessario nell'elemento `Resource`.

L'operazione `ec2:DescribeVpcs` è specificata per concedere l'autorizzazione agli utenti che utilizzano la console per connettersi alle tue istanze con un indirizzo IPv6. Se i tuoi utenti utilizzeranno solo un indirizzo IPv4, puoi ometterlo `ec2:DescribeVpcs`. Le operazioni API `ec2:Describe*` non supportano le autorizzazioni a livello di risorsa. Il carattere jolly `*` è quindi necessario nell'elemento `Resource`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/tag-key": "tag-value"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}
```

Installazione di EC2 Instance Connect sulle istanze EC2

Per connettersi a un'istanza Linux tramite EC2 Instance Connect, è necessario che EC2 Instance Connect sia installato sull'istanza. Tramite l'installazione di EC2 Instance Connect, si configura il daemon SSH sull'istanza.

Per ulteriori informazioni sul pacchetto EC2 Instance Connect, consulta aws/aws -ec2-instance-connect-config sul sito web. GitHub

> **Note**
>
> Se hai configurato le impostazioni `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` per l'autenticazione SSH, l'installazione di EC2 Instance Connect non le aggiorna. Di conseguenza, non puoi utilizzare EC2 Instance Connect.

Prerequisiti di installazione

Prima di installare EC2 Instance Connect, assicurati di soddisfare i seguenti prerequisiti.

- Verifica che l'istanza utilizzi uno dei seguenti:
  - Amazon Linux 2 precedente alla versione 2.0.20190618 *
  - AMI ECS-optimized minima AL2023 o Amazon AMI
  - CentOS Stream 8 e 9
  - macOS Sonoma precedente a 14.2.1, Ventura precedente a 13.6.3 e Monterey precedente a 12.7.2 *
  - Red Hat Enterprise Linux (RHEL) 8 e 9
  - Ubuntu 16.04 e 18.04 *

  > **Tip**
  >
  > * Per Amazon Linux 2, macOS e Ubuntu: se hai avviato l'istanza utilizzando una versione successiva a quelle elencate sopra, EC2 Instance Connect è preinstallato e non è richiesta alcuna installazione manuale.

- Verifica i prerequisiti generali per EC2 Instance Connect.

  Per ulteriori informazioni, consulta Prerequisiti per EC2 Instance Connect.

- Verifica i prerequisiti generali per la connessione all'istanza tramite un client SSH sul tuo computer locale.

  Per ulteriori informazioni, consulta Connessione a un'istanza Linux tramite SSH.

- Ottieni l'ID dell'istanza.

  Puoi ottenere l'ID dell'istanza mediante la console Amazon EC2 (dalla colonna Instance ID [ID dell'istanza]). Se preferisci, puoi usare il comando describe-instances (AWS CLI) o (). Get-EC2Instance AWS Tools for Windows PowerShell

Installazione manuale di EC2 Instance Connect

> **Note**
>
> Se hai avviato l'istanza utilizzando una delle seguenti AMI, EC2 Instance Connect è preinstallato e puoi saltare questa procedura:
>
> - AMI standard AL2023
> - Amazon Linux 2 2.0.20190618 o versioni successive
> - macOS Sonoma 14.2.1 o versioni successive
> - macOS Ventura 13.6.3 o versioni successive
> - macOS Monterey 12.7.2 o versioni successive
> - Ubuntu 20.04 o versioni successive

Segui una di queste procedure per installare EC2 Instance Connect, a seconda del sistema operativo dell'istanza.

Amazon Linux 2

Per installare EC2 Instance Connect su un'istanza avviata tramite Amazon Linux 2

1. Connettiti all'istanza tramite SSH.

   Sostituisci i valori di esempio nel seguente comando con i tuoi. Utilizzare la coppia di chiavi SSH assegnata all'istanza al momento dell'avvio e il nome utente predefinito dell'AMI utilizzata per avviare l'istanza. Per Amazon Linux 2, il nome utente predefinito è `ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Per ulteriori informazioni sulla connessione all'istanza, consulta Connessione all'istanza Linux tramite un client SSH.
2. Installare il pacchetto EC2 Instance Connect sull'istanza.

   ```
   [ec2-user ~]$ sudo yum install ec2-instance-connect
   ```

   Verranno visualizzati tre nuovi script nella cartella `/opt/aws/bin/`:

```
eic_curl_authorized_keys
eic_parse_authorized_keys
eic_run_authorized_keys
```

3. (Opzionale) Verificare che l'installazione di EC2 Instance Connect sull'istanza sia riuscita correttamente.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config
```

EC2 Instance Connect è stato installato correttamente se le righe `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contengono i seguenti valori:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` imposta lo script `eic_run_authorized_keys` sulla ricerca delle chiavi nei metadati dell'istanza
- `AuthorizedKeysCommandUser` imposta l'utente del sistema come `ec2-instance-connect`

> **Note**
>
> Se in precedenza hai configurato `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, l'installazione di EC2 Instance Connect non modificherà i valori e non potrai utilizzare EC2 Instance Connect.

CentOS

Per installare EC2 Instance Connect su un'istanza avviata tramite CentOS

1. Connettiti all'istanza tramite SSH.

   Sostituisci i valori di esempio nel seguente comando con i tuoi. Utilizzare la coppia di chiavi SSH assegnata all'istanza al momento dell'avvio e il nome utente predefinito dell'AMI

utilizzata per avviare l'istanza. Per CentOS, il nome utente predefinito è `centos` o `ec2-user`.

```
$ ssh -i my_ec2_private_key.pem centos@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Per ulteriori informazioni sulla connessione all'istanza, consulta Connessione all'istanza Linux tramite un client SSH.

2. Se si utilizza un proxy HTTP o HTTPS, è necessario impostare l'`http_proxy`o`https_proxy`nella sessione della shell corrente.

   Se non si utilizza un proxy, questa fase può essere ignorata.

   - Per un server proxy HTTP, eseguire i comandi seguenti:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Per un server proxy HTTPS, eseguire i comandi seguenti:

     ```
     $ export http_proxy=https://hostname:port
     $ export https_proxy=https://hostname:port
     ```

3. Installare il pacchetto EC2 Instance Connect sull'istanza eseguendo i seguenti comandi.

   I file di configurazione EC2 Instance Connect per CentOS sono forniti in un pacchetto Red Hat Package Manager (RPM), con diversi pacchetti RPM per CentOS 8 e CentOS 9 e, ad esempio, tipi che funzionano su Intel/AMD (x86_64) o ARM (AArch64).

   Utilizza il blocco di comando per il tuo sistema operativo e la tua architettura della CPU.

   - CentOS 8

     Intel/AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
     west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
     connect-2.0.0-5.rhel8.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm
     ```

```
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
connect-2.0.0-5.rhel8.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- CentOS 9

  Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
connect-2.0.0-5.rhel9.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

  ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
```

```
connect-2.0.0-5.rhel9.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Verrà visualizzato il seguente nuovo script nella cartella `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opzionale) Verificare che l'installazione di EC2 Instance Connect sull'istanza sia riuscita correttamente.

   - Per CentOS 8:

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/sshd.service.d/ec2-instance-
     connect.conf
     ```

   - Per CentOS 9:

     ```
     [ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
     ```

   EC2 Instance Connect è stato installato correttamente se le righe `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contengono i seguenti valori:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

   - `AuthorizedKeysCommand` imposta lo script `eic_run_authorized_keys` sulla ricerca delle chiavi nei metadati dell'istanza
   - `AuthorizedKeysCommandUser` imposta l'utente del sistema come `ec2-instance-connect`

> **Note**
>
> Se in precedenza hai configurato `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, l'installazione di EC2 Instance Connect non modificherà i valori e non potrai utilizzare EC2 Instance Connect.

macOS

Per installare EC2 Instance Connect su un'istanza avviata tramite macOS

1. Connettiti all'istanza tramite SSH.

   Sostituisci i valori di esempio nel seguente comando con i tuoi. Utilizzare la coppia di chiavi SSH assegnata all'istanza al momento dell'avvio e il nome utente predefinito dell'AMI utilizzata per avviare l'istanza. Per le istanze macOS, il nome utente predefinito è `ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Per ulteriori informazioni sulla connessione all'istanza, consulta Connessione all'istanza Linux tramite un client SSH.

2. Aggiornare Homebrew utilizzando il seguente comando. L'aggiornamento elencherà i software conosciuti da Homebrew. Il pacchetto EC2 Instance Connect viene fornito tramite Homebrew sulle istanze macOS. Per ulteriori informazioni, consulta Aggiornamento del sistema operativo e il software per le istanze Mac di Amazon EC2.

   ```
   [ec2-user ~]$ brew update
   ```

3. Installare il pacchetto EC2 Instance Connect sull'istanza. In questo modo il software verrà installato e configurato per essere utilizzato da sshd.

   ```
   [ec2-user ~]$ brew install ec2-instance-connect
   ```

   Verrà visualizzato il seguente nuovo script nella cartella `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opzionale) Verificare che l'installazione di EC2 Instance Connect sull'istanza sia riuscita correttamente.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect è stato installato correttamente se le righe `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contengono i seguenti valori:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` imposta lo script `eic_run_authorized_keys` sulla ricerca delle chiavi nei metadati dell'istanza
- `AuthorizedKeysCommandUser` imposta l'utente del sistema come `ec2-instance-connect`

> **Note**
>
> Se in precedenza hai configurato `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, l'installazione di EC2 Instance Connect non modificherà i valori e non potrai utilizzare EC2 Instance Connect.

RHEL

Per installare EC2 Instance Connect su un'istanza avviata tramite Red Hat Enterprise Linux (RHEL)

1. Connettiti all'istanza tramite SSH.

Sostituisci i valori di esempio nel seguente comando con i tuoi. Utilizzare la coppia di chiavi SSH assegnata all'istanza al momento dell'avvio e il nome utente predefinito dell'AMI utilizzata per avviare l'istanza. Per RHEL, il nome utente predefinito è `ec2-user` o `root`.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Per ulteriori informazioni sulla connessione all'istanza, consulta Connessione all'istanza Linux tramite un client SSH.

2. Se si utilizza un proxy HTTP o HTTPS, è necessario impostare l'`http_proxy`o`https_proxy`nella sessione della shell corrente.

   Se non si utilizza un proxy, questa fase può essere ignorata.

   - Per un server proxy HTTP, eseguire i comandi seguenti:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Per un server proxy HTTPS, eseguire i comandi seguenti:

     ```
     $ export http_proxy=https://hostname:port
     $ export https_proxy=https://hostname:port
     ```

3. Installare il pacchetto EC2 Instance Connect sull'istanza eseguendo i seguenti comandi.

   I file di configurazione EC2 Instance Connect per RHEL sono forniti in un pacchetto Red Hat Package Manager (RPM), con diversi pacchetti RPM per RHEL 8 e RHEL 9 e per tipi di istanza eseguiti su Intel/AMD (x86_64) o ARM (AArch64).

   Utilizza il blocco di comando per il tuo sistema operativo e la tua architettura della CPU.

   - RHEL 8

     Intel/AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
     west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
     connect-2.0.0-5.rhel8.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
     ```

```
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
connect-2.0.0-5.rhel8.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- RHEL 9

  Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
connect-2.0.0-5.rhel9.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

  ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
connect-2.0.0-5.rhel9.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
connect.rpm
```

```
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Verrà visualizzato il seguente nuovo script nella cartella `/opt/aws/bin/`:

```
eic_run_authorized_keys
```

4. (Opzionale) Verificare che l'installazione di EC2 Instance Connect sull'istanza sia riuscita correttamente.

   - Per RHEL 8:

     ```
     [ec2-user ~]$ sudo less /lib/systemd/system/sshd.service.d/ec2-instance-
     connect.conf
     ```

   - Per RHEL 9:

     ```
     [ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
     ```

   EC2 Instance Connect è stato installato correttamente se le righe `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contengono i seguenti valori:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

   - `AuthorizedKeysCommand` imposta lo script `eic_run_authorized_keys` sulla ricerca delle chiavi nei metadati dell'istanza
   - `AuthorizedKeysCommandUser` imposta l'utente del sistema come `ec2-instance-connect`

> **Note**
>
> Se in precedenza hai configurato `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, l'installazione di EC2 Instance Connect non modificherà i valori e non potrai utilizzare EC2 Instance Connect.

Ubuntu

Per installare EC2 Instance Connect su un'istanza avviata con Ubuntu 16.04 o versioni successive

1. Connettiti all'istanza tramite SSH.

   Sostituisci i valori di esempio nel seguente comando con i tuoi. Utilizzare la coppia di chiavi SSH assegnata all'istanza al momento dell'avvio e il nome utente predefinito dell'AMI utilizzata per avviare l'istanza. Per un'AMI Ubuntu, il nome utente è `ubuntu`.

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Per ulteriori informazioni sulla connessione all'istanza, consulta Connessione all'istanza Linux tramite un client SSH.

2. (Opzionale) Verificare che l'istanza disponga dell'AMI Ubuntu più recente.

   Eseguire i seguenti comandi per aggiornare tutti i pacchetti dell'istanza.

   ```
   ubuntu:~$ sudo apt-get update
   ```

   ```
   ubuntu:~$ sudo apt-get upgrade
   ```

3. Installare il pacchetto EC2 Instance Connect sull'istanza.

   ```
   ubuntu:~$ sudo apt-get install ec2-instance-connect
   ```

   Verranno visualizzati tre nuovi script nella cartella `/usr/share/ec2-instance-connect/`:

```
eic_curl_authorized_keys
eic_parse_authorized_keys
eic_run_authorized_keys
```

4. (Opzionale) Verificare che l'installazione di EC2 Instance Connect sull'istanza sia riuscita correttamente.

```
ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

EC2 Instance Connect è stato installato correttamente se le righe `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` contengono i seguenti valori:

```
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys %
%u %%f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` imposta lo script `eic_run_authorized_keys` sulla ricerca delle chiavi nei metadati dell'istanza
- `AuthorizedKeysCommandUser` imposta l'utente del sistema come `ec2-instance-connect`

> **Note**
>
> Se in precedenza hai configurato `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, l'installazione di EC2 Instance Connect non modificherà i valori e non potrai utilizzare EC2 Instance Connect.

Connessione alla tua istanza Linux tramite EC2 Instance Connect

Le seguenti istruzioni spiegano come connettersi alla tua istanza Linux utilizzando EC2 Instance Connect tramite la console Amazon EC2, il AWS CLI, o un client SSH.

Quando ti connetti a un'istanza utilizzando EC2 Instance Connect tramite la console o AWS CLI, l'API EC2 Instance Connect invia automaticamente una chiave pubblica SSH ai metadati dell'istanza dove rimane per 60 secondi. Una policy IAM collegata al tuo utente autorizza questa operazione. Se

preferisci utilizzare la tua chiave SSH, puoi utilizzare un client SSH e inviare esplicitamente la tua chiave SSH all'istanza utilizzando EC2 Instance Connect.

Considerazioni

Dopo la connessione a un'istanza tramite EC2 Instance Connect, la connessione persiste fino al termine della sessione SSH. La durata di una connessione RDP non è determinata dalla durata delle credenziali IAM. Se le credenziali IAM scadono, la connessione continua a persistere. Quando utilizzi l'esperienza della console di EC2 Instance Connect, se le credenziali IAM scadono, termina la connessione chiudendo la pagina del browser. Quando utilizzi il tuo client SSH ed EC2 Instance Connect per inviare la tua chiave, puoi impostare un valore di timeout SSH per terminare automaticamente la sessione SSH.

Requisiti

Prima di iniziare, assicurati di verificare i prerequisiti.

Opzioni di connessione

- Connessione tramite la console Amazon EC2
- Connettiti usando AWS CLI
- Connessione tramite la propria chiave e un client SSH
- Risoluzione dei problemi

Connessione tramite la console Amazon EC2

Puoi connetterti a un'istanza usando EC2 Instance Connect attraverso la console Amazon EC2.

Requisiti

Per la connessione tramite la console Amazon EC2, l'istanza deve disporre di un indirizzo IPv4 o IPv6 pubblico. Se l'istanza ha solo un indirizzo IPv4 privato, puoi utilizzare ec2-instance-connect AWS CLI per connetterti.

Per connettersi a un'istanza Linux tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza, quindi scegliere Collegarsi.

4. Scegli la scheda EC2 Instance Connect.
5. Scegli Connettiti usando un IP pubblico.
6. Se c'è una scelta, seleziona l'indirizzo IP a cui connetterti. In caso contrario, l'indirizzo IP viene selezionato automaticamente.
7. Per Nome utente, verifica il nome utente.
8. Scegli Connetti per stabilire una connessione. Verrà aperta una finestra del terminale nel browser.

Connettiti usando AWS CLI

Puoi usare ec2-instance-connect AWS CLI per connetterti alla tua istanza con un client SSH. EC2 Instance Connect tenta di stabilire una connessione utilizzando un indirizzo IP disponibile in un ordine predefinito, in base al tipo di connessione specificato. Se un indirizzo IP non è disponibile, prova automaticamente il successivo nell'ordine.

Tipi di connessione

`auto` (predefinito)

EC2 Instance Connect tenta di connettersi utilizzando gli indirizzi IP dell'istanza nel seguente ordine e con il tipo di connessione corrispondente:

1. IPv4 pubblico: `direct`
2. IPv4 privato: `eice`
3. IPv6: `direct`

`direct`

EC2 Instance Connect tenta di connettersi utilizzando gli indirizzi IP dell'istanza nel seguente ordine:

1. IPv4 pubblico
2. IPv6
3. IPv4 privato (non si connette tramite un endpoint EC2 Instance Connect)

`eice`

EC2 Instance Connect tenta di connettersi utilizzando l'indirizzo IPv4 privato dell'istanza e un endpoint EC2 Instance Connect.

> **Note**
>
> In futuro, il comportamento del tipo di connessione potrebbe cambiare. `auto` Per assicurarti che venga utilizzato il tipo di connessione desiderato, imposta esplicitamente `--connection-type` su `direct` `oeice`.

Requisiti

È necessario utilizzare la AWS CLI versione 2. Per ulteriori informazioni, consulta Installazione o aggiornamento della versione più recente della AWS CLI.

Per la connessione un'istanza tramite l'ID istanza

Se conosci solo l'ID istanza e desideri che EC2 Instance Connect determini il tipo di connessione da utilizzare per connetterti all'istanza, utilizza il comando della CLI ec2-instance-connect ssh e con l'ID dell'istanza.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example
```

Per la connessione all'istanza tramite l'ID istanza e un endpoint EC2 Instance Connect

Se desideri connetterti all'istanza tramite un endpoint EC2 Instance Connect, utilizza il comando precedente e specifica anche il parametro `--connection-type` con il valore `eice`.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

Per la connessione a un'istanza utilizzando l'ID istanza e il proprio file di chiave privata

Se desideri connetterti alla tua istanza tramite un endpoint EC2 Instance Connect utilizzando la tua chiave privata, specifica l'ID istanza e il percorso del file della chiave privata. Non includere *file://* nel percorso; il seguente esempio avrà esito negativo:*file:///path/to/key*.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --private-key-file /
path/to/key.pem
```

> **Tip**
>
> Se ricevi un errore durante l'utilizzo di questi comandi, assicurati di utilizzare la AWS CLI versione 2, poiché il `ssh` comando è disponibile solo in questa versione principale. Ti

consigliamo inoltre di eseguire regolarmente l'aggiornamento all'ultima versione secondaria della versione 2 della AWS CLI per accedere alle funzionalità più recenti. Per ulteriori informazioni, consulta Informazioni sulla versione 2 della AWS CLI nella Guida per l'utente di AWS Command Line Interface .

Connessione tramite la propria chiave e un client SSH

È possibile utilizzare la propria chiave SSH e connettersi all'istanza dal client SSH preferito durante l'utilizzo dell'API EC2 Instance Connect. In questo modo è possibile sfruttare la capacità di EC2 Instance Connect di inviare una chiave pubblica all'istanza. Questo metodo di connessione funziona per istanze con indirizzi IP pubblici e privati.

Requisiti

- Requisiti delle coppie di chiavi
  - Tipi supportati: RSA (OpenSSH e SSH2) e ED25519
  - Le lunghezze supportate sono 2048 e 4096.
  - Per ulteriori informazioni, consulta Creazione di una coppia di chiavi tramite uno strumento di terza parte e importazione della chiave pubblica in Amazon EC2.
- Quando ci si connette a un'istanza che dispone solo di indirizzi IP privati, il computer locale da cui si avvia la sessione SSH deve disporre di connettività all'endpoint del servizio EC2 Instance Connect (per inviare la chiave pubblica SSH nell'istanza) nonché della connettività di rete all'indirizzo IP privato dell'istanza per stabilire la sessione SSH. L'endpoint del servizio EC2 Instance Connect è raggiungibile tramite Internet o tramite un'interfaccia virtuale Direct Connect pubblica. Per connettersi all'indirizzo IP privato dell'istanza, è possibile utilizzare servizi come Direct Connect, AWS Site-to-Site VPN o il peering VPC.

Per connettersi all'istanza tramite la propria chiave e un client SSH

1. (Opzionale) Generazione di nuove chiavi SSH private e pubbliche

   È possibile generare nuove chiavi SSH private e pubbliche, `my_key` e `my_key.pub`, utilizzando il comando seguente:

   ```
   ssh-keygen -t rsa -f my_key
   ```

2. Invio della chiave pubblica SSH all'istanza

   Utilizza il comando send-ssh-public-key per inviare la chiave pubblica SSH all'istanza. Se l'istanza è stata avviata tramite AL2023 o Amazon Linux 2, il nome utente predefinito dell'AMI è `ec2-user`. Se l'istanza è stata avviata tramite Ubuntu, il nome utente predefinito dell'AMI è `ubuntu`.

   L'esempio seguente invia la chiave pubblica all'istanza specificata nella zona di disponibilità specificata, per autenticare `ec2-user`.

   ```
   aws ec2-instance-connect send-ssh-public-key \
       --region us-west-2 \
       --availability-zone us-west-2b \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --instance-os-user ec2-user \
       --ssh-public-key file://my_key.pub
   ```

3. Connessione all'istanza tramite la chiave privata

   Utilizzare il comando ssh per connettersi all'istanza tramite la chiave privata prima che la chiave pubblica venga rimossa dai metadati dell'istanza (si dispone di un intervallo di tempo di 60 secondi). Specificare la chiave privata che corrisponde alla chiave pubblica, il nome utente predefinito per l'AMI utilizzato per avviare l'istanza e il nome DNS pubblico dell'istanza (se la connessione avviene su una rete privata, specificare il nome DNS privato o l'indirizzo IP). Aggiungi l'opzione `IdentitiesOnly=yes` per garantire che solo i file nella configurazione ssh e la chiave specificata vengano utilizzati per la connessione.

   ```
   ssh -o "IdentitiesOnly=yes" -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

   L'esempio seguente utilizza `timeout 3600` per impostare la sessione SSH in modo che termini dopo 1 ora. I processi avviati durante la sessione possono continuare a essere eseguiti sull'istanza dopo la terminazione della sessione.

   ```
   timeout 3600 ssh -o “IdentitiesOnly=yes” -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

Risoluzione dei problemi

Se ricevi un errore mentre tenti di connetterti all'istanza, consulta l'argomento seguente:

- Risoluzione dei problemi di connessione all'istanza Linux di Amazon EC2
- In che modo posso risolvere i problemi di connessione alla mia istanza EC2 utilizzando EC2 Instance Connect?

Disinstallazione di EC2 Instance Connect

Per disabilitare EC2 Instance Connect, connettiti all'istanza Linux e disinstalla il pacchetto `ec2-instance-connect` installato sul sistema operativo. Se la configurazione di `sshd` corrisponde a quella impostata al momento dell'installazione di EC2 Instance Connect, la disinstallazione di `ec2-instance-connect` rimuove anche la configurazione di `sshd`. Se la configurazione di `sshd` è stata modificata dopo l'installazione di EC2 Instance Connect, è necessario eseguire manualmente l'aggiornamento.

Amazon Linux

Puoi disinstallare EC2 Instance Connect su AL2023 e Amazon Linux 2 versione 2.0.20190618 o successiva, dove EC2 Instance Connect è preconfigurata.

Per disinstallare EC2 Instance Connect su un'istanza avviata tramite Amazon Linux

1. Connettiti all'istanza tramite SSH. Specificare la coppia di chiavi SSH utilizzata per l'istanza all'avvio e il nome utente predefinito per l'AMI Amazon Linux 2 o AL2023, ovvero `ec2-user`.

   Ad esempio, il comando ssh seguente si connette all'istanza con il nome DNS pubblico `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, utilizzando la coppia di chiavi `my_ec2_private_key.pem`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

2. Disinstallare il pacchetto `ec2-instance-connect` utilizzando il comando yum.

   ```
   [ec2-user ~]$ sudo yum remove ec2-instance-connect
   ```

Ubuntu

Per disinstallare EC2 Instance Connect su un'istanza avviata con un'AMI Ubuntu

1. Connettiti all'istanza tramite SSH. Specificare la coppia di chiavi SSH utilizzata per l'istanza all'avvio e il nome utente predefinito per l'AMI Ubuntu, ovvero `ubuntu`.

   Ad esempio, il comando ssh seguente si connette all'istanza con il nome DNS pubblico `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, utilizzando la coppia di chiavi `my_ec2_private_key.pem`.

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

2. Disinstallare il pacchetto `ec2-instance-connect` utilizzando il comando apt-get.

   ```
   ubuntu:~$ sudo apt-get remove ec2-instance-connect
   ```

Connessione alle istanze usando un indirizzo IP privato e l'endpoint EC2 Instance Connect

EC2 Instance Connect Endpoint ti consente di connetterti in modo sicuro a un'istanza da Internet, senza utilizzare un host bastione o richiedere che il tuo cloud privato virtuale (VPC) disponga di una connettività Internet diretta.

Vantaggi

- Puoi connetterti alle tue istanze senza richiedere che abbiano un indirizzo IPv4 o IPv6 pubblico. AWS addebiti per tutti gli indirizzi IPv4 pubblici, inclusi gli indirizzi IPv4 pubblici associati alle istanze in esecuzione e gli indirizzi IP elastici. Per ulteriori informazioni, consulta la scheda Public IPv4 Address sulla pagina dei prezzi di Amazon VPC.
- Puoi connetterti alle tue istanze da Internet senza che il tuo VPC disponga di una connettività Internet diretta attraverso un gateway Internet.
- Puoi controllare l'accesso alla creazione e all'uso degli endpoint EC2 Instance Connect per connetterti a istanze usando policy IAM e autorizzazioni.
- Tutti i tentativi di connessione alle istanze, riusciti e non riusciti, vengono registrati. CloudTrail

Prezzi

Non sono previsti costi aggiuntivi per l'utilizzo di endpoint EC2 Instance Connect. Se utilizzi un endpoint EC2 Instance Connect per connetterti a un'istanza in una zona di disponibilità diversa, è previsto un costo aggiuntivo per il trasferimento dei dati tra zone di disponibilità.

Indice

- Come funziona
- Considerazioni
- Concessione delle autorizzazioni per utilizzare l'endpoint EC2 Instance Connect
- Gruppi di sicurezza per l'endpoint EC2 Instance Connect
- Creazione di un endpoint EC2 Instance Connect
- Modifica un endpoint EC2 Instance Connect
- Elimina un endpoint EC2 Instance Connect
- Connessione a un'istanza Amazon EC2 tramite l'endpoint EC2 Instance Connect
- Connessioni di log stabilite tramite endpoint EC2 Instance Connect
- Service-linked ruolo per EC2 Instance Connect Endpoint
- Quote per endpoint EC2 Instance Connect

Come funziona

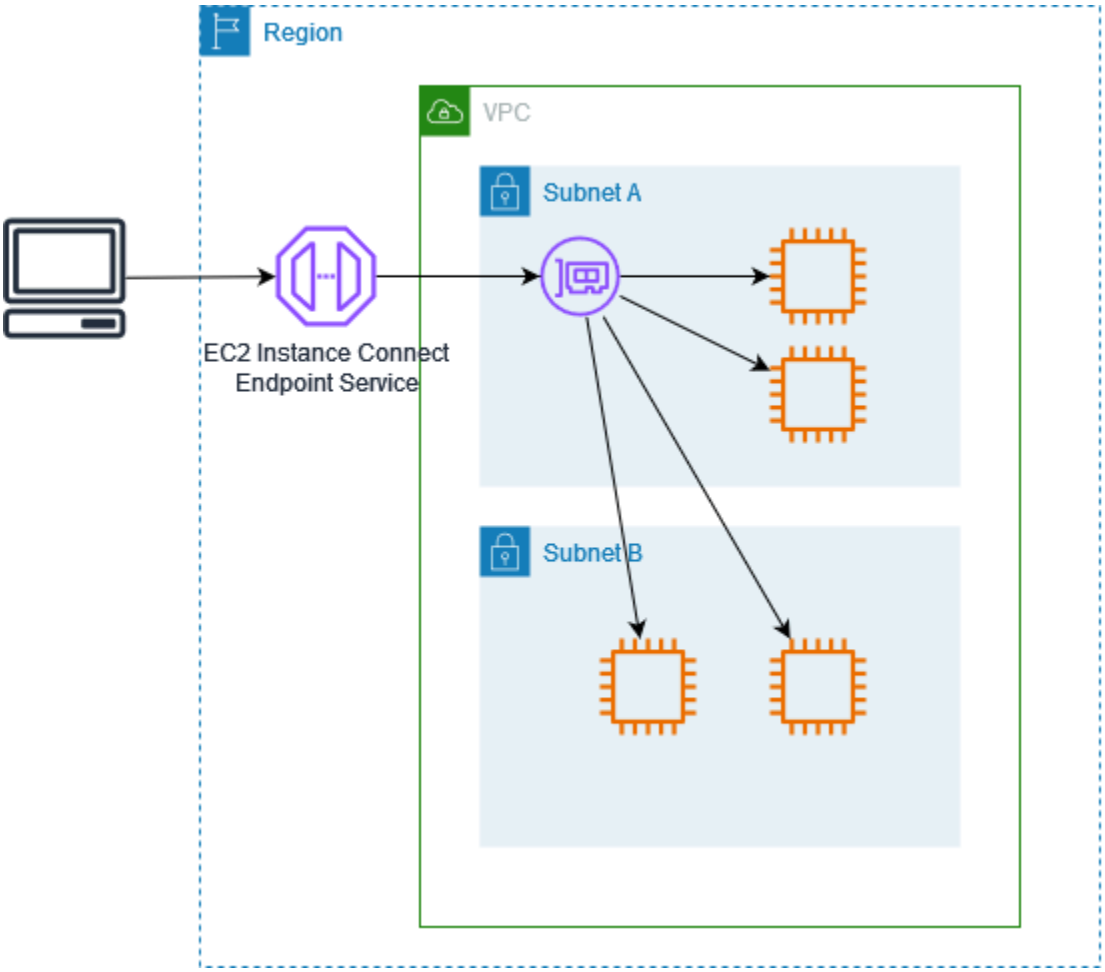
L'endpoint EC2 Instance Connect è un proxy TCP con riconoscimento dell'identità. Il servizio dell'endpoint EC2 Instance Connect stabilisce un tunnel privato dal computer all'endpoint utilizzando le credenziali per l'entità IAM. Il traffico viene autenticato e autorizzato prima di raggiungere il tuo VPC.

Puoi configurare regole aggiuntive per il gruppo di sicurezza per limitare il traffico in entrata sulle tue istanze. Ad esempio, puoi utilizzare le regole in entrata per consentire solo il traffico sulle porte di gestione dall'endpoint EC2 Instance Connect.

Puoi configurare le regole della tabella di routing per consentire all'endpoint di connettersi a qualsiasi istanza in qualsiasi sottorete del VPC.

Il seguente diagramma mostra come un utente può connettersi alle proprie istanze da Internet utilizzando un endpoint EC2 Instance Connect. Innanzitutto, crea un endpoint EC2 Instance Connect

nella sottorete A. Creiamo un'interfaccia di rete per l'endpoint nella sottorete, che funge da punto di ingresso per il traffico destinato alle tue istanze nel VPC. Se la tabella di routing per la sottorete B consente il traffico dalla sottorete A, puoi utilizzare l'endpoint per raggiungere le istanze nella sottorete B.



Considerazioni

Prima di iniziare, prendi in considerazioni le seguenti informazioni.

- L'endpoint EC2 Instance Connect è stato progettato specificamente per i casi d'uso del traffico di gestione e non per i trasferimenti di dati ad alto volume. I trasferimenti di grandi volumi di dati sono limitati.
- Puoi creare un endpoint EC2 Instance Connect per supportare il traffico verso un'istanza che dispone di un indirizzo IPv4 o IPv6 privato. Il tipo di indirizzo IP dell'endpoint deve corrispondere all'indirizzo IP dell'istanza. Puoi creare un endpoint che supporta tutti i tipi di indirizzi IP.
- (Istanze Linux) Se usi la tua coppia di chiavi, puoi usare qualsiasi AMI Linux. In caso contrario, sull'istanza deve essere installato EC2 Instance Connect. Per informazioni su quali AMI includono

EC2 Instance Connect e su come installarlo su altre AMI supportate, consulta Installazione di EC2 Instance Connect.

- Puoi assegnare un gruppo di sicurezza a un endpoint EC2 Instance Connect. In caso contrario, utilizziamo il gruppo di sicurezza predefinito per il VPC. Il gruppo di sicurezza per un endpoint EC2 Instance Connect deve consentire il traffico in uscita verso le istanze di destinazione. Per ulteriori informazioni, consulta Gruppi di sicurezza per l'endpoint EC2 Instance Connect.
- Puoi configurare un endpoint EC2 Instance Connect per preservare gli indirizzi IP di origine dei client durante il routing delle richieste verso le istanze. In caso contrario, l'indirizzo IP dell'interfaccia di rete diventa l'indirizzo IP client per tutto il traffico in entrata.
  - Se si attiva la conservazione degli IP dei client, i gruppi di sicurezza per le istanze devono consentire il traffico proveniente dai client. Inoltre, le istanze devono essere nello stesso VPC dell'endpoint EC2 Instance Connect.
  - Se si disattiva la conservazione degli IP dei client, i gruppi di sicurezza per le istanze devono consentire il traffico proveniente dal PVC. Questa è l'impostazione predefinita.
  - La conservazione dell'IP del client è supportata soltanto sugli endpoint EC2 Instance Connect di IPv4. Per utilizzare la conservazione dell'IP del client, il tipo di indirizzo IP dell'endpoint EC2 Instance Connect deve essere IPv4. La conservazione dell'IP del client non è supportata quando il tipo di indirizzo IP è dual-stack o IPv6.
  - I seguenti tipi di istanza non supportano la conservazione dell'IP client: C1, CG1, CG2, G1, HI1, M1, M2, M3 e T1. Se attivi la conservazione dell'IP del client e tenti di connetterti a un'istanza con uno di questi tipi di istanza utilizzando l'endpoint EC2 Instance Connect, la connessione avrà esito negativo.
  - La conservazione dell'IP client non è supportata quando il traffico viene indirizzato attraverso un gateway di transito.
- Quando si crea un endpoint EC2 Instance Connect, viene creato automaticamente un ruolo collegato al servizio per il servizio Amazon EC2 in (IAM). AWS Identity and Access Management Amazon EC2 utilizza il ruolo collegato ai servizi per fornire interfacce di rete nell'account, necessarie per creare endpoint EC2 Instance Connect. Per ulteriori informazioni, consulta Service-linked ruolo per EC2 Instance Connect Endpoint.
- Puoi creare solo 1 endpoint EC2 Instance Connect per VPC e per sottorete. Per ulteriori informazioni, consulta Quote per endpoint EC2 Instance Connect. Se devi creare un altro endpoint EC2 Instance Connect in una zona di disponibilità diversa all'interno dello stesso VPC, devi prima eliminare l'endpoint EC2 Instance Connect esistente. In caso contrario, riceverai un errore di quota.
- Ogni endpoint EC2 Instance Connect può supportare fino a 20 connessioni simultanee.

- La durata massima per una connessione TCP stabilita e 1 ora (3.600 secondi). Puoi specificare la durata massima consentita in una policy IAM, che può essere fino a 3.600 secondi. Per ulteriori informazioni, consulta Autorizzazioni per utilizzare l'endpoint EC2 Instance Connect per connettersi alle istanze.

  La durata di una connessione RDP non è determinata dalla durata delle credenziali IAM. Se le credenziali IAM scadono, la connessione continua a persistere fino al raggiungimento della durata massima specificata. Quando ti connetti a un'istanza utilizzando l'esperienza della console dell'endpoint EC2 Instance Connect, imposta la Durata massima del tunnel (secondi) su un valore inferiore alla durata delle tue credenziali IAM. Se le tue credenziali IAM scadono presto, termina la connessione all'istanza chiudendo la pagina del browser.

Concessione delle autorizzazioni per utilizzare l'endpoint EC2 Instance Connect

Per impostazione predefinita, le entità IAM non dispongono dell'autorizzazione per creare, descrivere o modificare gli endpoint EC2 Instance Connect. Un amministratore IAM può creare policy IAM che concedono le autorizzazioni richieste per svolgere operazioni specifiche sulle risorse necessarie.

Per informazioni sulla creazione di una policy IAM, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le seguenti policy di esempio mostrano come puoi controllare le autorizzazioni disponibili per gli utenti per gli endpoint EC2 Instance Connect.

Esempi

- Autorizzazioni per creare, descrivere, modificare ed eliminare gli endpoint EC2 Instance Connect
- Autorizzazioni per utilizzare l'endpoint EC2 Instance Connect per connettersi alle istanze
- Autorizzazioni per connettersi solo da un intervallo di indirizzi IP specifici

Autorizzazioni per creare, descrivere, modificare ed eliminare gli endpoint EC2 Instance Connect

Per creare e modificare un endpoint EC2 Instance Connect, gli utenti hanno bisogno delle autorizzazioni per le seguenti operazioni:

- `ec2:CreateInstanceConnectEndpoint`
- `ec2:CreateNetworkInterface`
- `ec2:CreateTags`

- `ec2:ModifyInstanceConnectEndpoint`
- `iam:CreateServiceLinkedRole`

Per descrivere ed eliminare gli endpoint EC2 Instance Connect, gli utenti hanno bisogno delle autorizzazioni per le seguenti operazioni:

- `ec2:DescribeInstanceConnectEndpoints`
- `ec2:DeleteInstanceConnectEndpoint`

Puoi creare una policy che concede le autorizzazioni per creare, descrivere, modificare ed eliminare gli endpoint EC2 Instance Connect in tutte le sottoreti. In alternativa, puoi limitare le operazioni per le sottoreti specificate solo indicando gli ARN della sottorete come `Resource` consentita o utilizzando la chiave di condizione `ec2:SubnetID`. Puoi anche utilizzare la chiave di condizione `aws:ResourceTag` per consentire o negare esplicitamente la creazione di endpoint con determinati tag. Per ulteriori informazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.

Policy IAM di esempio

Nel seguente esempio di policy IAM, la sezione `Resource` concede l'autorizzazione per creare, modificare ed eliminare gli endpoint in tutte le sottoreti, specificati dall'asterisco (`*`). Le operazioni API `ec2:Describe*` non supportano le autorizzazioni a livello di risorsa. Il carattere jolly `*` è quindi necessario nell'elemento `Resource`.

Autorizzazioni per utilizzare l'endpoint EC2 Instance Connect per connettersi alle istanze

L'operazione `ec2-instance-connect:OpenTunnel` concede l'autorizzazione per stabilire una connessione TCP a un'istanza da connettere tramite l'endpoint EC2 Instance Connect. Puoi specificare l'endpoint EC2 Instance Connect da utilizzare. In alternativa, una `Resource` con un asterisco (`*`) consente agli utenti di utilizzare qualsiasi endpoint EC2 Instance Connect disponibile. È inoltre possibile limitare l'accesso alle istanze in base alla presenza o all'assenza di tag risorsa come chiavi di condizione.

Condizioni

- `ec2-instance-connect:remotePort` – La porta sull'istanza che può essere utilizzata per stabilire una connessione TCP. Quando viene utilizzata questa chiave di condizione, il tentativo di connessione a un'istanza su una porta diversa da quella specificata nella policy genera un errore.

- `ec2-instance-connect:privateIpAddress` – L'indirizzo IP privato di destinazione associato all'istanza con cui desideri stabilire una connessione TCP. Puoi specificare un singolo indirizzo IP, ad esempio `10.0.0.1/32` oppure un intervallo di IP tramite CIDR, ad esempio `10.0.1.0/28`. Quando viene utilizzata questa chiave di condizione, il tentativo di connessione a un'istanza con un indirizzo IP privato diverso o al di fuori dell'intervallo CIDR genera un errore.
- `ec2-instance-connect:maxTunnelDuration` – La durata massima per una connessione TCP stabilita. L'unità è in secondi e la durata varia da un minimo di 1 secondo a un massimo di 3.600 secondi (1 ora). Se la condizione non è specificata, la durata predefinita è impostata su 3.600 secondi (1 ora). Il tentativo di connessione a un'istanza per un periodo superiore alla durata specificata nella policy IAM o per un periodo superiore al valore massimo predefinito genera un errore. La connessione viene interrotta dopo la durata specificata.

  Se `maxTunnelDuration` è specificato nella policy IAM e il valore indicato è inferiore a 3.600 secondi (impostazione predefinita), devi specificare `--max-tunnel-duration` nel comando quando ti connetti a un'istanza. Per informazioni su come connettersi a un'istanza, consulta Connessione a un'istanza Amazon EC2 tramite l'endpoint EC2 Instance Connect.

Puoi anche concedere l'accesso a un utente per stabilire connessioni alle istanze in base alla presenza di tag delle risorse sull'endpoint EC2 Instance Connect. Per ulteriori informazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.

Per le istanze Linux, l'operazione `ec2-instance-connect:SendSSHPublicKey` concede l'autorizzazione per inviare la chiave pubblica a un'istanza. La condizione `ec2:osuser` specifica il nome dell'utente del sistema operativo (SO) che può inviare la chiave pubblica a un'istanza. Utilizza il nome utente predefinito per l'AMI che è stata utilizzata per avviare l'istanza. Per ulteriori informazioni, consulta Concessione di un'autorizzazione IAM per EC2 Instance Connect.

Policy IAM di esempio

Le seguenti policy IAM di esempio consentono a un principale IAM di connettersi a un'istanza utilizzando solo l'endpoint EC2 Instance Connect, identificato dall'ID endpoint `eice-123456789abcdef` specificato. La connessione viene stabilita con successo solo se tutte le condizioni sono soddisfatte.

> **Note**
>
> Le operazioni API `ec2:Describe*` non supportano le autorizzazioni a livello di risorsa. Il carattere jolly `*` è quindi necessario nell'elemento `Resource`.

Linux

Questo esempio valuta se la connessione all'istanza è stabilita sulla porta 22 (SSH), se l'indirizzo IP privato dell'istanza è compreso nell'intervallo di `10.0.1.0/31` (tra `10.0.1.0` e `10.0.1.1`) e `maxTunnelDuration` è minore o uguale a `3600` secondi. La connessione viene interrotta dopo `3600` secondi (1 ora).

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Windows

Questo esempio valuta se la connessione all'istanza è stabilita sulla porta 3389 (RDP), se l'indirizzo IP privato dell'istanza è compreso nell'intervallo di `10.0.1.0/31` (tra `10.0.1.0` e `10.0.1.1`) e `maxTunnelDuration` è minore o uguale a `3600` secondi. La connessione viene interrotta dopo `3600` secondi (1 ora).

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "3389"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
```

```
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Autorizzazioni per connettersi solo da un intervallo di indirizzi IP specifici

L'esempio seguente di policy IAM consente a un principale IAM di connettersi a un'istanza a condizione che si connetta da un indirizzo IP all'interno dell'intervallo di indirizzi IP specificato nella policy. Se il principale IAM chiama `OpenTunnel` da un indirizzo IP che non rientra in `192.0.2.0/24` (l'intervallo di indirizzi IP di esempio in questa policy), la risposta è `Access Denied`. Per ulteriori informazioni, consulta la sezione `aws:SourceIp` nella Guida per l'utente di IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "192.0.2.0/24"
                },
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                }
```

```
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

Gruppi di sicurezza per l'endpoint EC2 Instance Connect

Un gruppo di sicurezza controlla il traffico consentito per raggiungere e lasciare le risorse a cui è associato. Ad esempio, neghiamo il traffico da e verso un'istanza Amazon EC2 a meno che non sia specificamente consentito dai gruppi di sicurezza associati all'istanza.

Gli esempi seguenti mostrano come configurare le regole dei gruppi di sicurezza per l'endpoint EC2 Instance Connect e le istanze di destinazione.

Esempi

- Regole del gruppo di sicurezza per l'endpoint EC2 Instance Connect
- Regole del gruppo di sicurezza dell'istanza di destinazione

Regole del gruppo di sicurezza per l'endpoint EC2 Instance Connect

Le regole del gruppo di sicurezza per un endpoint EC2 Instance Connect devono consentire il traffico in uscita destinato alle istanze di destinazione per lasciare l'endpoint. Puoi specificare il gruppo di sicurezza dell'istanza o l'intervallo di indirizzi IPv4 o IPv6 del VPC come destinazione.

Il traffico verso l'endpoint si origina dal servizio dell'endpoint EC2 Instance Connect ed è consentito indipendentemente dalle regole in entrata per il gruppo di sicurezza degli endpoint. Per controllare chi può utilizzare un endpoint EC2 Instance Connect per connettersi a un'istanza, utilizza una policy IAM. Per ulteriori informazioni, consulta Autorizzazioni per utilizzare l'endpoint EC2 Instance Connect per connettersi alle istanze.

Regola in uscita di esempio: Riferimenti dei gruppi di sicurezza

L'esempio seguente utilizza i riferimenti dei gruppi di sicurezza, il che significa che la destinazione è un gruppo di sicurezza associato alle istanze di destinazione. Questa regola consente il traffico in uscita dall'endpoint verso tutte le istanze che utilizzano questo gruppo di sicurezza.

Protocollo	Destinazione	Intervallo porte	Comment
TCP	*ID of instance security group*	22	Consente il traffico SSH in uscita verso tutte le istanze associate al gruppo di sicurezza dell'istanza

Regola in uscita di esempio: intervallo di indirizzi IPv4

L'esempio seguente consente il traffico in uscita verso l'intervallo di indirizzi IPv4 specificato. Gli indirizzi IPv4 di un'istanza vengono assegnati dalla relativa sottorete, quindi puoi utilizzare l'intervallo di indirizzi IPv4 del VPC.

Protocollo	Destinazione	Intervallo porte	Comment
TCP	*VPC IPv4 CIDR*	22	Consente il traffico SSH in uscita verso il VPC

Esempio di regola in uscita: intervallo di indirizzi IPv6

L'esempio seguente consente il traffico in uscita verso l'intervallo di indirizzi IPv6 specificato. Gli indirizzi IPv6 di un'istanza vengono assegnati dalla relativa sottorete, quindi puoi utilizzare l'intervallo di indirizzi IPv6 del VPC.

Protocollo	Destinazione	Intervallo porte	Comment
TCP	*VPC IPv6 CIDR*	22	Consente il traffico SSH in uscita verso il VPC

Regole del gruppo di sicurezza dell'istanza di destinazione

Le regole del gruppo di sicurezza per le istanze di destinazione devono consentire il traffico in entrata dall'endpoint EC2 Instance Connect. Puoi specificare il gruppo di sicurezza dell'endpoint o un intervallo di indirizzi IPv4 o IPv6 come origine. Se specifichi un intervallo di indirizzi IPv4, l'origine dipende dal fatto che la conservazione dell'IP del client sia attivata o disattivata. Per ulteriori informazioni, consulta Considerazioni.

Poiché i gruppi di sicurezza sono stateful, il traffico di risposta può lasciare il VPC indipendentemente dalle regole in uscita per il gruppo di sicurezza dell'istanza.

Regola in entrata di esempio: Riferimenti dei gruppi di sicurezza

L'esempio seguente utilizza i riferimenti dei gruppi di sicurezza, il che significa che l'origine è il gruppo di sicurezza associato all'endpoint. Questa regola consente il traffico SSH in entrata dall'endpoint verso tutte le istanze che utilizzano questo gruppo di sicurezza, indipendentemente dal fatto che la conservazione dell'IP del client sia attivata o disattivata. Se non vi sono altre regole del gruppo di sicurezza in entrata per SSH, le istanze accettano il traffico SSH solo dall'endpoint.

Protocollo	Origine	Intervallo porte	Comment
TCP	*ID of endpoint security group*	22	Consente il traffico SSH in entrata dalle risorse associate al gruppo di sicurezza dell'endpoint

Regola in entrata di esempio: conservazione dell'IP del client disattivata

L'esempio seguente consente il traffico SSH in entrata dall'intervallo di indirizzi IPv4 specificato. Poiché la conservazione dell'IP client è disattivata, l'indirizzo IPv4 di origine è l'indirizzo dell'interfaccia di rete dell'endpoint. L'indirizzo dell'interfaccia di rete dell'endpoint viene assegnato dalla relativa sottorete, quindi puoi utilizzare l'intervallo di indirizzi IPv4 del VPC per consentire le connessioni a tutte le istanze del VPC.

Protocollo	Origine	Intervallo porte	Comment
TCP	*VPC IPv4 CIDR*	22	Consente il traffico SSH in entrata dal VPC.

Regola in entrata di esempio: conservazione dell'IP del client attivata

L'esempio seguente consente il traffico SSH in entrata dall'intervallo di indirizzi IPv4 specificato. Poiché la conservazione dell'IP client è attivata, l'indirizzo IPv4 di origine è l'indirizzo del client.

Protocollo	Origine	Intervallo porte	Comment
TCP	*Public IPv4 address range*	22	Consente il traffico in entrata dall'intervallo di indirizzi IPv4 del client specificato.

Creazione di un endpoint EC2 Instance Connect

Puoi creare un endpoint EC2 Instance Connect per consentire una connessione sicura alle tue istanze.

Considerazioni

- Sottoreti condivise: puoi creare un endpoint EC2 Instance Connect in una sottorete condivisa con te. Tuttavia, non puoi usare endpoint EC2 Instance Connect creati dal proprietario del VPC in una sottorete condivisa con te.
- Tipi di indirizzi IP: gli endpoint EC2 Instance Connect supportano i seguenti tipi di indirizzi, che devono essere compatibili con la sottorete:
  - `ipv4`: connessione a istanze EC2 solo con indirizzi IPv4 privati.
  - `dualstack`: connessione a istanze EC2 con indirizzi IPv4 o indirizzi IPv6 privati.

- `ipv6`: connessione a istanze EC2 solo con indirizzi IPv6.

Prerequisiti

Devi disporre delle autorizzazioni IAM necessarie per creare un endpoint EC2 Instance Connect. Per ulteriori informazioni, consulta Autorizzazioni per creare, descrivere, modificare ed eliminare gli endpoint EC2 Instance Connect.

Console

Come creare un endpoint EC2 Instance Connect

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Endpoints (Endpoint).
3. Scegli Crea endpoint, poi specifica le impostazioni dell'endpoint come indicato di seguito:
   a. (Facoltativo) in Tag nome, inserisci un nome per l'endpoint.
   b. Per Tipo, scegli Endpoint EC2 Instance Connect.
   c. In Impostazioni di rete, per VPC, scegli il VPC che ha le istanze di destinazione.
   d. (Facoltativo) Per conservare gli indirizzi IP dei client, espandi Impostazioni aggiuntive e seleziona la casella di spunta Conserva IP del client. In caso contrario, l'impostazione predefinita prevede l'utilizzo dell'interfaccia di rete dell'endpoint come indirizzo IP del client.

      > **Note**
      >
      > Questa opzione è disponibile solo quando il tipo di indirizzo IP dell'endpoint è configurato come IPv4.

   e. (Facoltativo) in Gruppi di sicurezza, scegli il gruppo di sicurezza da associare all'endpoint. In caso contrario, l'impostazione predefinita prevede l'utilizzo del gruppo di sicurezza predefinito per il VPC. Per ulteriori informazioni, consulta Gruppi di sicurezza per l'endpoint EC2 Instance Connect.
   f. In Sottorete, seleziona la sottorete in cui creare l'endpoint.
   g. Per Tipo di indirizzo IP, scegli il tipo di indirizzo IP per l'endpoint. Scegli Dualstack se devi supportare connessioni IPv4 e IPv6 alle tue istanze. Scegli IPv4 se devi supportare la conservazione degli IP dei client.

h. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.

4. Esaminare le impostazioni e quindi scegliere Crea endpoint.

   Lo stato iniziale dell'endpoint è In sospeso. Prima di connetterti a un'istanza utilizzando questo endpoint, devi attendere che lo stato dell'endpoint sia Disponibile. Ciò può richiedere alcuni minuti.

5. Per connetterti a un'istanza tramite il tuo endpoint, consulta Connessione a un'istanza.

AWS CLI

Come creare un endpoint EC2 Instance Connect

Utilizza il comando create-instance-connect-endpoint.

```
aws ec2 create-instance-connect-endpoint \
    --subnet-id subnet-0123456789example
```

Per specificare il tipo di traffico supportato dall'endpoint, includi il parametro `--ip-address-type`. I valori validi sono `ipv4`, `dualstack` o `ipv6`. La sottorete deve supportare il tipo di indirizzo IP specificato. Quando il parametro `--ip-address-type` viene omesso, il valore predefinito è determinato dal tipo di indirizzo IP supportato dalla sottorete.

```
aws ec2 create-instance-connect-endpoint \
    --subnet-id subnet-0123456789example \
    --ip-address-type ipv4
```

Di seguito è riportato un output di esempio.

```
{
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "create-complete",
        "StateMessage": "",
        "DnsName": "eice-0123456789example.0123abcd.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
        "FipsDnsName": "eice-0123456789example.0123abcd.fips.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
```

```
        "NetworkInterfaceIds": [
            "eni-0123abcd"
        ],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1a",
        "AvailabilityZoneId": "use1-az4",
        "CreatedAt": "2023-04-07T15:43:53.000Z",
        "SubnetId": "subnet-0123abcd",
        "PreserveClientIp": false,
        "SecurityGroupIds": [
            "sg-0123abcd"
        ],
        "Tags": [],
        "IpAddressType": "ipv4"
}
```

Per monitorare lo stato della creazione

Il valore iniziale per il campo `State` è `create-in-progress`. Prima di connetterti a un'istanza utilizzando questo endpoint, devi attendere che lo stato sia `create-complete`. Usa il comando describe-instance-connect-endpoints per monitorare lo stato dell'endpoint EC2 Instance Connect. Il parametro `--query` filtra i risultati nel campo `State`.

```
aws ec2 describe-instance-connect-endpoints --instance-connect-endpoint-
ids eice-0123456789example --query InstanceConnectEndpoints[*].State --output text
```

Di seguito è riportato un output di esempio.

```
create-complete
```

PowerShell

Per creare l'endpoint EC2 Instance Connect

Utilizza il cmdlet New-EC2InstanceConnectEndpoint.

```
New-EC2InstanceConnectEndpoint -SubnetId subnet-0123456789example
```

Per specificare il tipo di traffico supportato dall'endpoint, includi il parametro `-IpAddressType`. I valori validi sono `ipv4`, `dualstack` o `ipv6`. La sottorete deve supportare il tipo di indirizzo

IP specificato. Quando il parametro `-IpAddressType` viene omesso, il valore predefinito è determinato dal tipo di indirizzo IP supportato dalla sottorete.

```
New-EC2InstanceConnectEndpoint -SubnetId subnet-0123456789example -
IpAddressType ipv4
```

Di seguito è riportato un output di esempio.

```
OwnerId                     : 111111111111
InstanceConnectEndpointId   : eice-0123456789example
InstanceConnectEndpointArn  : arn:aws:ec2:us-east-1:111111111111:instance-connect-
endpoint/eice-0123456789example
State                       : create-complete
StateMessage                :
DnsName                     : eice-0123456789example.0123abcd.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com
FipsDnsName                 : eice-0123456789example.0123abcd.fips.ec2-instance-
connect-endpoint.us-east-1.amazonaws.com
NetworkInterfaceIds         : {eni-0123abcd}
VpcId                       : vpc-0123abcd
AvailabilityZone            : us-east-1a
AvailabilityZoneId          : use1-az4
CreatedAt                   : 4/7/2023 3:43:53 PM
SubnetId                    : subnet-0123abcd
PreserveClientIp            : False
SecurityGroupIds            : {sg-0123abcd}
Tags                        : {}
IpAddressType               : ipv4
```

Per monitorare lo stato della creazione

Il valore iniziale per il campo `State` è `create-in-progress`. Prima di connetterti a un'istanza utilizzando questo endpoint, devi attendere che lo stato sia `create-complete`. Utilizza il cmdlet Get-EC2InstanceConnectEndpoint per monitorare lo stato dell'endpoint EC2 Instance Connect. `.State.Value` filtra i risultati nel campo `State`.

```
(Get-EC2InstanceConnectEndpoint -InstanceConnectEndpointId
 "eice-0123456789example").State.Value
```

Di seguito è riportato un output di esempio.

```
create-complete
```

Modifica un endpoint EC2 Instance Connect

È possibile modificare gli endpoint EC2 Instance Connect esistenti utilizzando la console o un SDK. AWS CLI

Prima di iniziare, devi disporre delle autorizzazioni IAM richieste. Per ulteriori informazioni, consulta Autorizzazioni per creare, descrivere, modificare ed eliminare gli endpoint EC2 Instance Connect.

Parametri che puoi modificare

Puoi modificare i parametri dell'endpoint EC2 Instance Connect:

Gruppi di sicurezza

Puoi specificare nuovi gruppi di sicurezza per l'endpoint EC2 Instance Connect. I nuovi gruppi di sicurezza sostituiscono i gruppi di sicurezza attuali.

Quando si modificano i gruppi di sicurezza, devi specificare:

- Almeno un gruppo di sicurezza, anche se è solo il gruppo di sicurezza predefinito nel VPC.
- Gli ID dei gruppi di sicurezza, non i nomi.

Tipo di indirizzo IP

Puoi specificare un nuovo tipo di indirizzo IP per l'endpoint EC2 Instance Connect.

Valori validi: `ipv4` | `dualstack` | `ipv6`

Conserva l'impostazione dell'IP del client

Puoi specificare se conservare l'indirizzo IP del client come origine.

> **Note**
>
> La conservazione dell'IP del client è supportata soltanto sugli endpoint EC2 Instance Connect di IPv4. Quando si abilita `PreserveClientIp`, il tipo di indirizzo IP esistente dell'endpoint deve essere `ipv4`, oppure, se si modifica il tipo di indirizzo IP nella stessa richiesta, il nuovo valore deve essere `ipv4`.

Console

Per modificare un endpoint EC2 Instance Connect

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Endpoints (Endpoint).
3. Seleziona l'endpoint.
4. Scegli Azioni, Modifica le impostazioni degli endpoint.
5. Modifica le impostazioni degli endpoint.
6. Scegli Save changes (Salva modifiche).

   L'endpoint entra nello stato In sospeso. Al termine della modifica, l'endpoint torna allo stato Disponibile.

AWS CLI

Per modificare un endpoint EC2 Instance Connect

Utilizza il comando modify-instance-connect-endpoint e specifica l'endpoint EC2 Instance Connect e i parametri da modificare. L'esempio seguente modifica tutti i parametri in una singola richiesta.

```
aws ec2 modify-instance-connect-endpoint \
    --instance-connect-endpoint-id eice-0123456789example \
    --security-group-ids sg-0123456789example \
    --ip-address-type dualstack \
    --no-preserve-client-ip
```

Di seguito è riportato un output di esempio.

```
{
    "Return": true
}
```

Per monitorare lo stato dell'aggiornamento

Durante la modifica, lo stato dell'endpoint EC2 Instance Connect cambia in `update-in-progress`. Il processo di aggiornamento viene eseguito in modo asincrono e viene completato con uno stato `update-complete` o `update-failed`. L'endpoint utilizza la sua vecchia configurazione fino a quando lo stato non cambia a `update-complete`.

Utilizza il comando describe-instance-connect-endpoints per monitorare lo stato dell'aggiornamento. Il parametro `--query` filtra i risultati nel campo `State`.

```
aws ec2 describe-instance-connect-endpoints \
    --instance-connect-endpoint-ids eice-0123456789example \
    --query InstanceConnectEndpoints[*].State --output text
```

Di seguito è riportato un output di esempio.

```
update-complete
```

PowerShell

Per modificare un endpoint EC2 Instance Connect

Utilizza il cmdlet Edit-EC2InstanceConnectEndpoint e specifica l'endpoint EC2 Instance Connect e i parametri da modificare. L'esempio seguente modifica tutti i parametri in una singola richiesta.

```
Edit-EC2InstanceConnectEndpoint `
    -InstanceConnectEndpointId eice-0123456789example `
    -SecurityGroupIds sg-0123456789example `
    -IpAddressType dualstack `
    -PreserveClientIp $false
```

Di seguito è riportato un output di esempio.

```
True
```

Per monitorare lo stato dell'aggiornamento

Durante la modifica, lo stato dell'endpoint EC2 Instance Connect cambia in `update-in-progress`. Il processo di aggiornamento viene eseguito in modo asincrono e viene completato con uno stato `update-complete` o `update-failed`. L'endpoint utilizza la sua vecchia configurazione fino a quando lo stato non cambia a `update-complete`.

Utilizza il comando Get-EC2InstanceConnectEndpoint per monitorare lo stato dell'aggiornamento. `.State.Value` filtra i risultati nel campo `State`.

```
(Get-EC2InstanceConnectEndpoint -InstanceConnectEndpointId
 "eice-0123456789example").State.Value
```

Di seguito è riportato un output di esempio.

```
update-complete
```

Elimina un endpoint EC2 Instance Connect

Quando un endpoint EC2 Instance Connect non è più necessario, puoi eliminarlo.

Devi disporre delle autorizzazioni IAM necessarie per creare un endpoint EC2 Instance Connect. Per ulteriori informazioni, consulta Autorizzazioni per creare, descrivere, modificare ed eliminare gli endpoint EC2 Instance Connect.

Quando elimini un endpoint EC2 Instance Connect tramite la console, questo entra nello stato In eliminazione. Se l'eliminazione ha esito positivo, l'endpoint eliminato non viene più visualizzato. Se l'eliminazione ha esito negativo, lo stato è delete-failed e il Messaggio di stato fornisce il motivo dell'esito negativo.

Quando si elimina un endpoint EC2 Instance Connect utilizzando il AWS CLI, questo entra nello stato. `delete-in-progress` Se l'eliminazione ha esito positivo, entra nello stato `delete-complete`. Se l'eliminazione ha esito negativo, lo stato è `delete-failed` e `StateMessage` fornisce il motivo dell'esito negativo.

Console

Come eliminare un endpoint EC2 Instance Connect

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione a sinistra, scegli Endpoints (Endpoint).
3. Seleziona l'endpoint.
4. Seleziona Actions (Operazioni), Delete VPC endpoints (Eliminazione di endpoint VPC).
5. Quando viene richiesta la conferma, immetti **`delete`**.
6. Scegli Elimina.

AWS CLI

Per eliminare un endpoint EC2 Instance Connect

Utilizza il comando delete-instance-connect-endpoint e specifica l'ID endpoint EC2 Instance Connect da eliminare.

```
aws ec2 delete-instance-connect-endpoint --instance-connect-endpoint-
id eice-03f5e49b83924bbc7
```

Di seguito è riportato un output di esempio.

```
{
    "InstanceConnectEndpoint": {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "delete-in-progress",
        "StateMessage": "",
        "NetworkInterfaceIds": [],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1d",
        "AvailabilityZoneId": "use1-az2",
        "CreatedAt": "2023-02-07T12:05:37+00:00",
        "SubnetId": "subnet-0123abcd"
    }
}
```

PowerShell

Come eliminare un endpoint EC2 Instance Connect

Utilizza il cmdlet Remove-EC2InstanceConnectEndpoint e specifica l'ID endpoint EC2 Instance Connect da eliminare.

```
Remove-EC2InstanceConnectEndpoint -InstanceConnectEndpointId eice-03f5e49b83924bbc7
```

Di seguito è riportato un output di esempio.

```
@{
    InstanceConnectEndpoint = @{
        OwnerId = "111111111111"
        InstanceConnectEndpointId = "eice-0123456789example"
        InstanceConnectEndpointArn = "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example"
```

```
        State = "delete-in-progress"
        StateMessage = ""
        NetworkInterfaceIds = @()
        VpcId = "vpc-0123abcd"
        AvailabilityZone = "us-east-1d"
        AvailabilityZoneId = "use1-az2"
        CreatedAt = "2023-02-07T12:05:37+00:00"
        SubnetId = "subnet-0123abcd"
    }
}
```

Connessione a un'istanza Amazon EC2 tramite l'endpoint EC2 Instance Connect

Puoi utilizzare l'endpoint EC2 Instance Connect per connetterti a un'istanza Amazon EC2 che supporta SSH o RDP.

Prerequisiti

- Devi disporre dell'autorizzazione IAM richiesta per connetterti a un endpoint EC2 Instance Connect. Per ulteriori informazioni, consulta Autorizzazioni per utilizzare l'endpoint EC2 Instance Connect per connettersi alle istanze.
- L'endpoint EC2 Instance Connect deve avere uno dei seguenti stati:
  - create-complete per un nuovo endpoint
  - update-in-progress, update-complete, oppure update-failed per la modifica di un endpoint esistente. Quando si modifica un endpoint, questo continua a utilizzare la configurazione originale fino a quando lo stato non cambia in update-complete.

    Se il VPC non dispone di un endpoint EC2 Instance Connect, potrai crearne uno. Per ulteriori informazioni, consulta Creazione di un endpoint EC2 Instance Connect.
- Il tipo di indirizzo IP dell'endpoint EC2 Instance Connect deve essere compatibile con il tipo di indirizzo IP dell'istanza. Se il tipo di indirizzo IP dell'endpoint è dual-stack, può funzionare sia per gli indirizzi IPv4 che IPv6.
- (istanze Linux) Per utilizzare la console Amazon EC2 per connettersi all'istanza o per utilizzare la CLI per connettersi e far gestire la chiave temporanea a EC2 Instance Connect, è necessario che EC2 Instance Connect sia installato sull'istanza. Per ulteriori informazioni, consulta Installazione di EC2 Instance Connect.

- Assicurati che il gruppo di sicurezza dell'istanza consenta il traffico SSH in entrata dall'endpoint EC2 Instance Connect. Per ulteriori informazioni, consulta Regole del gruppo di sicurezza dell'istanza di destinazione.

Opzioni di connessione

- Connessione a un'istanza Linux tramite la console Amazon EC2
- Connessione a un'istanza Linux tramite SSH
- Connettiti alla tua istanza Linux con il relativo ID di istanza usando AWS CLI
- Connessione all'istanza Windows con il protocollo RDP
- Risoluzione dei problemi

Connessione a un'istanza Linux tramite la console Amazon EC2

Puoi connetterti a un'istanza tramite la console Amazon EC2 (un client basato su browser) come indicato di seguito.

Per connettersi a un'istanza Linux tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza quindi scegli Connetti.
4. Scegli la scheda EC2 Instance Connect.
5. Per Tipo di connessione, scegli Connetti utilizzando un IP privato.
6. Scegli Indirizzo IPv4 privato o Indirizzo IPv6. Le opzioni sono disponibili in base agli indirizzi IP assegnati all'istanza. Se un'opzione è disattivata, l'istanza non dispone di un indirizzo IP di quel tipo assegnato a esso.
7. Per Endpoint EC2 Instance Connect, scegli l'ID dell'endpoint EC2 Instance Connect.

> **Note**
>
> L'endpoint EC2 Instance Connect deve essere compatibile con l'indirizzo IP scelto nel passaggio precedente. Se il tipo di indirizzo IP dell'endpoint è dual-stack, può funzionare sia per gli indirizzi IPv4 che IPv6. Per ulteriori informazioni, consulta Creazione di un endpoint EC2 Instance Connect.

8. Per Nome utente, se l'AMI che hai usato per avviare l'istanza utilizza un nome utente diverso da `ec2-user`, inserisci il nome utente corretto.
9. In Durata massima del tunnel (secondi), inserisci la durata massima consentita per la connessione SSH.

   La durata deve essere conforme a qualsiasi condizione `maxTunnelDuration` specificata nella policy IAM. Se non disponi dell'accesso alla policy IAM, contatta l'amministratore.
10. Scegli Connetti. Si apre una finestra del terminale per la tua istanza.

Connessione a un'istanza Linux tramite SSH

Puoi utilizzare l'SSH per connetterti all'istanza Linux e usare il comando `open-tunnel` per stabilire un tunnel privato. Puoi utilizzare il `open-tunnel` in modalità connessione singola o multipla. Puoi specificare l'ID dell'istanza, un indirizzo IPv4 privato o un indirizzo IPv6.

Per informazioni sull'utilizzo di AWS CLI per connettersi all'istanza tramite SSH, consultaConnettiti usando AWS CLI.

Nell'esempio seguente viene utilizzato OpenSSH. Puoi usare qualsiasi altro client SSH che supporti una modalità proxy.

Connessione singola

Per consentire solo una connessione singola a un'istanza utilizzando l'SSH e il comando **`open-tunnel`**

Usa `ssh` e il open-tunnel AWS CLI comando come segue. Il comando proxy `-o` racchiude il comando `open-tunnel` che crea il tunnel privato verso l'istanza.

```
ssh -i my-key-pair.pem ec2-user@i-1234567890abcdef0 \
    -o ProxyCommand='aws ec2-instance-connect open-tunnel --instance-
id i-1234567890abcdef0'
```

Per:

- `-i`: specifica la coppia di chiavi utilizzata per avviare l'istanza.
- *`ec2-user`*`@`*`i-1234567890abcdef0`*: specifica il nome utente dell'AMI utilizzata per avviare l'istanza e l'ID istanza. Per le istanze con un indirizzo IPv6, devi specificare l'indirizzo IPv6 anziché l'ID dell'istanza.

- `--instance-id`: specifica l'ID istanza a cui connetterti. In alternativa, specifica `%h` che estrae l'ID istanza dall'utente. Per le istanze con un indirizzo IPv6, sostituire `--instance-id` *`i-1234567890abcdef0`* con `--private-ip-address` *`2001:db8::1234:5678:1.2.3.4`*.

Multi-connection

Per consentire più connessioni a un'istanza, esegui prima il open-tunnel AWS CLI comando per iniziare ad ascoltare nuove connessioni TCP, quindi utilizzalo per `ssh` creare una nuova connessione TCP e un tunnel privato verso la tua istanza.

Per consentire più connessioni alla tua istanza usando SSH e il comando open-tunnel

1. Inserisci il comando seguente per avviare l'ascolto di nuove connessioni TCP sulla porta specificata del computer locale.

   ```
   aws ec2-instance-connect open-tunnel \
       --instance-id i-1234567890abcdef0 \
       --local-port 8888
   ```

   Output previsto:

   ```
   Listening for connections on port 8888.
   ```

2. In una nuova finestra del terminale, esegui il seguente comando `ssh` per creare una nuova connessione TCP e un tunnel privato verso la tua istanza.

   ```
   ssh -i my-key-pair.pem ec2-user@localhost -p 8888
   ```

   Output previsto: nella prima finestra del terminale, visualizzi le seguenti informazioni:

   ```
   [1] Accepted new tcp connection, opening websocket tunnel.
   ```

   Potresti anche visualizzare le seguenti informazioni:

   ```
   [1] Closing tcp connection.
   ```

Connettiti alla tua istanza Linux con il relativo ID di istanza usando AWS CLI

Se conosci solo l'ID della tua istanza, puoi usare il AWS CLI comando ssh ec2-instance-connect per connetterti alla tua istanza usando un client SSH. Per ulteriori informazioni, consulta Connettiti usando AWS CLI.

Prerequisiti

- Installa la AWS CLI versione 2 e configurala utilizzando le tue credenziali. Per ulteriori informazioni, consulta Installa o aggiorna la versione più recente della AWS CLI e Configura la AWS CLI nella Guida per l'utente di AWS Command Line Interface .
- In alternativa, apri AWS CloudShell ed AWS CLI esegui i comandi nella sua shell preautenticata.

Per la connessione all'istanza tramite l'ID istanza e un endpoint EC2 Instance Connect

Se conosci solo l'ID dell'istanza, utilizza il comando CLI ec2-instance-connect ssh e specifica il comando `ssh`, l'ID dell'istanza e il parametro `--connection-type` con il valore `eice` per utilizzare un endpoint EC2 Instance Connect. Se l'istanza dispone solo di un indirizzo IPv6, devi includere anche il parametro `--instance-ip` con l'indirizzo IPv6.

- Se l'istanza ha un indirizzo IPv4 privato (può avere anche un indirizzo IPv6), utilizza il comando e i parametri seguenti:

```
aws ec2-instance-connect ssh \
    --instance-id i-1234567890example \
    --os-user ec2-user \
    --connection-type eice
```

- Se l'istanza dispone solo di un indirizzo IPv6, includi il parametro `--instance-ip` con l'indirizzo IPv6:

```
aws ec2-instance-connect ssh \
    --instance-id i-1234567890example \
    --instance-ip 2001:db8::1234:5678:1.2.3.4 \
    --os-user ec2-user \
    --connection-type eice
```

> **Tip**
>
> Se ricevi un errore, assicurati di utilizzare la AWS CLI versione 2. Il `ssh` parametro è disponibile solo nella AWS CLI versione 2. Per ulteriori informazioni, consulta Informazioni sulla versione 2 della AWS CLI nella Guida per l'utente di AWS Command Line Interface .

Connessione all'istanza Windows con il protocollo RDP

Puoi utilizzare il Remote Desktop Protocol (RDP) sull'endpoint EC2 Instance Connect per connetterti a un'istanza Windows senza un indirizzo IPv4 o un nome DNS pubblici.

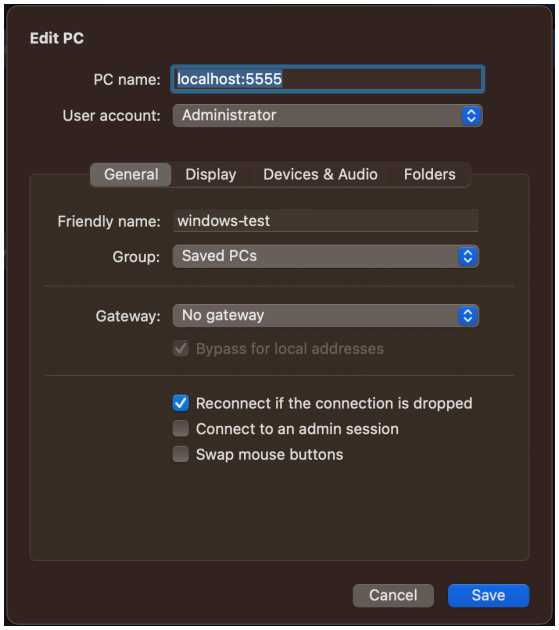
Per connetterti alla tua istanza Windows utilizzando un client RDP

1. Completa le fasi da 1 a 8 in Connessione all'istanza Windows tramite RDP. Dopo aver scaricato il file desktop RDP alla fase 8, ricevi un messaggio Impossibile connettersi, come previsto perché l'istanza non dispone di un indirizzo IP pubblico.
2. Esegui il comando seguente per stabilire un tunnel privato verso il VPC in cui si trova l'istanza. `--remote-port` deve essere `3389` perché il protocollo RDP utilizza la porta 3389 per impostazione predefinita.

   ```
   aws ec2-instance-connect open-tunnel \
       --instance-id i-1234567890abcdef0 \
       --remote-port 3389 \
       --local-port any-port
   ```

3. Nella cartella Download, trova il file desktop RDP che hai scaricato e trascinalo nella finestra del client RDP.
4. Apri il menu contestuale (clic con il pulsante destro del mouse) per il file desktop RDP e scegli Modifica.
5. Nella finestra Modifica PC, in Nome del PC (l'istanza a cui connettersi) inserisci `localhost:`*`local-port`*, in cui *`local-port`* utilizza lo stesso valore specificato nella fase 2, poi scegli Salva.

   Nota che la seguente schermata della finestra Modifica PC proviene da Microsoft Remote Desktop su un Mac. Se utilizzi un client Windows, la finestra potrebbe essere diversa.



6. Nel client RDP, apri il menu contestuale (clic con il pulsante destro del mouse) del PC (che hai appena configurato) e scegli Connetti per connetterti alla tua istanza.
7. Nel prompt, specifica la password decriptata dell'account dell'amministratore.

Risoluzione dei problemi

Utilizza le seguenti informazioni per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo dell'endpoint EC2 Instance Connect per connettere un'istanza.

Impossibile connettersi all'istanza

Di seguito sono riportati i motivi più comuni per cui potresti non essere in grado di connetterti alla tua istanza.

- Gruppi di sicurezza: controlla i gruppi di sicurezza assegnati all'endpoint EC2 Instance Connect e alla tua istanza. Per ulteriori informazioni sulle regole necessarie del gruppo di sicurezza, consulta Gruppi di sicurezza per l'endpoint EC2 Instance Connect.
- Stato dell'istanza: varica che la tua istanza abbia lo stato `running`.
- Coppia di chiavi: se il comando che stai utilizzando per la connessione richiede una chiave privata, verifica che l'istanza disponga di una chiave pubblica e di disporre della chiave privata corrispondente.
- Autorizzazioni IAM: verifica di disporre delle autorizzazioni IAM richieste. Per ulteriori informazioni, consulta Concessione delle autorizzazioni per utilizzare l'endpoint EC2 Instance Connect.

Per altri suggerimenti sulla risoluzione dei problemi per le istanze Linux, consulta Risoluzione dei problemi di connessione all'istanza Linux di Amazon EC2. Per suggerimenti sulla risoluzione dei problemi per le istanze Windows, consulta the section called "Problematiche RDP relative all'istanza Windows".

ErrorCode: AccessDeniedException

Se ricevi un errore `AccessDeniedException` e la condizione `maxTunnelDuration` è specificata nella policy IAM, assicurati di indicare il parametro `--max-tunnel-duration` quando ti connetti a un'istanza. Per ulteriori informazioni su questo parametro, consulta open-tunnel in AWS CLI Command Reference.

Connessioni di log stabilite tramite endpoint EC2 Instance Connect

È possibile registrare le operazioni sulle risorse e verificare le connessioni stabilite tramite l'endpoint EC2 Instance Connect con i log. AWS CloudTrail

Per ulteriori informazioni sull'utilizzo AWS CloudTrail con Amazon EC2, consulta. Registra le chiamate API Amazon EC2 utilizzando AWS CloudTrail

Registra le chiamate API EC2 Instance Connect Endpoint con AWS CloudTrail

Le operazioni sulle risorse di EC2 Instance Connect Endpoint vengono registrate come eventi di gestione. CloudTrail Quando vengono effettuate le seguenti chiamate API, l'attività viene registrata come CloudTrail evento nella cronologia degli eventi:

- `CreateInstanceConnectEndpoint`
- `DescribeInstanceConnectEndpoints`
- `DeleteInstanceConnectEndpoint`

Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi nella Guida AWS CloudTrail per l'utente.

Utilizzo AWS CloudTrail per controllare gli utenti che si connettono a un'istanza utilizzando EC2 Instance Connect Endpoint

I tentativi di connessione alle istanze tramite EC2 Instance Connect Endpoint vengono registrati nella cronologia degli eventi. CloudTrail Quando viene avviata una connessione a un'istanza tramite

un endpoint EC2 Instance Connect, la connessione viene registrata come evento di gestione con l'estensione of. CloudTrail `eventName` `OpenTunnel`

Puoi creare EventBridge regole Amazon che indirizzano l' CloudTrail evento a un target. Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

Di seguito è riportato un esempio di evento di `OpenTunnel` gestione a cui è stato effettuato l'accesso. CloudTrail


```
{
     "eventVersion": "1.08",
     "userIdentity": {
         "type": "IAMUser",
         "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
         "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
         "accountId": "123456789012",
         "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
         "userName": "IAM-friendly-name"
     },
     "eventTime": "2023-04-11T23:50:40Z",
     "eventSource": "ec2-instance-connect.amazonaws.com",
     "eventName": "OpenTunnel",
     "awsRegion": "us-east-1",
     "sourceIPAddress": "1.2.3.4",
     "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
     "requestParameters": {
         "instanceConnectEndpointId": "eici-0123456789EXAMPLE",
         "maxTunnelDuration": "3600",
         "remotePort": "22",
         "privateIpAddress": "10.0.1.1"
     },
     "responseElements": null,
     "requestID": "98deb2c6-3b3a-437c-a680-03c4207b6650",
     "eventID": "bbba272c-8777-43ad-91f6-c4ab1c7f96fd",
     "readOnly": false,
     "resources": [{
         "accountId": "123456789012",
         "type": "AWS::EC2::InstanceConnectEndpoint",
         "ARN": "arn:aws:ec2:us-east-1:123456789012:instance-connect-endpoint/
eici-0123456789EXAMPLE"
     }],
     "eventType": "AwsApiCall",
     "managementEvent": true,
```

```
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Service-linked ruolo per EC2 Instance Connect Endpoint

Amazon EC2 utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html#iam-term-service-linked-role Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente ad Amazon EC2. Service-linked i ruoli sono predefiniti da Amazon EC2 e includono tutte le autorizzazioni richieste da Amazon EC2 per chiamare altri per tuo conto. Servizi AWS Per ulteriori informazioni, consulta Service-linked i ruoli nella IAM User Guide.

Service-linked autorizzazioni di ruolo per EC2 Instance Connect Endpoint

Amazon EC2 utilizza AWSServiceRoleForEC2InstanceConnect per creare e gestire le interfacce di rete nel tuo account che sono richieste da EC2 Instance Connect Endpoint.

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi AWSServiceRoleForEC2InstanceConnect considera attendibile il seguente servizio:

- `ec2-instance-connect.amazonaws.com`

Il ruolo AWSServiceRoleForEC2InstanceConnect collegato al servizio utilizza la seguente policy gestita:

- Ec2InstanceConnectEndpoint

Per visualizzare le autorizzazioni per la policy gestita, consulta il Managed Policy Ec2InstanceConnectEndpoint AWS Reference.

Creazione di un ruolo collegato ai servizi per l'endpoint EC2 Instance Connect

Non è necessario creare manualmente questo ruolo collegato ai servizi. Quando si crea un endpoint EC2 Instance Connect, Amazon EC2 crea il ruolo collegato ai servizi per tuo conto.

Modifica un ruolo collegato ai servizi per l'endpoint EC2 Instance Connect

EC2 Instance Connect Endpoint non consente di modificare il AWSServiceRoleForEC2InstanceConnect ruolo collegato al servizio.

Elimina un ruolo collegato ai servizi per l'endpoint EC2 Instance Connect

Se non hai più bisogno di utilizzare EC2 Instance Connect Endpoint, ti consigliamo di eliminare il ruolo collegato al servizio. AWSServiceRoleForEC2InstanceConnect

Puoi eliminare tutte le risorse degli endpoint EC2 Instance Connect prima di eliminare il ruolo collegato ai servizi.

Per eliminare il ruolo collegato ai servizi, consulta Delete a service-linked role nella Guida per l'utente IAM.

Per consentire a un'entità IAM (un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta le autorizzazioni dei Service-linked ruoli nella IAM User Guide.

Quote per endpoint EC2 Instance Connect

Hai delle Account AWS quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota è. Region-specific

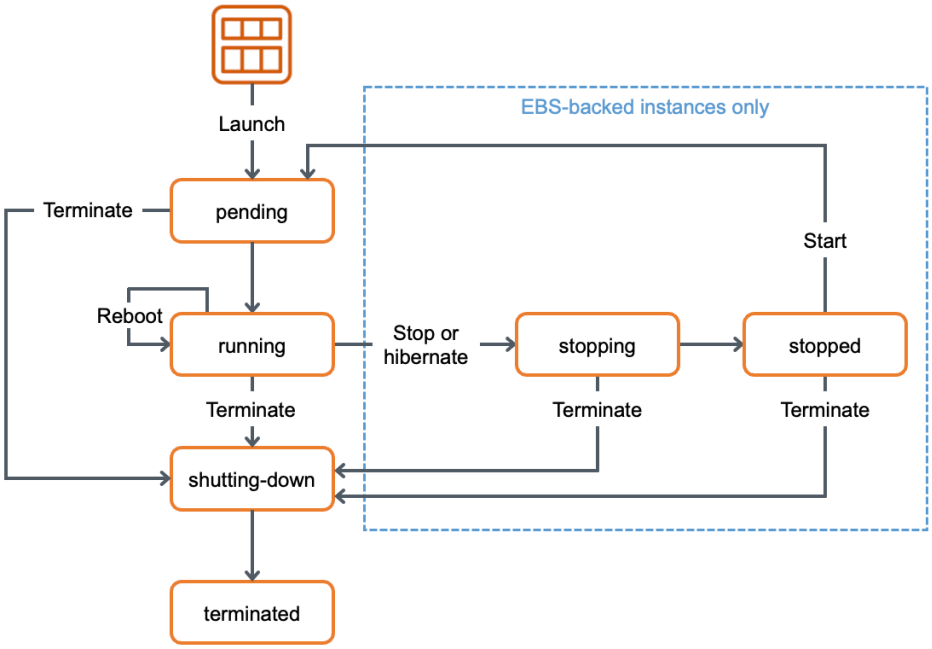
La tua Account AWS ha le seguenti quote relative a EC2 Instance Connect Endpoint.

Nome	Predefinita	Adattabile
Numero massimo di endpoint EC2 Instance Connect per Account AWS Regione AWS	5	No
Numero massimo di endpoint EC2 Instance Connect per VPC	1	No
Numero massimo di endpoint EC2 Instance Connect per sottorete	1	No
Numero massimo di connessioni simultanee per endpoint EC2 Instance Connect	20	No

Cambio di stato di un'istanza Amazon EC2

Un'istanza Amazon EC2 passa attraverso stati diversi dal momento in cui la si avvia fino alla sua terminazione.

La figura che segue rappresenta le transizioni tra gli stati di un'istanza.



Puoi continuare a ricevere notifiche quando le istanze cambiano stato. Per ulteriori informazioni, consulta the section called "Eventi di modifica dello stato".

Fatturazione per stato dell'istanza

La tabella seguente fornisce una breve descrizione di ogni stato dell'istanza e indica se questa è stata fatturata. Alcune AWS risorse, come i volumi Amazon EBS e gli indirizzi IP elastici, comportano costi indipendentemente dallo stato dell'istanza. Per ulteriori informazioni, consulta l'argomento Evitare costi inattesi nella Guida per l'utente AWS Billing .

Stato istanza	Descrizione	Fatturazione per l'utilizzo dell'istanza
`pendinc`	L'istanza si sta preparando a diventare `running`. Un'istanza assume lo stato `pending` quando viene avviata o quando viene aperta dopo che è stata `stopped`.	Non fatturato

Stato istanza	Descrizione	Fatturazione per l'utilizzo dell'istanza
`running`	L'istanza è in esecuzione e pronta per l'uso.	Fatturato
`stopping`	L'istanza si sta preparando all'arresto.	Non fatturato **Note** Se metti in ibernazione un'istanza, ti viene addebitata la fattura mentre l'istanza si trova nello stato `stopping`.
`stopped`	L'istanza è terminata e non può essere utilizzata. L'istanza può essere avviata in qualsiasi momento.	Non fatturata
`shutting-down`	L'istanza si sta preparando a essere terminata.	Non fatturata
`terminated`	L'istanza è stata eliminata definitivamente e non può essere avviata.	Non fatturata **Note** Le istanze riservate applicate a istanze terminate sono fatturate fino alla fine del loro termine in base alla loro opzione di pagamento. Per ulteriori informazioni, consulta Panoramica delle istanze riservate per Amazon EC2

Istanze in sospeso

Quando avvii un'istanza, il suo stato è `pending`. Il tipo di istanza specificato all'avvio determina l'hardware del computer host utilizzato per tale istanza. L'Amazon Machine Image (AMI) che hai specificato all'avvio viene utilizzata per avviare l'istanza. Quando l'istanza è pronta, il relativo stato diventa `running`. Puoi collegarti all'istanza in esecuzione e utilizzarla come un normale computer.

Non appena lo stato dell'istanza diventa `running`, ti verrà addebitato il costo al secondo, con un minimo di un minuto, per il tempo che l'istanza è in esecuzione, anche se inattiva e non ti colleghi a essa.

Istanze arrestate

Se l'istanza non supera il controllo dello stato oppure se non esegue le applicazioni nel modo previsto e se il volume root dell'istanza è un volume Amazon EBS, puoi arrestare e avviare l'istanza per cercare di risolvere il problema.

Quando arresti l'istanza, il relativo stato diventa `stopping` e quindi `stopped`. Non ti vengono addebitati i costi di utilizzo o di trasferimento dei dati per la tua istanza quando è `stopped`. Sono previsti costi per l'archiviazione di qualsiasi volume Amazon EBS. Quando lo stato dell'istanza è `stopped`, puoi modificare determinati attributi dell'istanza, compreso il tipo di istanza.

Una volta avviata, l'istanza entra nello stato `pending` e viene spostata su un nuovo computer host (anche se in alcuni casi, rimane sull'host corrente). Quando arresti e avvii un'istanza, perdi tutti i dati sui volumi di instance store collegati al precedente computer host.

L'istanza conserva il proprio indirizzo IPv4 privato, ovvero all'istanza continua a essere associato un indirizzo IP elastico associato all'indirizzo IPv4 privato o all'interfaccia di rete. Se l'istanza dispone di un indirizzo IPv6, conserverà il relativo indirizzo IPv6.

Ogni volta che si esegue la transizione di un'istanza da `stopped` a `running`, ti verrà addebitato un costo al secondo quando l'istanza è in esecuzione, con un minimo di un minuto per avvio di istanza.

Per ulteriori informazioni sull'arresto e sull'avvio di un'istanza, consulta Avvio e arresto di un'istanza Amazon EC2.

Istanze ibernate

Quando ibernate un'istanza, al sistema operativo viene segnalato di eseguire l'ibernazione (sospensione su disco), che salva i contenuti dalla memoria dell'istanza (RAM) nel volume principale

di Amazon EBS. Il volume radice Amazon EBS dell'istanza e tutti i volumi di dati Amazon EBS collegati vengono mantenuti. Quando avvii l'istanza, il volume root di Amazon EBS viene ripristinato allo stato precedente e i contenuti RAM vengono ricaricati. I volumi di dati precedentemente collegati vengono collegati nuovamente e l'istanza conserva il proprio ID.

Quando iberni l'istanza, il relativo stato diventa `stopping` e quindi `stopped`. Non ti viene addebitato alcun costo per l'utilizzo di un'istanza ibernata quando è nello `stopped` stato, ma ti viene addebitato mentre è nello `stopping` stato, a differenza di quando interrompi un'istanza senza ibernarla. Non ti vengono addebitati costi per il trasferimento dei dati, ma ti vengono addebitati i costi di archiviazione per qualsiasi volume Amazon EBS, incluso lo storage per i dati RAM.

Quando avvii l'istanza ibernata, questa entra `pending` nello stato e l'istanza viene spostata su un nuovo computer host (anche se in alcuni casi rimane sull'host corrente).

L'istanza conserva il proprio indirizzo IPv4 privato, ovvero all'istanza continua a essere associato un indirizzo IP elastico associato all'indirizzo IPv4 privato o all'interfaccia di rete. Se l'istanza dispone di un indirizzo IPv6, essa conserverà il relativo indirizzo IPv6.

Per ulteriori informazioni, consulta Metti in ibernazione la tua istanza Amazon EC2.

Riavvio delle istanze

Puoi riavviare l'istanza utilizzando la console Amazon EC2, uno strumento a riga di comando e l'API Amazon EC2. Ti consigliamo di utilizzare Amazon EC2 per riavviare l'istanza anziché eseguire il comando di riavvio del sistema operativo dall'interno dell'istanza.

Il riavvio di un'istanza equivale al riavvio di un sistema operativo. L'istanza rimane sullo stesso computer host e mantiene il nome DNS pubblico e l'indirizzo IP privato propri e tutti i dati presenti nei volumi instance store. Il completamento del riavvio in genere richiede pochi minuti, ma il tempo necessario dipende dalla configurazione dell'istanza.

Il reboot di un'istanza non comporta l'inizio di un nuovo periodo di fatturazione. La fatturazione al secondo continua senza un ulteriore addebito minimo di un minuto.

Per ulteriori informazioni, consulta Riavvio di un'istanza Amazon EC2.

Istanze interrotte

Se decidi che un'istanza non è più necessaria, puoi interromperla. Appena lo stato di un'istanza cambia in `shutting-down` o `terminated`, vengono bloccati i rispettivi addebiti.

Se hai abilitato la protezione da interruzione, non puoi interrompere l'istanza tramite la console, le CLI o l'API.

Dopo essere stata interrotta, un'istanza rimane visibile nella console per un breve periodo, trascorso il quale la relativa voce viene eliminata automaticamente. Puoi definire un'istanza interrotta anche tramite la CLI e l'API. Le risorse, ad esempio i tag, vengono gradualmente scollegate dall'istanza interrotta e pertanto potrebbero non risultare più visibili sull'istanza interrotta dopo un breve periodo di tempo. Non puoi collegarti a un'istanza interrotta, né recuperarla.

Ogni EBS-backed istanza Amazon supporta l'`InstanceInitiatedShutdownBehavior`attributo, che controlla se l'istanza si arresta o termina quando si avvia lo spegnimento dall'interno dell'istanza stessa (ad esempio, utilizzando il shutdown comando su Linux). Il comportamento di default prevede l'arresto dell'istanza. Puoi modificare l'impostazione di questo attributo mentre l'istanza è in esecuzione o quando è arrestata.

Ogni volume Amazon EBS supporta l'attributo `DeleteOnTermination` che controlla se il volume viene eliminato o conservato quando interrompi l'istanza a cui è collegato. Il comportamento predefinito prevede l'eliminazione del volume root e la conservazione di qualsiasi altro volume EBS.

Per ulteriori informazioni, consulta Terminare le istanze Amazon EC2.

Differenze tra gli stati dell'istanza

La tabella che segue riepiloga le principali differenze tra riavvio, arresto, ibernazione e interruzione dell'istanza.

Caratteristica	Riavvia	Stop/start (solo EBS-backed istanze Amazon)	Hibernate (solo istanze Amazon EBS-backed)	Interruzione
Computer host	L'istanza rimane sullo stesso computer host.	L'istanza viene spostata su un nuovo computer host (sebbene in alcuni casi rimanga sull'host corrente).	L'istanza viene spostata su un nuovo computer host (sebbene in alcuni casi rimanga sull'host corrente).	Nessuno

Caratteristica	Riavvia	Stop/start (solo EBS-backed istanze Amazon)	Hibernate (solo istanze Amazon EBS-backed)	Interruzione
Indirizzo IPv4 privato	L'istanza conserva il proprio indirizzo IPv4 privato.	L'istanza conserva il proprio indirizzo IPv4 privato.	L'istanza conserva il proprio indirizzo IPv4 privato.	Nessuno
Indirizzo IPv4 pubblico	L'istanza conserva il proprio indirizzo IPv4 pubblico.	All'istanza viene assegnato un nuovo indirizzo IPv4 pubblico, a meno che non abbia un'interfaccia di rete secondaria o un indirizzo IPv4 privato secondario associato a un indirizzo IP elastico.	All'istanza viene assegnato un nuovo indirizzo IPv4 pubblico, a meno che non abbia un'interfaccia di rete secondaria o un indirizzo IPv4 privato secondario associato a un indirizzo IP elastico.	Nessuno
Indirizzo IP elastico (IPv4)	L'indirizzo IP elastico rimane associato all'istanza	L'indirizzo IP elastico rimane associato all'istanza	L'indirizzo IP elastico rimane associato all'istanza	L'indirizzo IP elastico viene scollegato dall'istanza
Indirizzo IPv6	L'istanza conserva il proprio indirizzo IPv6	L'istanza conserva il proprio indirizzo IPv6	L'istanza conserva il proprio indirizzo IPv6	Nessuno
Volumi di instance store	I dati vengono conservati	I dati vengono cancellati	I dati vengono cancellati	I dati vengono cancellati

Caratteristica	Riavvia	Stop/start (solo EBS-backed istanze Amazon)	Hibernate (solo istanze Amazon EBS-backed)	Interruzione
Volume root	Il volume viene conservato	Il volume viene conservato	Il volume viene conservato	Per impostazione di default, il volume viene eliminato
RAM (contenuto della memoria)	La RAM viene cancellata	La RAM viene cancellata	La RAM viene salvata in un file nel volume root	La RAM viene cancellata
Fatturazione	La fatturazione oraria dell'istanza non cambia	Appena lo stato di un'istanza diventa `stopping`, vengono bloccati i rispettivi addebiti. Ogni volta che lo stato dell'istanza passa da `stopped` a `running`, inizia un nuovo periodo di fatturazione, con un minimo di un minuto ogni volta che l'istanza viene avviata.	Vengono addebitati dei costi mentre l'istanza è nello stato `stopping`, ma gli addebiti terminano quando l'istanza è nello stato `stopped`. Ogni volta che lo stato dell'istanza passa da `stopped` a `running`, inizia un nuovo periodo di fatturazione, con un minimo di un minuto ogni volta che l'istanza viene avviata.	Appena lo stato di un'istanza diventa `shutting-down` , vengono bloccati i rispettivi addebiti.

I comandi di chiusura del sistema operativo interrompono sempre un'istanza con un volume root dell'archivio dell'istanza. Puoi determinare se i comandi di chiusura del sistema operativo arrestano o interrompono un'istanza con un volume root EBS. Per ulteriori informazioni, consulta Modificare il comportamento di arresto avviato dall'istanza.

Avvio e arresto di un'istanza Amazon EC2

Puoi arrestare e avviare la tua istanza se provvista di un volume Amazon EBS come volume root. Quando arresti un'istanza, viene chiusa. Quando avvii un'istanza, solitamente, viene eseguita la migrazione di quest'ultima su un nuovo computer host sottostante e viene assegnato un nuovo indirizzo IPv4 pubblico.

Un arresto dell'istanza può essere avviato dall'utente (dove si arresta manualmente l'istanza) o avviato da AWS (in risposta a un evento di arresto pianificato quando AWS rileva un errore irreparabile dell'host sottostante per l'istanza).

Per gli arresti avviati dall'utente, consigliamo di utilizzare la console Amazon EC2, la CLI o l'API anziché eseguire il comando di arresto del sistema operativo dall'interno dell'istanza. Quando utilizzi Amazon EC2, se l'istanza non si arresta correttamente entro pochi minuti, Amazon EC2 esegue un arresto forzato. Inoltre, AWS CloudTrail crea un record API di quando l'istanza è stata interrotta.

Questo argomento descrive come eseguire un'arresto avviato dall'utente. Per informazioni su un arresto eseguito da AWS, consultaGestisci le istanze Amazon EC2 pianificate per l'arresto o il ritiro.

Quando interrompi un'istanza, questa non viene eliminata. Se decidi che non ti occorre più un'istanza, puoi terminarla. Per ulteriori informazioni, consulta Terminare le istanze Amazon EC2. Se desideri ibernare un'istanza per salvare il contenuto dalla memoria dell'istanza (RAM), consulta Metti in ibernazione la tua istanza Amazon EC2. Per le distinzioni tra le operazioni relative al ciclo di vita delle istanze, consultare Differenze tra gli stati dell'istanza.

Indice

- Funzionamento dell'arresto e dell'avvio dell'istanza EC2
- Metodi per arrestare un'istanza
- Arresto e avvio manuale dell'istanza
- Arrestare e avviare automaticamente le istanze
- Trova tutte le istanze in esecuzione e interrotte
- Individuazione dell'ora di avvio iniziale e di quella più recente
- Abilitazione della protezione da arresto per le istanze EC2

Funzionamento dell'arresto e dell'avvio dell'istanza EC2

Quando arresti un'istanza Amazon EC2, le modifiche sono registrate a livello di sistema operativo (OS) dell'istanza, alcune risorse sono perse e altre persistono. Quando si avvia un'istanza, le modifiche vengono registrate a livello di istanza.

Argomenti

- Cosa succede quando arresti un'istanza
- Cosa succede quando avvii un'istanza
- Testare la risposta dell'applicazione per interromperla e avviarla
- Costi relativi all'avvio e all'arresto di un'istanza

Cosa succede quando arresti un'istanza

Di seguito è descritto cosa accade in genere quando si arresta un'istanza utilizzando il metodo di arresto predefinito. Tieni presente che alcuni aspetti potrebbero variare a seconda del metodo di arresto utilizzato.

Le modifiche vengono registrate a livello di sistema operativo

- La richiesta dell'API invia un evento di pressione del pulsante al sistema guest.
- Vari servizi di sistema vengono arrestati a seguito dell'evento di pressione del pulsante. L'arresto controllato è attivato dall'evento di pressione del pulsante di arresto ACPI dall'hypervisor.
- L'arresto ACPI viene avviato.
- L'istanza è arrestata quando si esce dal processo di arresto normale OS controllato. Non c'è un orario di arresto del sistema operativo configurabile.
- Se il sistema operativo dell'istanza non si chiude correttamente entro alcuni minuti, viene eseguito un arresto forzato.
- L'esecuzione dell'istanza viene interrotta.
- Lo stato dell'istanza cambia in `stopping` e quindi in `stopped`.
- [Dimensionamento automatico] Se la tua istanza è un gruppo Auto Scaling, quando l'istanza è in qualsiasi stato dell'istanza Amazon EC2 diverso da `running` oppure se lo stato del sistema è `impaired`, Amazon EC2 Auto Scaling considera l'istanza non integra e la sostituisce. Per ulteriori informazioni, consulta Controllo dell'integrità per istanze in un gruppo Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.

- [Istanze Windows] Quando arresti e avvii un'istanza Windows, l'agente di avvio esegue delle attività, ad esempio la modifica delle lettere di unità per tutti i volumi Amazon EBS collegati. Per ulteriori informazioni su queste impostazioni predefinite e su come modificarle, consulta the section called "EC2Launch v2".

Risorse perse

- I dati archiviati nella RAM.
- I dati archiviati nei volumi dell'instance store.
- L'indirizzo IPv4 pubblico assegnato automaticamente ad Amazon EC2 all'istanza all'avvio o all'inizio. Per mantenere un indirizzo IPv4 pubblico che non cambia mai, è possibile associare un indirizzo IP elastico all'istanza.

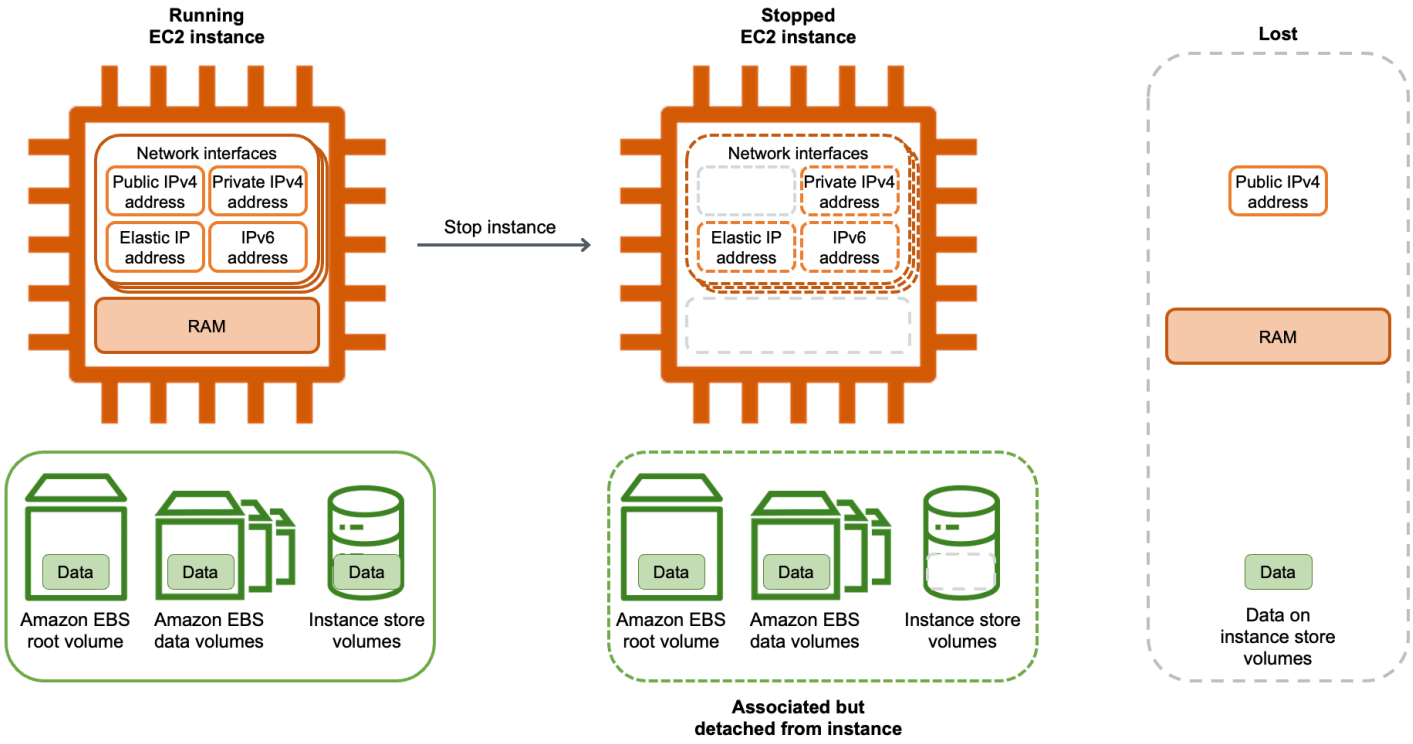
Risorse mantenute

- Qualsiasi volume Amazon EBS e volume dati collegato.
- I dati archiviati nei volumi Amazon EBS.
- Qualsiasi interfaccia di rete collegata.

  Un'interfaccia di rete include le seguenti risorse, anch'esse persistenti:

  - Gli indirizzi IPv4 privati.
  - Gli indirizzi IPv6.
  - L'indirizzo IP elastico associato all'istanza. Tieni presente che quando l'istanza viene interrotta, ti verranno addebitati i costi degli indirizzi IP elastici associati.

Il diagramma seguente mostra cosa è perso e cosa persiste quando un'istanza Amazon EC2 è arrestata. Il diagramma è diviso in tre parti: la prima parte, denominata Avvio dell'istanza EC2, mostra l'istanza nello stato `running` con le relative risorse. La seconda parte, denominata Istanza EC2 arrestata, mostra l'istanza nello stato `stopped` con le risorse che persistono. La terza parte, denominata Perse, mostra le risorse che sono perse quando l'istanza è interrotta.



Per ulteriori informazioni su cosa accade quando arresti un'istanza Mac, consulta Come terminare l'istanza Mac di Amazon EC2.

Cosa succede quando avvii un'istanza

- Nella maggior parte dei casi, l'istanza viene migrata in un nuovo computer host sottostante (sebbene in alcuni casi, come quando un'istanza è assegnata a un host in una configurazione del Host dedicato, rimanga sull'host corrente).
- I volumi EBS e le interfacce di rete associati sono ricollegati all'istanza.
- Amazon EC2 assegna un nuovo indirizzo IPv4 pubblico all'istanza se la stessa è configurata per ricevere un indirizzo IPv4 pubblico, a meno che non abbia un'interfaccia di rete secondaria o un indirizzo IPv4 privato secondario associato a un indirizzo IP elastico.
- Se arresti un'istanza in un gruppo di collocamento e poi la riavvii, quest'ultima continua a essere eseguita nel gruppo di collocamento. Tuttavia, l'avvio non riesce se non è presente capacità sufficiente per l'istanza. Se ricevete un errore di capacità quando avviate un'istanza in un gruppo di collocamento che ha già delle istanze in esecuzione, arrestate tutte le istanze del gruppo di posizionamento e riavviatele tutte. Il riavvio delle istanze potrebbe causarne la migrazione sull'hardware che dispone della capacità per tutte le istanze richieste.

Testare la risposta dell'applicazione per interromperla e avviarla

Puoi utilizzarlo AWS Fault Injection Service per verificare come risponde l'applicazione quando l'istanza viene interrotta e avviata. Per ulteriori informazioni, consulta la Guida per l'utente AWS Fault Injection Service.

Costi relativi all'avvio e all'arresto di un'istanza

I seguenti costi sono associati all'arresto e all'avvio di un'istanza.

Arresto: non appena lo stato di un'istanza cambia in `shutting-down` o `terminated`, non sono più addebitati costi per l'istanza. Non ti vengono addebitati i costi di utilizzo o di trasferimento dei dati per un'istanza arrestata. Vengono addebitati costi per archiviare i volumi di archiviazione Amazon EBS.

Avvio: ogni volta che avvii un'istanza arrestata, ti viene addebitato un minimo di un minuto per l'utilizzo. Dopo un minuto, ti vengono addebitati soli i secondi che utilizzi. Ad esempio, se esegui un'istanza per 20 secondi e poi la arresti, ti viene addebitato un minuto di utilizzo. Se esegui un'istanza per 3 minuti e 40 secondi, ti vengono addebitati 3 minuti e 40 secondi di utilizzo.

Metodi per arrestare un'istanza

Esistono quattro modi per eseguire un arresto avviato dall'utente: arresto predefinito, arresto saltando lo spegnimento dell'OS, arresto forzato e arresto forzato saltando lo spegnimento dell'OS. La tabella seguente confronta le differenze chiave tra i due metodi di arresto:

Arresto del metodo	Scopo principale	Caso d'uso	Comando della CLI
Arresto predefinito	Arresto normale dell'istanza con tentativo di spegnimento controllato del sistema operativo.	Arresto tipico dell'istanza.	`aws ec2 stop-instances \ --instance-id i-1234567890abcdef0`
Arresto saltando lo spegnime	Ignora lo spegnimento controllato del sistema operativo quando si arresta un'istanza.	Quando si ignora, è necessario lo spegnere il sistema operativo in modo controllato.	`aws ec2 stop-instances \ --instance-id i-1234567`

Arresto del metodo	Scopo principale	Caso d'uso	Comando della CLI
to del sistema operativo			890abcdef0 \ --skip-os-shutdown
Arresto forzato	Gestisce le istanze bloccate. Tenta prima un arresto predefinito; se l'istanza non viene interrotta, la arresta forzatamente.	Quando l'istanza è bloccata nello stato `stopping`.	aws ec2 stop-instances \ --instance-id i-1234567890abcdef0 \ --force
Arresto forzato saltando lo spegnimento del sistema operativo	L'attività forzata arresta e ignora lo spegnimento controllato del sistema operativo quando si arresta un'istanza.	Quando è necessario arrestare forzatamente e ignorare, lo spegnimento controllato del sistema operativo è necessario.	aws ec2 stop-instances \ --instance-id i-1234567890abcdef0 \ --force \ --skip-os-shutdown

Per istruzioni su come utilizzare ogni metodo, consulta quanto segue:

- Arresto di un'istanza con un corretto spegnimento del sistema operativo
- Arresto di un'istanza e aggiramento dello spegnimento controllato del sistema operativo
- Arresto forzato di un'istanza

Metodi di arresto:

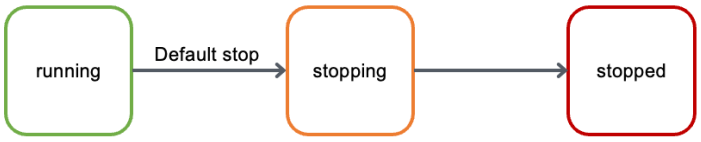
- Arresto predefinito
- Arresto saltando lo spegnimento del sistema operativo
- Arresto forzato

- Arresto forzato saltando lo spegnimento del sistema operativo

Le sezioni seguenti forniscono informazioni più dettagliate sui quattro diversi metodi di arresto avviati dall'utente.

Arresto predefinito

Il metodo di arresto predefinito è il metodo standard per arrestare un'istanza. Quando si immette il StopInstances comando, l'istanza passa dallo `running` stato, a e infine a `stoppingstopped`, come illustrato dal diagramma seguente:



Scopo: arresto normale dell'istanza con tentativo di spegnimento controllato del sistema operativo.

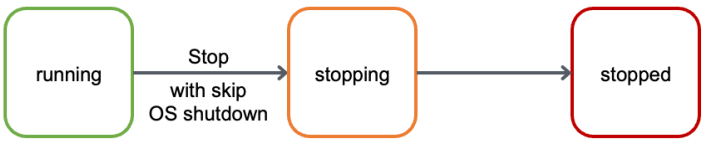
Impatto sui dati: conserva i dati sul volume root e sui volumi di dati EBS. Perdite di dati nei volumi dell'archivio dell'istanza

Quando utilizzarlo: primo tentativo di arresto per gli arresti tipici.

> **Note**
>
> Se hai già tentato un arresto saltando lo spegnimento del sistema operativo, un successivo tentativo di arresto predefinito durante la stessa sessione di transizione di stato non eseguirà un arresto controllato del sistema operativo. Ignorare lo spegnimento controllato del sistema operativo è un'operazione irreversibile per la sessione corrente dell'istanza.

Arresto saltando lo spegnimento del sistema operativo

Quando è necessario ignorare lo spegnimento controllato del sistema operativo, puoi utilizzare il metodo di arresto saltando lo spegnimento controllato del sistema operativo per arrestare un'istanza e ignorare lo spegnimento controllato del sistema operativo, come illustrato dal diagramma seguente:



> **Warning**
>
> Ignorare lo spegnimento controllato del sistema operativo potrebbe determinare la perdita o il danneggiamento dei dati (ad esempio, il mancato trasferimento del contenuto della memoria su disco o la perdita degli I/O in esecuzione) o saltare gli script di spegnimento.

Scopo: ignorare lo spegnimento controllato del sistema operativo quando si arresta un'istanza.

Impatto sui dati: potrebbe causare la perdita o il danneggiamento dei dati. Il contenuto della memoria potrebbe non essere scaricato su disco e gli I/O in esecuzione potrebbero andare persi. Potrebbe ignorare gli script di spegnimento.

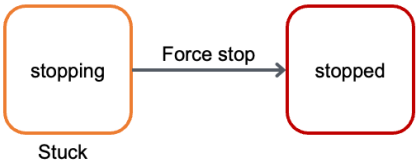
Quando utilizzarlo: quando si ignora lo spegnimento controllato del sistema operativo è necessario. Se utilizzato mentre è in corso un arresto predefinito con spegnimento controllato del sistema operativo, tale arresto controllato del sistema operativo sarà ignorato.

> **Note**
>
> Ignorare lo spegnimento controllato del sistema operativo è irreversibile per la sessione di trasferimento dello stato corrente dell'istanza. Un successivo tentativo di arresto predefinito durante questa sessione non tenterà di spegnere in modo controllato il sistema operativo.

Arresto forzato

Il metodo di arresto forzato è utilizzato per gestire le istanze bloccate nello stato `stopping`. Tipicamente, un'istanza si blocca per via di un problema hardware sottostante (indicato da una verifica dello stato del sistema non riuscita).

Il metodo di arresto forzato tenta innanzitutto un arresto predefinito. Se l'istanza rimane bloccata nello stato `stopping`, il parametro `force` spegne forzatamente l'istanza e la trasferisce allo stato `stopped`, come indicato dal diagramma seguente:



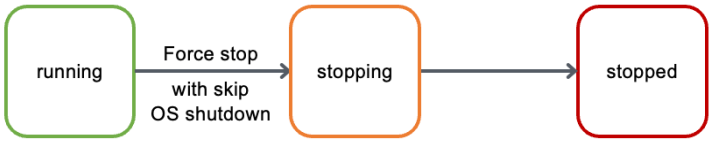
Scopo: gestisce le istanze bloccate nello stato `stopping`. Tenta prima un arresto predefinito. Se l'istanza non viene interrotta, viene arrestata in modo forzato.

Impatto sui dati: tenta prima un arresto predefinito, ma se l'arresto forzato procede, potrebbe causare la perdita o il danneggiamento dei dati. In rari casi, ciò determina operazioni di scrittura post-arresto su volumi EBS o altre risorse condivise.

Quando utilizzarlo: secondo tentativo di arresto quando un'istanza rimane bloccata dopo un arresto predefinito. Per ulteriori informazioni, consulta Risoluzione dei problemi di arresto dell'istanza Amazon EC2.

Arresto forzato saltando lo spegnimento del sistema operativo

Quando è necessario arrestare forzatamente e ignorare lo spegnimento controllato del sistema operativo, puoi utilizzare il metodo di arresto forzato saltando lo spegnimento del sistema operativo per portare un'istanza allo stato `stopped`, come illustrato nel diagramma seguente:



Scopo: combina l'arresto forzato con l'aggiramento di un arresto controllato del sistema operativo quando si arresta un'istanza.

Impatto sui dati: ignorare lo spegnimento del sistema operativo potrebbe causare la perdita o il danneggiamento dei dati. Il contenuto della memoria potrebbe non essere scaricato su disco e gli I/O in esecuzione potrebbero andare persi. Potrebbe ignorare gli script di spegnimento. Se si verifica un arresto forzato, ciò potrebbe causare un'ulteriore perdita o danneggiamento dei dati. In rari casi, ciò determina operazioni di scrittura post-arresto sui volumi EBS o altre risorse condivise.

Quando utilizzarlo: quando desideri assicurarti che l'istanza si arresti e desideri ignorare lo spegnimento controllato del sistema operativo. Se utilizzato mentre è in corso un arresto predefinito con spegnimento controllato del sistema operativo, tale arresto controllato del sistema operativo sarà ignorato.

Arresto e avvio manuale dell'istanza

Puoi interrompere e avviare le tue istanze Amazon (EBS-backed istanze con volumi root EBS). Non puoi arrestare e avviare le istanze con il volume root dell'archivio dell'istanza.

Quando si utilizza il metodo predefinito per arrestare un'istanza, si tenta di spegnere in modo corretto il sistema operativo (OS). Puoi evitare lo spegnimento controllato del sistema operativo; tuttavia, ciò potrebbe mettere a rischio l'integrità dei dati.

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'archivio dell'istanza vengono cancellati. Prima di arrestare un'istanza, verifica di aver copiato tutti i dati necessari dai volumi dell'archivio dell'istanza nell'archiviazione persistente, ad esempio Amazon EBS o Amazon S3.

[Istanze Linux] L'utilizzo del comando halt del sistema operativo da un'istanza non avvia un arresto. Se si utilizza il comando halt, l'istanza non termina, ma metterà la CPU in stato HLT, che sospende il funzionamento della CPU. L'istanza rimane in esecuzione.

Puoi avviare lo spegnimento utilizzando i comandi shutdown o poweroff del sistema operativo. Quando si utilizza un comando del sistema operativo, l'istanza si interrompe per impostazione predefinita. Puoi modificare questo comportamento. Per ulteriori informazioni, consulta Modificare il comportamento di arresto avviato dall'istanza.

> **Note**
>
> Se hai interrotto un' EBS-backed istanza Amazon e questa appare «bloccata» nello `stopping` stato, puoi fermarla forzatamente. Per ulteriori informazioni, consulta Risoluzione dei problemi di arresto dell'istanza Amazon EC2.

Metodi di arresto e avvio

- Arresto di un'istanza con un corretto spegnimento del sistema operativo
- Arresto di un'istanza e aggiramento dello spegnimento controllato del sistema operativo
- Avviare un'istanza

Arresto di un'istanza con un corretto spegnimento del sistema operativo

Puoi arrestare un'istanza utilizzando il metodo di arresto predefinito, che include un tentativo di spegnimento regolare del sistema operativo. Per ulteriori informazioni, consulta Arresto predefinito.

Console

Per arrestare un'istanza utilizzando il metodo di arresto predefinito

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione a sinistra, scegli Istanze, quindi seleziona l'istanza.
3. Scegli Instance state (Stato istanza), Stop instance (Arresta istanza). Se questa opzione è disabilitata, l'istanza è già arrestata oppure il suo volume root è un volume di archivio dell'istanza.
4. Quando viene richiesta la conferma, selezionare Stop (Arresta). Possono essere necessari alcuni minuti per arrestare l'istanza.

AWS CLI

Per arrestare un'istanza utilizzando il metodo di arresto predefinito

Utilizza il comando stop-instances.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Per arrestare un'istanza utilizzando il metodo di arresto predefinito

Usa il cmdlet Stop-EC2Instance

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0
```

Arresto di un'istanza e aggiramento dello spegnimento controllato del sistema operativo

Puoi ignorare lo spegnimento controllato del sistema operativo quando si arresta un'istanza. Per ulteriori informazioni, consulta Arresto saltando lo spegnimento del sistema operativo.

> **Warning**
>
> Ignorare lo spegnimento controllato del sistema operativo potrebbe determinare la perdita o il danneggiamento dei dati (ad esempio, il mancato trasferimento del contenuto della memoria su disco o la perdita degli I/O in esecuzione) o saltare gli script di spegnimento.

Console

Per arrestare un'istanza e ignorare lo spegnimento controllato del sistema operativo

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza.
3. Scegli Instance state (Stato istanza), Stop instance (Arresta istanza).
4. In Ignora l'arresto del sistema operativo, seleziona la casella di controllo Ignora lo spegnimento del sistema operativo. Se questa opzione non è mostrata nella console, significa che non è ancora disponibile nella console nell'attuale Regione. Tuttavia, puoi accedere a questa funzionalità utilizzando AWS CLI o SDK, o provare un'altra Regione nella console.
5. Scegli Stop (Arresta).

AWS CLI

Per arrestare un'istanza e ignorare lo spegnimento controllato del sistema operativo

Utilizza il comando stop-instances con `--skip-os-shutdown`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --skip-os-shutdown
```

PowerShell

Per arrestare un'istanza e ignorare lo spegnimento controllato del sistema operativo

Utilizzare il Stop-EC2Instance cmdlet con. `-SkipOsShutdown $true`

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -SkipOsShutdown $true
```

Avviare un'istanza

Puoi avviare un'istanza arrestata.

Console

Per avviare un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Istanze.
3. Seleziona l'istanza e scegli Stato istanza, Avvia istanza.

   Possono essere necessari alcuni minuti affinché l'istanza entri nello stato `running`.

AWS CLI

Per avviare un'istanza

Utilizzare il comando start-instances:

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Come avviare un'istanza

Utilizza il cmdlet Start-EC2Instance.

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

Arrestare e avviare automaticamente le istanze

Puoi automatizzare l'arresto e l'avvio delle istanze con i seguenti servizi:

Instance Scheduler attivo AWS

È possibile utilizzare Instance Scheduler su AWS per automatizzare l'avvio e l'arresto delle istanze EC2. Per ulteriori informazioni, vedi Come si usa Instance Scheduler con CloudFormation per pianificare le istanze EC2? Si noti che sono previsti costi aggiuntivi.

AWS Lambda e una EventBridge regola Amazon

Puoi utilizzare Lambda e una EventBridge regola per interrompere e avviare le istanze in base a una pianificazione. Per ulteriori informazioni, consulta la pagina Come posso utilizzare Lambda per arrestare e avviare istanze Amazon EC2 a intervalli regolari?

Amazon EC2 Auto Scaling

Per assicurarti di disporre del numero corretto di istanze Amazon EC2 disponibili per gestire il carico di un'applicazione, crea gruppi con dimensionamento automatico. Amazon EC2 Auto Scaling garantisce che l'applicazione abbia sempre la capacità giusta per gestire la domanda di traffico e consente di risparmiare sui costi avviando le istanze solo quando sono necessarie. Tieni presente che Amazon EC2 Auto Scaling termina, anziché arrestare, le istanze non necessarie. Per configurare i gruppi con dimensionamento automatico, consulta Nozioni di base su Amazon EC2 Auto Scaling.

Trova tutte le istanze in esecuzione e interrotte

Puoi trovare tutte le istanze in esecuzione e interrotte Regioni AWS su un'unica pagina utilizzando Amazon EC2 Global View. Questa funzionalità è particolarmente utile per fare l'inventario e trovare istanze dimenticate. Per informazioni su come usare Global View, consulta Visualizza le risorse tra le regioni utilizzando AWS Global View.

In alternativa, puoi eseguire un comando o un cmdlet in ciascuna Regione in cui sono presenti istanze.

AWS CLI

Per ottenere il numero di istanze EC2 in una Regione

Utilizza il seguente comando describe-instances per contare le istanze nella Regione corrente. È necessario eseguire questo comando in ciascuna Regione in cui sono disponibili istanze.

```
aws ec2 describe-instances \
    --region us-east-2 \
    --query "length(Reservations[].Instances[])"
```

Di seguito è riportato un output di esempio.

```
27
```

Per ottenere informazioni riepilogative sulle istanze EC2 in una Regione

Utilizza seguente il comando describe-instances. È necessario eseguire questo comando in ciascuna Regione in cui sono disponibili istanze.

```
aws ec2 describe-instances \
    --region us-east-2 \
    --query "Reservations[].Instances[].[InstanceId,InstanceType,PrivateIpAddress]"
 \
    --output table
```

Di seguito è riportato un output di esempio.

```
-----------------------------------------------------------
|                  DescribeInstances                      |
+---------------------+---------------+-----------------+
|  i-0e3e777f4362f1bf7|  t2.micro     |  10.0.12.9      |
|  i-09453945dcf1529e9|  t2.micro     |  10.0.143.213   |
|  i-08fd74f3f1595fdbd|  m7i.4xlarge  |  10.0.1.103     |
+---------------------+---------------+-----------------+
```

PowerShell

Per ottenere il numero di istanze EC2 in una Regione

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance -Region us-east-2).Instances.Length
```

Di seguito è riportato un output di esempio.

```
27
```

Per ottenere informazioni riepilogative sulle istanze EC2 in una Regione

Utilizza il cmdlet Get-EC2Instance. È necessario eseguire questo comando in ciascuna Regione in cui sono disponibili istanze.

```
(Get-EC2Instance).Instances | Select InstanceId, InstanceType, PrivateIpAddress
```

Di seguito è riportato un output di esempio.

```
InstanceId          InstanceType PrivateIpAddress
----------          ------------ ----------------
i-0e3e777f4362f1bf7 t2.micro     10.0.12.9
i-09453945dcf1529e9 t2.micro     10.0.143.213
```

```
i-08fd74f3f1595fdbd m7i.4xlarge  10.0.1.103
```

Individuazione dell'ora di avvio iniziale e di quella più recente

Quando descrivi un'istanza, l'ora di avvio dell'istanza è l'ora di avvio più recente. Dopo l'arresto e l'avvio di un'istanza, l'ora di avvio corrisponde all'ora di avvio della nuova istanza. Per individuare l'ora di avvio iniziale di un'istanza, anche dopo averla interrotta e avviata, visualizza l'ora in cui l'interfaccia di rete principale è stata collegata all'istanza.

Console

Per individuare l'ora di avvio più recente

Seleziona l'istanza e trova Ora di avvio in Dettagli dell'istanza nella scheda Dettagli.

Per individuare l'ora di avvio iniziale

Seleziona l'istanza e trova l'interfaccia di rete principale (l'indice del dispositivo è 0) in Interfacce di rete nella scheda Rete.

AWS CLI

Per individuare dell'ora di avvio iniziale e di quella più recente

Utilizzando il comando describe-instances per visualizzare sia l'ora di avvio iniziale che l'ora di avvio più recente per l'istanza specificata.

```
aws ec2 describe-instances \
    --instance-id i-1234567890abcdef0 \
    --query 'Reservations[].Instances[].
{InstanceID:InstanceId,InitialLaunch:NetworkInterfaces[0].Attachment.AttachTime,LastLaunch:L
```

Di seguito è riportato un output di esempio.

```
[
    {
        "InstanceID": "i-1234567890abcdef0",
        "InitialLaunch": "2024-04-19T00:47:08+00:00",
        "LastLaunch": "2024-05-27T06:24:06+00:00"
    }
]
```

PowerShell

Per individuare l'ora di avvio più recente

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.LaunchTime
```

Di seguito è riportato un output di esempio.

```
Monday, May 27, 2024 6:24:06 AM
```

Per individuare l'ora di avvio iniziale

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance -
InstanceId i-1234567890abcdef0).Instances.NetworkInterfaces.Attachment.AttachTime
```

Di seguito è riportato un output di esempio.

```
Friday, April 19, 2024 12:47:08 AM
```

Abilitazione della protezione da arresto per le istanze EC2

Se desideri che un'istanza non venga arrestata per errore, puoi abilitare la funzionalità di protezione da arresto per tale istanza. La protezione da arresto protegge la tua istanza anche dalla chiusura accidentale.

L'`DisableApiStop`attributo dell'`ModifyInstanceAttribute`API Amazon EC2 controlla se l'istanza può essere interrotta utilizzando la console Amazon EC2 AWS CLI, l'API o Amazon EC2. Puoi impostare il valore di questo attributo quando avvii l'istanza, mentre l'istanza è in esecuzione oppure mentre l'istanza è arrestata.

Considerazioni

- L'attivazione della protezione da arresto non impedisce di arrestare un'istanza accidentalmente avviando un arresto dall'istanza stessa utilizzando un comando del sistema operativo come shutdown o poweroff.

- L'attivazione della protezione dall'arresto non AWS impedisce l'arresto dell'istanza quando è previsto un evento di arresto dell'istanza.
- L'attivazione della protezione da arresto non impedisce al Amazon EC2 Auto Scaling di terminare un'istanza quando l'istanza non è integra o durante eventi di riduzione orizzontale. Puoi controllare se un gruppo con scalabilità automatica può terminare una determinata istanza durante la riduzione utilizzando la protezione per la riduzione delle istanze.
- La protezione contro l'arresto non solo impedisce l'arresto accidentale dell'istanza, ma anche la chiusura accidentale quando si utilizza la console o l'API AWS CLI. Tuttavia, non imposta automaticamente l'attributo `DisableApiTermination`. Tieni presente che quando l'`DisableApiStop`attributo è impostato su`false`, l'impostazione dell'`DisableApiTermination`attributo determina se l'istanza può essere terminata utilizzando la console o l'API. AWS CLI Per ulteriori informazioni, consulta Terminare le istanze Amazon EC2.
- Non puoi abilitare la protezione da arresto per le istanze con un volume root dell'archivio dell'istanza.
- Non è possibile abilitare la protezione da arresto per istanze spot.
- L'API Amazon EC2 segue un modello di consistenza eventuale quando abiliti o disabiliti la protezione da arresto. Ciò significa che il risultato dell'esecuzione dei comandi per impostare l'attributo Protezione da arresto potrebbe non essere immediatamente visibile a tutti i comandi successivi eseguiti. Per ulteriori informazioni, consulta la sezione Eventual consistency nella Guida per gli sviluppatori di Amazon EC2.

Attività della protezione da arresto

- Abilitazione della protezione da arresto per un'istanza all'avvio
- Abilitazione della protezione da arresto per un'istanza in esecuzione o arrestata
- Disabilitazione della protezione da arresto per un'istanza in esecuzione o arrestata

Abilitazione della protezione da arresto per un'istanza all'avvio

Puoi abilitare la protezione da arresto per un'istanza al suo avvio.

Console

Come abilitare la protezione da arresto per un'istanza all'avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel pannello di controllo scegliere Avvia istanza.
3. Configura l'istanza tramite la nuova procedura guidata di avvio dell'istanza.
4. Nella procedura guidata, abilita la protezione da arresto scegliendo Abilita per Protezione da arresto in Dettagli avanzati.

AWS CLI

Come abilitare la protezione da arresto per un'istanza all'avvio

Utilizza il comando run-instances per avviare un'istanza. Aggiungi il seguente parametro.

```
--disable-api-stop
```

PowerShell

Come abilitare la protezione da arresto per un'istanza all'avvio

Usa il New-EC2Instance cmdlet per avviare l'istanza. Aggiungi il seguente parametro.

```
-DisableApiStop $true
```

Abilitazione della protezione da arresto per un'istanza in esecuzione o arrestata

Puoi abilitare la protezione da arresto per un'istanza in esecuzione o arrestata.

Console

Per abilitare la protezione da arresto per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Istanze.
3. Seleziona l'istanza, quindi scegli Operazioni > Impostazioni dell'istanza > Modifica protezione da arresto.
4. Seleziona la casella di controllo Abilita, quindi scegli Salva.

AWS CLI

Per abilitare la protezione da arresto per un'istanza

Utilizza il comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-stop
```

PowerShell

Per abilitare la protezione da arresto per un'istanza

Utilizza il cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiStop $true
```

Disabilitazione della protezione da arresto per un'istanza in esecuzione o arrestata

Puoi disabilitare la protezione da arresto per un'istanza in esecuzione o arrestata utilizzando uno dei metodi descritti di seguito.

Console

Per disabilitare la protezione da arresto per un'istanza in esecuzione o arrestata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Istanze.
3. Seleziona l'istanza, quindi scegli Actions (Operazioni), Instance settings (Impostazioni dell'istanza) e Change stop protection (Modifica protezione da arresto).
4. Deseleziona la casella di spunta Abilita, quindi scegli Salva.

AWS CLI

Per disabilitare la protezione da arresto per un'istanza in esecuzione o arrestata

Utilizza il comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-stop
```

PowerShell

Per disabilitare la protezione da arresto per un'istanza

Utilizza il cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiStop $false
```

Metti in ibernazione la tua istanza Amazon EC2

Quando iberni un'istanza, Amazon EC2 segnala al sistema operativo di eseguire l'ibernazione (suspend to disk), L'ibernazione salva il contenuto della memoria dell'istanza (RAM) nel volume di root di Amazon Elastic Block Store (Amazon EBS). Amazon EC2 rende persistente il volume di root dell'istanza EBS ed eventuali volumi di dati EBS collegati. Quando l'istanza viene avviata:

- Il volume root EBS viene ripristinato allo stato precedente
- I contenuti RAM vengono ricaricati
- I processi precedentemente in esecuzione vengono ripresi
- I volumi di dati precedentemente collegati vengono collegati nuovamente e l'istanza conserva il proprio ID

Puoi ibernare un'istanza solo se è abilitata per l'ibernazione e soddisfa i prerequisiti di ibernazione.

Se un'istanza o un'applicazione impiega molto tempo per eseguire il bootstrap e creare un footprint di memoria per diventare pienamente produttiva, puoi utilizzare l'ibernazione per inizializzare l'istanza. Per inizializzare l'istanza, è necessario:

1. Avviarla con l'ibernazione abilitata.
2. Portarla nello stato desiderato.
3. Puoi ibernarla in modo che sia pronta per essere ripresa nello stato desiderato quando necessario.

Non sono previsti addebiti per l'utilizzo di un'istanza ibernata, finché questa si trova nello stato `stopped`, né per il trasferimento dei dati, se il contenuto della RAM viene trasferito al volume root EBS. È previsto l'addebito per l'archiviazione di tutti i volumi EBS, compresa l'archiviazione dei contenuti RAM.

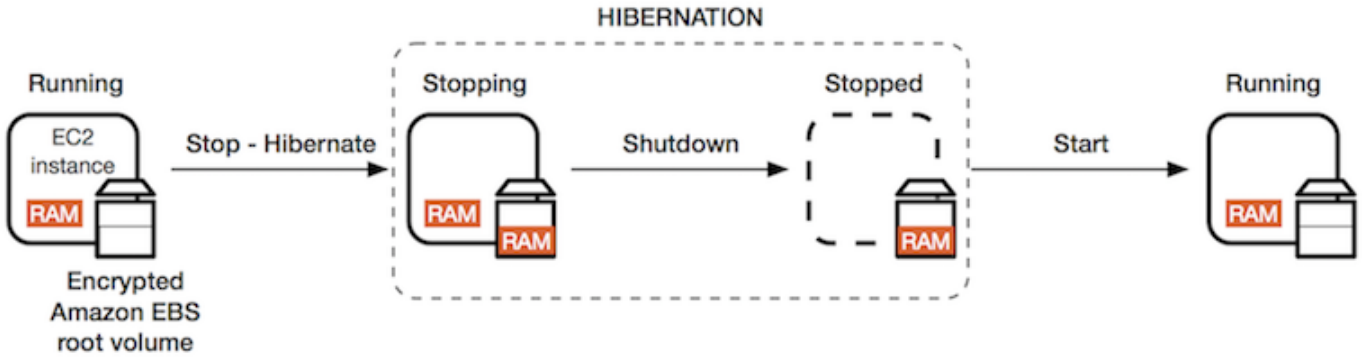
Se non hai più bisogno di un'istanza, puoi terminarla in qualsiasi momento, anche quando si trova nello stato `stopped` (ibernata). Per ulteriori informazioni, consulta Terminare le istanze Amazon EC2.

Indice

- Come funziona l'ibernazione delle istanze Amazon EC2
- Prerequisiti per l'ibernazione dell'istanza EC2
- Configurare un'AMI Linux per il supporto dell'ibernazione
- Abilitazione dell'ibernazione per un'istanza Amazon EC2
- Disabilitazione di KASLR su un'istanza (solo Ubuntu)
- Metti in ibernazione un'istanza Amazon EC2
- Riavvio di un'istanza Amazon EC2 ibernata
- Risoluzione dei problemi di ibernazione delle istanze Amazon EC2

Come funziona l'ibernazione delle istanze Amazon EC2

Il seguente diagramma mostra una panoramica di base del processo di ibernazione per istanze EC2.



Cosa succede quando si iberna un'istanza

Quando iberni un'istanza, si verifica quanto segue:

- L'istanza passa allo stato `stopping`. Amazon EC2 segnala al sistema operativo di eseguire l'ibernazione (suspend to disk). L'ibernazione blocca tutti i processi, salva il contenuto della memoria RAM nel volume root EBS, quindi esegue la normale chiusura del sistema.
- Una volta completata la chiusura, l'istanza passa allo stato `stopped`.
- Tutti i volumi EBS restano collegati all'istanza e i rispettivi dati vengono conservati, incluso il contenuto salvato della RAM.

- Tutti i volumi di instance store Amazon EC2 rimangono collegati all'istanza, ma i dati sui volumi di instance store vengono persi.
- Nella maggior parte dei casi, all'avvio l'istanza migra su un nuovo computer host sottostante. Questo è anche quello che accade quando si arresta e avvia un'istanza.
- Quando l'istanza viene avviata, il sistema operativo legge il contenuto della RAM dal volume root EBS prima di sbloccare i processi per riprendere il proprio stato.
- L'istanza mantiene i suoi indirizzi IPv4 privati e tutti gli indirizzi IPv6. Quando l'istanza viene avviata, l'istanza continua a mantenere i relativi indirizzi IPv4 privati e gli eventuali indirizzi IPv6.
- Amazon EC2 rilascia l'indirizzo IPv4 pubblico. Quando l'istanza viene avviata, Amazon EC2 le assegna un nuovo indirizzo IPv4 pubblico.
- L'istanza mantiene gli indirizzi IP elastici associati. Ti verranno addebitati gli indirizzi IP elastici associati a un'istanza ibernata.

Per ulteriori informazioni sulla differenza tra ibernare e riavviare, arrestare o terminare un'istanza, consulta Differenze tra gli stati dell'istanza.

Limitazioni

- Quando iberni un'istanza, i dati presenti sui volumi dell'instance store vengono persi.
- (Istanze Linux) Non puoi ibernare un'istanza Linux che ha più di 150 GiB di RAM.
- (Istanze Windows) Non puoi ibernare un'istanza Windows che ha più di 16 GiB di RAM.
- Mentre l'istanza è ibernata, non puoi modificarla. Ciò è diverso da un'istanza arrestata che non è in ibernazione, in cui puoi modificare determinati attributi, come il tipo o la dimensione dell'istanza.
- Se si crea uno snapshot o un'AMI da un'istanza che è ibernata o ha attivato la modalità di ibernazione, potrebbe non essere possibile connettersi a una nuova istanza avviata dall'AMI o da un'AMI creata da uno snapshot.
- (Solo istanze spot) Se l'istanza spot viene messa in ibernazione da Amazon EC2, solo Amazon EC2 può riprenderla. Se l'istanza spot viene messa in ibernazione da te (ibernazione avviata dall'utente), puoi riprendere l'istanza in autonomia. Un'istanza spot ibernata può essere ripresa solo se la capacità è disponibile e il prezzo spot è inferiore o uguale al prezzo massimo specificato.
- Non è possibile ibernare un'istanza che si trova in un gruppo Auto Scaling o viene utilizzata da Amazon ECS. Se l'istanza si trova in un gruppo Auto Scaling e si prova a ibernarla, il servizio Amazon EC2 Auto Scaling contrassegna l'istanza arrestata come non integra, pertanto potrebbe terminarla e avviare un'istanza sostitutiva. Per ulteriori informazioni, consulta Controllo dell'integrità per istanze in un gruppo Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.

- Non è possibile ibernare un'istanza configurata per l'avvio in modalità UEFI con UEFI Secure Boot abilitato.
- Se si iberna un'istanza che è stata lanciata in un Prenotazione di capacità, il Prenotazione di capacità non garantisce che l'istanza ibernata possa riprendere dopo aver provato ad avviarla.
- Non è possibile ibernare un'istanza che utilizza un kernel inferiore a 5.10 se è abilitata la modalità FIPS (Federal Information Processing Standard).
- Non è possibile mantenere un'istanza ibernata per più di 60 giorni. Per prolungare il periodo di ibernazione oltre i 60 giorni, è necessario avviare l'istanza ibernata, arrestarla e avviarla.
- Aggiorniamo costantemente la nostra piattaforma con upgrade e patch di sicurezza che possono entrare in conflitto con le istanze ibernate. Ti avvisiamo in caso di aggiornamenti critici che richiedono un avvio per le istanze ibernate per potere eseguire la chiusura o il riavvio per applicare gli upgrade e le patch di sicurezza necessari.

Considerazioni sull'ibernazione di un'istanza spot

- Se l'istanza spot viene messa in ibernazione da te, puoi riavviarla a condizione che la capacità sia disponibile e il prezzo spot sia inferiore o uguale al prezzo massimo specificato.
- Se Amazon EC2 mette in ibernazione l'istanza spot:
  - Solo Amazon EC2 può riprendere l'istanza.
  - Amazon EC2 riprende l'istanza spot ibernata quando la capacità diventa disponibile con un prezzo spot pari o inferiore al prezzo massimo specificato.
  - Due minuti prima che Amazon EC2 metta in ibernazione l'istanza spot, riceverai un avviso di interruzione.

  Per ulteriori informazioni, consulta Interruzioni dell'istanza spot.

Prerequisiti per l'ibernazione dell'istanza EC2

Puoi abilitare il supporto per l'ibernazione per un' On-Demand istanza o un'istanza Spot quando la avvii. Non puoi abilitare l'ibernazione su un'istanza esistente, in esecuzione o arrestata. Per ulteriori informazioni, consulta Abilitazione dell'ibernazione delle istanze.

Requisiti per ibernare un'istanza

- Regioni AWS
- AMI

- Famiglie di istanze
- Dimensioni RAM dell'istanza
- Tipo di volume root
- Dimensione del volume root
- Crittografia del volume root
- Tipi di volume EBS
- Richieste di istanza spot

Regioni AWS

Puoi utilizzare l'ibernazione con tutte le istanze. Regioni AWS

AMI

Devi usare un'AMI HVM che supporta l'ibernazione. Le seguenti AMI supportano l'ibernazione:

AMI di Linux

AMI per tipi di istanza Intel e AMD

- AMI AL2023 rilasciata il 20.09.2023 o successivamente[2]
- AMI Amazon Linux 2 rilasciata il 29.08.2019 o successivamente
- AMI Amazon Linux 2018.03 rilasciata il 16.11.2018 o successivamente
- AMI CentOS versione 8[2] (la configurazione aggiuntiva è obbligatoria)
- AMI Fedora versione 34 o successiva[2] (la configurazione aggiuntiva è obbligatoria)
- AMI Red Hat Enterprise Linux (RHEL) 9[2] (la configurazione aggiuntiva è obbligatoria)
- AMI Red Hat Enterprise Linux (RHEL) 8[2] (la configurazione aggiuntiva è obbligatoria)
- AMI Ubuntu 22.04.2 LTS (Jammy Jellyfish) rilasciata con numero di serie 20230303 o successivo[3]
- AMI Ubuntu 20.04 LTS (Focal Fossa) AMI rilasciata con numero di serie 20210820 o successivo[3]
- AMI Ubuntu 18.04 LTS (Bionic Beaver) AMI rilasciata con numero di serie 20190722.1 o successivo [3] [5]
- AMI Ubuntu 16.04 LTS (Xenial Xerus) AMI [3] [4] [5] (la configurazione aggiuntiva è obbligatoria)

AMI per tipi di istanza Graviton

- AMI AL2023 (Arm a 64 bit) rilasciata il 01/07/2024 o successivamente[1]

- AMI Amazon Linux 2 (Arm a 64 bit) rilasciata il 20/06/2024 o successivamente
- AMI Ubuntu 22.04.2 LTS (Arm a 64 bit) (Jammy Jellyfish) rilasciata con numero di serie 20240701 o successivo[3]
- AMI Ubuntu 20.04 LTS (Arm a 64 bit) (Focal Fossa) rilasciata con numero di serie 20240701 o successivo[3]

[1] Per l'AMI minima AL2023, è richiesta una configurazione aggiuntiva.

[2] Per CentOS, Fedora e Red Hat Enterprise Linux, l'ibernazione è supportata solo nelle istanze. Nitro-based

[3] Suggeriamo di disabilitare KASLR sulle istanze con 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa), Ubuntu 18.04 LTS (Bionic Beaver) e Ubuntu 16.04 LTS (Xenial Xerus). Per ulteriori informazioni, consulta Disabilitazione di KASLR su un'istanza (solo Ubuntu).

[4] Per Ubuntu 16.04 LTS - (Xenial Xerus) AMI, l'ibernazione non è supportata su tipi di istanza `t3.nano`. Nessuna patch sarà resa disponibile perché Ubuntu (Xenial Xerus) ha terminato il supporto nell'aprile 2021. Per utilizzare i tipi di istanza `t3.nano`, consigliamo di eseguire l'aggiornamento alle AMI Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa) ooppure Ubuntu 18.04 LTS (Bionic Beaver).

[5] Il supporto per Ubuntu 18.04 LTS (Bionic Beaver) e Ubuntu 16.04 LTS (Xenial Xerus) ha raggiunto la fine del ciclo di vita.

Per configurare la tua AMI per il supporto dell'ibernazione, consulta Configurare un'AMI Linux per il supporto dell'ibernazione.

Il supporto per altre versioni di Ubuntu e altri sistemi operativi sarà disponibile a breve.

AMI di Windows

- AMI Windows Server 2022 rilasciata il 13.09.2023 o successivamente
- AMI Windows Server 2019 rilasciata il 11.09.2019 o successivamente
- AMI Windows Server 2016 rilasciata il 11.09.2019 o successivamente
- AMI Windows Server 2012 R2 rilasciata il 11.09.2019 o successivamente
- AMI Windows Server 2012 rilasciata il 11.09.2019 o successivamente

Famiglie di istanze

Devi usare una famiglia di istanze che supporta l'ibernazione. Tuttavia, le istanze bare metal non sono supportate.

- Uso generale: M3, M4, M5, M5a, M5ad, M5d, M6a, M6g, M6gd, M6i, M6id, M6idn, M6in, M7a, M7g, M7gd, M7i,, M8a, M8aZn, M8g, M8gb, M8gd, M8gd, M8gd, M8gd, M8zn M8gN, M8i, M8in M7i-flex, M8idn, M8ib, M8idb, M9g, M9gd, T2, T3, T3a, T4g M8i-flex
- Ottimizzato per il calcolo: C3, C4, C5, C5d, C6a, C6g, C6gd, C6gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i,, C8a C7i-flex, C8g, C8gb, C8gd, C8gn, C8i,, C8g C8i-flex, C8gb 8iN, C8ib, C9g, C9gd
- Memoria ottimizzata: R3, R4, R5, R5a, R5ad, R5d, R6a, R6g, R6gd, R6idn, R6in, R7a, R7g, R7gd, R7i, R7iz, R8a, R8g, R8gb, R8gd, R8gn, R8i, R8b iN, R8idn R8i-flex, R8ib, R8idb, R9g, R9gd, X2gd, X8aedz, X8i
- Ottimizzate per l'archiviazione: I3, I3en, I4g, I7i, I7ie, I8g, I8ge, Im4gn, Is4gen

Console

Per ottenere i tipi di istanza che supportano l'ibernazione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instance Types (Tipi di istanza).
3. Aggiungi il filtro On-Demand Hibernation support = true.
4. (Facoltativo) Aggiungi filtri per approfondire l'ambito di specifici tipi di istanze di interesse.

AWS CLI

Per ottenere i tipi di istanza che supportano l'ibernazione

Utilizza il comando describe-instance-types. Nota che i tipi di istanza disponibili variano in base alla Regione.

```
aws ec2 describe-instance-types \
    --filters Name=hibernation-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Per ottenere i tipi di istanza che supportano l'ibernazione

Utilizza il cmdlet Get-EC2InstanceType. Nota che i tipi di istanza disponibili variano in base alla Regione.

```
(Get-EC2InstanceType `
    -Filter @{Name="hibernation-supported"; Values="true"}).InstanceType | Sort-
Object
```

Dimensioni RAM dell'istanza

Istanze Linux: devono essere inferiori a 150 GiB.

Istanze Windows: devono essere uguali o inferiori a 16 GiB. Per l'ibernazione di un'istanza Windows T3 o T3a, consigliamo almeno 1 GiB di RAM.

Tipo di volume root

Il volume root deve essere un volume EBS e non un volume instance store.

Dimensione del volume root

Il volume root deve essere sufficientemente ampio da archiviare il contenuto della RAM e da ottimizzare l'utilizzo previsto, ad esempio sistema operativo o applicazioni. Se abiliti l'ibernazione, lo spazio viene allocato sul volume root al lancio per archiviare la RAM.

Crittografia del volume root

Il volume principale deve essere crittografato per proteggere i contenuti sensibili presenti in memoria durante l'ibernazione. Puoi abilitare l'ibernazione per un'istanza tramite Amazon EC2 utilizzando la console o l'API. AWS CLI Prima del lancio dell'istanza, Amazon EC2 verifica che il volume root sia crittografato. Poiché il volume root EBS è crittografato, anche i dati RAM scritti su di esso durante l'ibernazione sono crittografati.

⚠ Solo l'API Amazon EC2 applica la crittografia a riposo per l'ibernazione

Amazon EC2 convalida i prerequisiti di ibernazione, inclusa la crittografia del volume root, solo per l'ibernazione avviata tramite Amazon EC2. Ciò include la console e l'API. AWS CLI

Questi controlli non si applicano se si avvia l'ibernazione dall'interno del sistema operativo guest, ad esempio con sospensione su disco di Linux o Windows. In tal caso, assicurati che il volume root EBS sia crittografato. Il sistema operativo mantiene il contenuto della memoria su questo volume prima di interrompere l'istanza. Secondo il modello di responsabilità condivisa, sei responsabile della crittografia dei dati inattivi per le azioni eseguite nel sistema operativo guest. Per ulteriori informazioni, consulta Modello di responsabilità condivisa e Protezione dei dati inattivi nel Security Pillar - AWS Well-Architected Framework.

Utilizzare una delle tre opzioni seguenti per garantire che il volume root sia un volume EBS crittografato:

- Crittografia EBS per impostazione predefinita: puoi abilitare la crittografia EBS per impostazione predefinita per assicurarti che tutti i nuovi volumi EBS creati nel tuo AWS account siano crittografati. In questo modo è possibile abilitare l'ibernazione per le istanze senza specificare l'intento di crittografia all'avvio delle istanze. Per ulteriori informazioni, consulta Abilita crittografia per impostazione predefinita.
- Crittografia EBS «in un solo passaggio»: è possibile avviare istanze EBS-backed EC2 crittografate da un'AMI non crittografata e contemporaneamente abilitare l'ibernazione. Per ulteriori informazioni, consulta Usa la crittografia con le EBS-backed AMI.
- AMI crittografata: puoi abilitare la crittografia EBS utilizzando un'AMI crittografata per avviare l'istanza. Se l'AMI non dispone di una snapshot root crittografata, è possibile copiarla in una nuova AMI e richiederne la crittografia. Per ulteriori informazioni, consulta Crittografia di un'immagine non crittografata durante la copia e Copiare un'AMI.

Tipi di volume EBS

I volumi EBS devono utilizzare uno dei seguenti tipi di volume EBS:

- Scopo generico (SSD) (`gp2` e `gp3`)
- IOPS con provisioning (SSD) (`io1` e `io2`)

Se scegli un tipo di volume SSD IOPS con provisioning, per ottenere prestazioni ottimali per l'ibernazione devi eseguire il provisioning del volume EBS con l'IOPS appropriato. Per ulteriori informazioni, consulta Tipi di volumi di Amazon EBS nella Guida per l'utente di Amazon EBS.

Richieste di istanza spot

Per le istanze spot, si applicano i seguenti requisiti:

- Il tipo di richiesta di istanza spot deve essere `persistent`.
- Non è possibile specificare un gruppo di avvio nella richiesta di istanza spot.

Configurare un'AMI Linux per il supporto dell'ibernazione

Le seguenti AMI Linux possono supportare l'ibernazione di un'istanza Amazon EC2, a condizione di completare le fasi di configurazione aggiuntive descritte in questa sezione.

Una configurazione aggiuntiva è richiesta per:

- AMI minima AL2023 rilasciata il 20/09/2023 o successivamente
- AMI Amazon Linux 2 versione minima rilasciata il 29/08/2019 o successivamente
- Amazon Linux 2 rilasciato prima del 29.08.2019
- Amazon Linux rilasciato prima del 16.11.2018
- CentOS versione 8 o successiva
- Fedora versione 34 o successive
- Red Hat Enterprise Linux versione 8 o 9
- Ubuntu 20.04 LTS (Focal Fossa) rilasciata prima del numero di serie 20210820
- Ubuntu 18.04 (Bionic Beaver) rilasciata prima del numero seriale 20190722.1
- Ubuntu 16.04 (Xenial Xerus)

Per le AMI Linux e Windows che supportano l'ibernazione e per cui non è richiesta alcuna configurazione aggiuntiva, consulta AMI.

Per maggiori informazioni, consulta Aggiornamento software dell'istanza sull'istanza Amazon Linux 2.

AMI minima AL2023 rilasciata il 20/09/2023 o successivamente

Per configurare un'AMI minima AL2023 rilasciata il 20/09/2023 o successivamente per il supporto dell'ibernazione

1. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

2. Riavvia il servizio .

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

AMI Amazon Linux 2 versione minima rilasciata il 29/08/2019 o successivamente

Per configurare un'AMI Amazon Linux 2 versione minima rilasciata il 29/08/2019 o successivamente per il supporto dell'ibernazione

1. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

2. Riavvia il servizio .

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

Amazon Linux 2 rilasciato prima del 29.08.2019

Per configurare un'AMI Amazon Linux 2 rilasciata prima del 29.08.2019 per il supporto dell'ibernazione

1. Aggiornare il kernel a `4.14.138-114.102` o versione successiva.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

4. Verificare che il kernel sia aggiornato alla versione `4.14.138-114.102` o successiva.

```
[ec2-user ~]$ uname -a
```

5. Arrestare l'istanza e creare un'AMI. Per ulteriori informazioni, consulta Crea un' EBS-backed AMI Amazon.

Amazon Linux rilasciato prima del 16.11.2018

Per configurare un'AMI Amazon Linux rilasciata prima del 16.11.2018 per il supporto dell'ibernazione

1. Aggiornare il kernel a `4.14.77-70.59` o versione successiva.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

4. Verificare che il kernel sia aggiornato alla versione `4.14.77-70.59` o successiva.

```
[ec2-user ~]$ uname -a
```

5. Arrestare l'istanza e creare un'AMI. Per ulteriori informazioni, consulta Crea un' EBS-backed AMI Amazon.

CentOS versione 8 o successiva

Per configurare un'AMI CentOS versione 8 o successiva per il supporto dell'ibernazione

1. Aggiornare il kernel a `4.18.0-305.7.1.el8_4.x86_64` o versione successiva.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installare il repository EPEL (Extra Packages for Enterprise Linux) Fedora.

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

3. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Attivare l'agente di ibernazione perché venga lanciato all'avvio.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

6. Verificare che il kernel sia aggiornato alla versione `4.18.0-305.7.1.el8_4.x86_64` o successiva.

```
[ec2-user ~]$ uname -a
```

Fedora versione 34 o successive

Per configurare un'AMI Fedora versione 34 o successiva per il supporto dell'ibernazione

1. Aggiornare il kernel a `5.12.10-300.fc34.x86_64` o versione successiva.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

3. Attivare l'agente di ibernazione perché venga lanciato all'avvio.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

4. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

5. Verificare che il kernel sia aggiornato alla versione `5.12.10-300.fc34.x86_64` o successiva.

```
[ec2-user ~]$ uname -a
```

Red Hat Enterprise Linux versione 8 o 9

Per configurare un'AMI Red Hat Enterprise Linux 8 o 9 per supportare l'ibernazione

1. Aggiornare il kernel a `4.18.0-305.7.1.el8_4.x86_64` o versione successiva.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installare il repository EPEL (Extra Packages for Enterprise Linux) Fedora.

   Versione 8 RHEL:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   Versione 9 RHEL:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

3. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Attivare l'agente di ibernazione perché venga lanciato all'avvio.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

6. Verificare che il kernel sia aggiornato alla versione `4.18.0-305.7.1.el8_4.x86_64` o successiva.

```
[ec2-user ~]$ uname -a
```

Ubuntu 20.04 LTS (Focal Fossa) rilasciata prima del numero di serie 20210820

Configurazione di un Ubuntu 20.04 LTS (Focal Fossa) AMI rilasciata prima del numero di serie 20210820 a supporto dell'ibernazione

1. Aggiorna il linux-aws-kernel a `5.8.0-1038.40` o versione successiva e grub2 a `2.04-1ubuntu26.13`o versione successiva.

   ```
   [ec2-user ~]$ sudo apt update
   [ec2-user ~]$ sudo apt dist-upgrade
   ```

2. Riavviare l'istanza.

   ```
   [ec2-user ~]$ sudo reboot
   ```

3. Verificare che il kernel sia aggiornato alla versione `5.8.0-1038.40` o successiva.

   ```
   [ec2-user ~]$ uname -a
   ```

4. Confermare che la versione grub2 sia aggiornata alla versione `2.04-1ubuntu26.13` o successiva.

   ```
   [ec2-user ~]$ dpkg --list | grep grub2-common
   ```

Ubuntu 18.04 (Bionic Beaver) rilasciata prima del numero seriale 20190722.1

Per configurare un'AMI Ubuntu 18.04 LTS rilasciata prima del numero seriale 20190722.1 per il supporto dell'ibernazione

1. Aggiornare il kernel a `4.15.0-1044` o versione successiva.

   ```
   [ec2-user ~]$ sudo apt update
   [ec2-user ~]$ sudo apt dist-upgrade
   ```

2. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

4. Verificare che il kernel sia aggiornato alla versione `4.15.0-1044` o successiva.

```
[ec2-user ~]$ uname -a
```

Ubuntu 16.04 (Xenial Xerus)

Per configurare Ubuntu 16.04 LTS per supportare l'ibernazione, devi installare il pacchetto kernel linux-aws-hwe versione 4.15.0-1058-aws o successiva e ec2-hibinit-agent.

> **Important**
>
> Il pacchetto kernel `linux-aws-hwe` è supportato da Canonical. Il supporto standard per Ubuntu 16.04 LTS è terminato nell'aprile 2021 e il pacchetto non riceve più aggiornamenti regolari. Tuttavia, riceverà ulteriori aggiornamenti della sicurezza fino al termine del supporto per la manutenzione estesa della sicurezza nel 2024. Per ulteriori informazioni, consulta Amazon EC2 Hibernation per Ubuntu 16.04 LTS ora disponibile sul blog Canonical Ubuntu. Ti consigliamo di eseguire l'aggiornamento a Ubuntu 20.04 LTS (Focal Fossa) AMI o Ubuntu 18.04 LTS (Bionic Beaver) AMI.

Per configurare un'AMI Ubuntu 16.04 LTS e supportare l'ibernazione

1. Aggiornare il kernel a `4.15.0-1058-aws` o versione successiva.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt install linux-aws-hwe
```

2. Installare il pacchetto `ec2-hibinit-agent` dai repository.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

4. Verificare che il kernel sia aggiornato alla versione `4.15.0-1058-aws` o successiva.

```
[ec2-user ~]$ uname -a
```

Abilitazione dell'ibernazione per un'istanza Amazon EC2

Per ibernare un'istanza, devi prima abilitarla per l'ibernazione durante l'avvio dell'istanza.

> **Important**
>
> Non è possibile abilitare o disabilitare l'ibernazione di un'istanza dopo averla avviata.

Processi

- On-Demand Abilita l'ibernazione per le istanze
- Abilitazione dell'ibernazione per le istanze spot
- Verificare se un'istanza è abilitata per l'ibernazione

On-Demand Abilita l'ibernazione per le istanze

Puoi abilitare l'ibernazione per le tue istanze. On-Demand

Console

Per abilitare l'ibernazione per un'istanza On-Demand

1. Segui la procedura per l'avvio di un'istanza, ma non avviare l'istanza finché non avrai completato i seguenti passaggi per abilitare l'ibernazione.
2. Per abilitare l'ibernazione, configura i seguenti campi nella procedura guidata di avvio dell'istanza:

   a. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), seleziona un'AMI che supporta l'ibernazione. Per ulteriori informazioni, consulta AMI.

b. In Instance type (Tipo di istanza), seleziona un tipo di istanza supportato. Per ulteriori informazioni, consulta Famiglie di istanze.

c. In Configure storage (Configura lo storage), scegli Advanced (Avanzate) a destra e specifica le informazioni seguenti per il volume root:

- Per Dimensione (GiB), immettere la dimensione del volume EBS principale. Il volume deve essere sufficientemente grande per memorizzare il contenuto della RAM e soddisfare l'utilizzo previsto.
- Per Volume Type (Tipo di volume), seleziona un tipo di volume EBS supportato: SSD per scopo generico (`gp2` e `gp3`) o SSD con capacità di IOPS allocata (`io1` e `io2`).
- Per Encrypted (Crittografato), scegli Yes (Sì). Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, è selezionato Sì.
- Per KMS key (Chiave KMS), seleziona la chiave di crittografia per il volume. Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, viene selezionata la chiave di crittografia predefinita.

Per ulteriori informazioni sui prerequisiti per il volume radice, consulta Prerequisiti per l'ibernazione dell'istanza EC2.

d. Espandi Advanced details (Dettagli avanzati) e in Stop - Hibernate behavior (Comportamento di arresto/ibernazione) scegli Enable (Abilita).

3. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

AWS CLI

Per abilitare l'ibernazione per un'istanza On-Demand

Utilizzare il comando run-instances per avviare un'istanza. Specificare i parametri del volume principale EBS utilizzando il parametro `--block-device-mappings file://mapping.json` e abilitare l'ibernazione utilizzando il parametro `--hibernation-options Configured=true`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type m5.large \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
```

```
    --count 1 \
    --key-name MyKeyPair
```

Specifica quanto segue nel file `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

Il valore per `DeviceName` deve corrispondere al nome del dispositivo root associato all'AMI. Per trovare il nome del dispositivo root, utilizza il comando describe-images.

```
aws ec2 describe-images --image-id ami-0abcdef1234567890
```

Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, puoi ometterla. `"Encrypted": true`

PowerShell

Per abilitare l'ibernazione per un'istanza On-Demand

Usa il New-EC2Instance comando per avviare un'istanza. Specificare il volume principale EBS definendo innanzitutto la mappatura dei dispositivi a blocchi e quindi aggiungendolo al comando mediante il parametro `-BlockDeviceMappings`. Abilitare l'ibernazione utilizzando il parametro `-HibernationOptions_Configured $true`.

```
$ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
$ebs_encrypt.DeviceName = "/dev/xvda"
$ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
$ebs_encrypt.Ebs.VolumeSize = 30
$ebs_encrypt.Ebs.VolumeType = "gp2"
$ebs_encrypt.Ebs.Encrypted = $true

New-EC2Instance `
```

```
    -ImageId ami-0abcdef1234567890 `
    -InstanceType m5.large `
    -BlockDeviceMappings $ebs_encrypt `
    -HibernationOptions_Configured $true `
    -MinCount 1 `
    -MaxCount 1 `
    -KeyName MyKeyPair
```

Il valore per `DeviceName` deve corrispondere al nome del dispositivo radice associato all'AMI. Per trovare il nome del dispositivo root, usate il Get-EC2Image comando.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, puoi omettere la `Encrypted = $true` mappatura dei dispositivi a blocchi.

Abilitazione dell'ibernazione per le istanze spot

Puoi abilitare l'ibernazione per le istanze spot. Per informazioni su come ibernare un'istanza spot in fase di interruzione, consulta la pagina Interruzioni dell'istanza spot.

Console

Abilitazione dell'ibernazione per un'istanza spot

1. Segui la procedura per richiedere un'istanza spot utilizzando la procedura guidata di avvio di un'istanza, ma non avviare l'istanza finché non avrai completato i seguenti passaggi per abilitare l'ibernazione.
2. Per abilitare l'ibernazione, configura i seguenti campi nella procedura guidata di avvio dell'istanza:
   a. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), seleziona un'AMI che supporta l'ibernazione. Per ulteriori informazioni, consulta AMI.
   b. In Instance type (Tipo di istanza), seleziona un tipo di istanza supportato. Per ulteriori informazioni, consulta Famiglie di istanze.
   c. In Configure storage (Configura lo storage), scegli Advanced (Avanzate) a destra e specifica le informazioni seguenti per il volume root:

- Per Dimensione (GiB), immettere la dimensione del volume EBS principale. Il volume deve essere sufficientemente grande per memorizzare il contenuto della RAM e soddisfare l'utilizzo previsto.
- Per Volume Type (Tipo di volume), seleziona un tipo di volume EBS supportato: SSD per scopo generico (`gp2` e `gp3`) o SSD con capacità di IOPS allocata (`io1` e `io2`).
- Per Encrypted (Crittografato), scegli Yes (Sì). Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, è selezionato Sì.
- Per KMS key (Chiave KMS), seleziona la chiave di crittografia per il volume. Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, viene selezionata la chiave di crittografia predefinita.

Per ulteriori informazioni sui prerequisiti per il volume radice, consulta Prerequisiti per l'ibernazione dell'istanza EC2.

d. Espandi Dettagli avanzati e, oltre ai campi per la configurazione di un'istanza spot, procedi come segue:

   i. Per Tipo di richiesta, scegli Persistente.

   ii. Per Comportamento di interruzione, scegli Iberna. In alternativa, per Comportamento di arresto/ibernazione, scegli Abilita. Entrambi i campi abilitano l'ibernazione sull'istanza spot. È necessario configurarne solo uno.

3. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

AWS CLI

Abilitazione dell'ibernazione per un'istanza spot

Utilizza il comando run-instances per richiedere un'istanza spot. Specificare i parametri del volume principale EBS utilizzando il parametro `--block-device-mappings file://mapping.json` e abilitare l'ibernazione utilizzando il parametro `--hibernation-options Configured=true`. Il tipo di richiesta spot (`SpotInstanceType`) deve essere `persistent`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c4.xlarge \
```

```
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
    --instance-market-options
        {
           "MarketType":"spot",
           "SpotOptions":{
              "MaxPrice":"1",
              "SpotInstanceType":"persistent"
            }
        }
```

Specifica i parametri del volume root EBS in `mapping.json` nel modo seguente.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

Il valore per `DeviceName` deve corrispondere al nome del dispositivo root associato all'AMI. Per trovare il nome del dispositivo root, utilizza il comando describe-images.

```
aws ec2 describe-images --image-id ami-0abcdef1234567890
```

Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, puoi ometterla`"Encrypted": true`.

PowerShell

Abilitazione dell'ibernazione per un'istanza spot

Usa il New-EC2Instance comando per richiedere un'istanza Spot. Specificare il volume principale EBS definendo innanzitutto la mappatura dei dispositivi a blocchi e quindi aggiungendolo al comando mediante il parametro `-BlockDeviceMappings`. Abilitare l'ibernazione utilizzando il parametro `-HibernationOptions_Configured $true`.

```
$ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
$ebs_encrypt.DeviceName = "/dev/xvda"
$ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
$ebs_encrypt.Ebs.VolumeSize = 30
$ebs_encrypt.Ebs.VolumeType = "gp2"
$ebs_encrypt.Ebs.Encrypted = $true

New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType m5.large `
    -BlockDeviceMappings $ebs_encrypt `
    -HibernationOptions_Configured $true `
    -MinCount 1 `
    -MaxCount 1 `
    -KeyName MyKeyPair `
    -InstanceMarketOption @(
        MarketType = spot;
        SpotOptions @{
        MaxPrice = 1;
        SpotInstanceType = persistent}
    )
```

Il valore per `DeviceName` deve corrispondere al nome del dispositivo radice associato all'AMI. Per trovare il nome del dispositivo root, usate il Get-EC2Image comando.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Se hai abilitato la crittografia per impostazione predefinita in questa AWS regione, puoi omettere la `Encrypted = $true` mappatura dei dispositivi a blocchi.

Verificare se un'istanza è abilitata per l'ibernazione

Puoi verificare se un'istanza è abilitata per l'ibernazione.

Console

Per vedere se un'istanza è abilitata per l'ibernazione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).

3. Seleziona l'istanza e, nella scheda Dettagli, nella sezione Dettagli dell'istanza, controlla il comportamento. Stop-hibernate Enabled (Abilitata) indica che l'istanza è abilitata per l'ibernazione.

AWS CLI

Per vedere se un'istanza è abilitata per l'ibernazione

Utilizzare il comando describe-instances e specificare il parametro `--filters "Name=hibernation-options.configured,Values=true"` per filtrare le istanze abilitate per l'ibernazione.

```
aws ec2 describe-instances \
    --filters "Name=hibernation-options.configured,Values=true"
```

Il campo seguente nell'output indica che l'istanza è abilitata per l'ibernazione.

```
"HibernationOptions": {
    "Configured": true
}
```

PowerShell

Per vedere se un'istanza è abilitata per l'ibernazione

Utilizza il Get-EC2Instance cmdlet e filtra le istanze abilitate per l'ibernazione.

```
(Get-EC2Instance `
    -Filter @{Name="hibernation-options.configured"; Values="true"}).Instances
```

Disabilitazione di KASLR su un'istanza (solo Ubuntu)

Per eseguire l'ibernazione su un'istanza avviata di recente con Ubuntu 16.04 LTS (Xenial Xerus), Ubuntu 18.04 LTS (Bionic Beaver) rilasciata con numero di serie 20190722.1 o versione successiva, o Ubuntu 20.04 LTS (Focal Fossa) rilasciata con numero di serie 20210820 o versione successiva, consigliamo di disabilitare KASLR (Kernel Address Space Layout Randomization). In Ubuntu 16.04 LTS o Ubuntu 18.04 LTS, o Ubuntu 20.04 LTS, KASLR è abilitato per impostazione predefinita.

KASLR è una funzionalità di sicurezza standard del kernel di Linux che consente di mitigare l'esposizione e le ramificazioni di vulnerabilità di accesso alla memoria non ancora scoperte

riproducendo in maniera casuale il valore di base dell'indirizzo del kernel. Con KASLR abilitato, c'è la possibilità che l'istanza non venga riavviata dopo l'ibernazione.

Per ulteriori informazioni su KASLR, consultare Funzionalità di Ubuntu.

Per disabilitare KASLR su un'istanza avviata con Ubuntu

1. Connettersi all'istanza tramite SSH. Per ulteriori informazioni, consulta Connessione a un'istanza Linux tramite SSH.
2. Aprire il file `/etc/default/grub.d/50-cloudimg-settings.cfg` con un editor a scelta. Modificare la riga `GRUB_CMDLINE_LINUX_DEFAULT` per collegare l'opzione `nokaslr`, come mostrato nell'esempio seguente.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295 nokaslr"
```

3. Salvare il file e uscire dall'editor.
4. Eseguire il comando riportato di seguito per ricreare la configurazione di grub.

```
sudo update-grub
```

5. Riavviare l'istanza.

```
sudo reboot
```

6. Esegui il comando seguente per confermare che `nokaslr` è stato aggiunto.

```
cat /proc/cmdline
```

   L'output del comando deve includere l'opzione `nokaslr`.

Metti in ibernazione un'istanza Amazon EC2

È possibile avviare l'ibernazione su un' On-Demand istanza o un'istanza Spot se l'istanza è un' EBS-backedistanza, è abilitata per l'ibernazione e soddisfa i prerequisiti di ibernazione. ??? Se l'ibernazione di un'istanza non riesce, si verifica una normale chiusura.

Console

Ibernazione di un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Seleziona un'istanza e scegli Instance state (Stato istanza), Hibernate instance (Sospendi istanza). Se Hibernate instance (Sospendi istanza) è disabilitato, l'istanza è già sospesa o arrestata oppure non può essere sospesa. Per ulteriori informazioni, consulta Prerequisiti per l'ibernazione dell'istanza EC2.
4. Quando viene richiesta la conferma scegli Hibernate (Sospendi). Possono essere necessari alcuni minuti per ibernare l'istanza. Lo stato dell'istanza diventa prima Stopping (in arresto), quindi passa a Stopped (arrestata) una volta ibernata l'istanza.

AWS CLI

Ibernazione di un'istanza

Utilizzare il comando stop-instances e specificare il parametro `--hibernate`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --hibernate
```

PowerShell

Ibernazione di un'istanza

Utilizza il cmdlet Stop-EC2Instance.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Hibernate $true
```

Puoi verificare se è stata avviata l'ibernazione per un'istanza.

Console

Per vedere se è stata avviata l'ibernazione per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e, nella scheda Dettagli, nella sezione Dettagli istanza, verifica il valore di Messaggio transizione stato.

   Client.UserInitiatedHibernate: l'ibernazione avviata dall'utente indica che l'ibernazione è stata avviata sull'istanza o sull'istanza Spot. On-Demand

AWS CLI

Per vedere se è stata avviata l'ibernazione per un'istanza

Utilizzare il comando describe-instances e specificare il filtro `state-reason-code` per vedere le istanze su cui è stata avviata l'ibernazione.

```
aws ec2 describe-instances \
    --filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

Il seguente campo nell'output indica che l'ibernazione è stata avviata sull'istanza o sull'istanza Spot. On-Demand

```
"StateReason": {
    "Code": "Client.UserInitiatedHibernate"
}
```

PowerShell

Per vedere se è stata avviata l'ibernazione per un'istanza

Utilizza il Get-EC2Instance cmdlet e specifica il `state-reason-code` filtro per visualizzare le istanze in cui è stata avviata l'ibernazione.

```
Get-EC2Instance `
    -Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

Riavvio di un'istanza Amazon EC2 ibernata

Avvia un'istanza ibernata avviandola come faresti con un'istanza arrestata.

Per le istanze spot, se l'istanza è stata messa in ibernazione da Amazon EC2, solo Amazon EC2 può riprenderla. Puoi riprendere un'istanza spot ibernata solo se l'hai ibernata tu. Le istanze spot possono essere riprese solo se la capacità è disponibile e il prezzo spot è inferiore o uguale al prezzo massimo specificato.

Console

Per riavviare un'istanza ibernata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Seleziona un'istanza sospesa e scegli Instance state (Stato istanza), Start instance (Avvia istanza). Possono essere necessari alcuni minuti affinché l'istanza entri nello stato `running`. In questo periodo di tempo le verifiche dello stato mostrano l'istanza come non riuscita, fino a quando questa non viene avviata.

AWS CLI

Per riavviare un'istanza ibernata

Utilizzare il comando start-instances:

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Per riavviare un'istanza ibernata

Utilizza il cmdlet Start-EC2Instance.

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

Risoluzione dei problemi di ibernazione delle istanze Amazon EC2

Utilizza queste informazioni per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'ibernazione di un'istanza.

Problemi di ibernazione

- Non si riesce a eseguire l'ibernazione immediatamente dopo il lancio
- La transizione da stopping (in arresto) in stoppede lo stato della memoria non viene ripristinato dopo l'avvio
- Istanza «bloccata» nel stopping (in arresto) stato
- Impossibile avviare l'istanza spot subito dopo l'ibernazione
- Ripristino delle istanze spot non riuscito

Non si riesce a eseguire l'ibernazione immediatamente dopo il lancio

Se provi a ibernare un'istanza troppo presto dopo il lancio, ricevi un errore.

Devi aspettare circa due minuti per le istanze Linux e circa cinque minuti per le istanze Windows dopo l'avvio prima di ibernare l'istanza.

La transizione da stopping (in arresto) in stoppede lo stato della memoria non viene ripristinato dopo l'avvio

Se l'istanza che stai ibernando impiega troppo tempo per passare dallo stato `stopping` allo stato `stopped` e lo stato della memoria non viene ripristinato dopo l'avvio, è possibile che l'ibernazione non sia stata configurata in modo appropriato.

Istanze Linux

Verifica il log di sistema dell'istanza e cerca i messaggi correlati all'ibernazione. Per accedere al log di sistema, connettiti all'istanza o usa il comando get-console-output. Trova le righe del log che iniziano con `hibinit-agent`. Se le righe del log indicano un errore o se mancano, molto probabilmente c'è stato un errore di configurazione dell'ibernazione al lancio.

Ad esempio, il messaggio seguente indica che il volume root dell'istanza non è abbastanza grande: `hibinit-agent: Insufficient disk space. Cannot create setup for hibernation. Please allocate a larger root device.`

Se l'ultima riga del log registro da `hibinit-agent` è `hibinit-agent: Running: swapoff / swap`, l'ibernazione è stata configurata correttamente.

Se non vedi log relativi a questi processi, è possibile che l'AMI non supporti l'ibernazione. Per informazioni sulle AMI supportate, vedi Prerequisiti per l'ibernazione dell'istanza EC2. Se hai utilizzato un'AMI Linux personalizzata, verifica di aver seguito le istruzioni per Configurare un'AMI Linux per il supporto dell'ibernazione.

Windows Server 2016 e versioni successive

Verifica il log di avvio EC2 e cerca i messaggi correlati all'ibernazione. Per accedere al log di avvio EC2, connettersi all'istanza da configurare e aprire il file `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\Ec2Launch.log` in un editor di testo. Se utilizzi EC2Launch v2, apri `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Per impostazione predefinita, Windows nasconde i file e le cartelle in `C:\ProgramData`. Per visualizzare le directory e i file di avvio EC2, digitare il percorso in Windows Explorer risorse o modificare le proprietà della cartella per visualizzare i file e le cartelle nascosti.

Individuare le righe di log per l'ibernazione. Se le righe del log indicano un errore o se mancano, molto probabilmente c'è stato un errore di configurazione dell'ibernazione al lancio.

Ad esempio, il seguente messaggio indica che l'ibernazione non è stata configurata: `Message: Failed to enable hibernation.` se il messaggio di errore include valori ASCII decimali, puoi convertire i valori ASCII in testo semplice per leggere il messaggio di errore completo.

Se la riga del log contiene `HibernationEnabled: true`, l'ibernazione è stata configurata correttamente.

Windows Server 2012 R2 e versione precedente

Verifica il log di configurazione EC2 e cerca i messaggi correlati all'ibernazione. Per accedere al log di configurazione EC2, connettersi all'istanza da configurare e aprire il file `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` in un editor di testo. Trovare le righe del log che iniziano con `SetHibernateOnSleep`. Se le righe del log indicano un errore o se mancano, molto probabilmente c'è stato un errore di configurazione dell'ibernazione al lancio.

Ad esempio, il messaggio seguente indica che il volume root dell'istanza non è abbastanza grande: `SetHibernateOnSleep: Failed to enable hibernation: Hibernation failed with the following error: There is not enough space on the disk.`

Se la riga del log è `SetHibernateOnSleep: HibernationEnabled: true`, l'ibernazione è stata configurata correttamente.

Dimensioni delle istanze Windows

Se utilizzi un'istanza Windows T3 o T3a con meno di 1 GiB di RAM, prova ad aumentare la dimensione dell'istanza ad almeno 1 GiB di RAM.

Istanza «bloccata» nel stopping (in arresto) stato

Se hai ibernato un'istanza e questa appare bloccata nello stato `stopping`, puoi forzarne l'arresto. Per ulteriori informazioni, consulta Risoluzione dei problemi di arresto dell'istanza Amazon EC2.

Impossibile avviare l'istanza spot subito dopo l'ibernazione

Se provi ad avviare un'istanza spot entro due minuti dall'ibernazione, potresti ricevere il seguente errore:

`You failed to start the Spot Instance because the associated Spot Instance request is not in an appropriate state to support start.`

Attendi per circa due minuti per le istanze Linux e circa cinque minuti per le istanze Windows, poi riprova ad avviare l'istanza.

Ripristino delle istanze spot non riuscito

Se l'istanza spot è stata ibernata correttamente ma non è stato possibile riattivarla e invece è stata riavviata (un nuovo riavvio in cui lo stato di ibernazione non viene mantenuto), è possibile che i dati dell'utente contenessero lo script seguente:

```
/usr/bin/enable-ec2-spot-hibernation
```

Rimuovi questo script dal campo Dati utente nel modello di avvio, quindi richiedi una nuova istanza spot.

Tieni presente che anche se l'istanza non è stata ripristinata senza che lo stato di ibernazione fosse mantenuto, potrà comunque essere avviata nello stesso modo in cui è stata avviata dallo stato `stopped`.

Riavvio di un'istanza Amazon EC2

Il riavvio di un'istanza equivale al riavvio di un sistema operativo. Nella maggior parte dei casi, sono necessari pochi minuti per riavviare l'istanza.

Quando riavvii un'istanza, mantiene quanto segue:

- Nome DNS pubblico (IPv4)
- Indirizzo IPv4 privato
- Indirizzo IPv4 pubblico
- Indirizzo IPv6 (se applicabile)
- Tutti i dati presenti nei volumi dell'archivio dell'istanza

A differenza dell'arresto e avvio, che dà inizio a un nuovo periodo di fatturazione dell'istanza con addebito minimo di un minuto, il riavvio di un'istanza non comporta l'inizio di un nuovo periodo di fatturazione.

Il riavvio dell'istanza può essere avviato dall'utente (in cui si riavvia manualmente l'istanza) o avviato da AWS (per il ripristino automatico dell'istanza o in risposta a un evento di riavvio pianificato per la manutenzione necessaria, ad esempio per applicare gli aggiornamenti che richiedono un riavvio).

Per i riavvii avviati dall'utente, ti consigliamo di utilizzare la console Amazon EC2, la CLI o l'API anziché eseguire il comando di riavvio del sistema operativo dall'istanza. Quando utilizzi Amazon EC2, se l'istanza non si arresta correttamente entro pochi minuti, Amazon EC2 esegue un riavvio a freddo. Inoltre, AWS CloudTrail crea un record API di quando l'istanza è stata riavviata.

Questo argomento illustra come eseguire un riavvio avviato dall'utente. Per informazioni sui riavvii eseguiti da AWS, consulta e. Ripristino automatico dell'istanza Gestione delle istanze Amazon EC2 per le quali è pianificato il riavvio

> **Important**
>
> Se nell'istanza è in corso l'installazione di aggiornamenti, ti consigliamo di non riavviare o arrestare l'istanza utilizzando la console Amazon EC2 o la riga di comando fino alla completa installazione di tutti gli aggiornamenti. Quando utilizzi la console Amazon EC2 o la riga di comando per riavviare o arrestare l'istanza, sussiste il rischio che l'istanza venga riavviata

a freddo. Un riavvio a freddo durante l'installazione degli aggiornamenti potrebbe rendere instabile l'istanza.

Console

Come riavviare un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza e scegliere Instance state (Stato istanza), Reboot instance (Riavvia istanza).
4. Scegliere Reboot (Riavvia) quando viene richiesta la conferma.

   L'istanza rimane in stato di `running`.

AWS CLI

Per riavviare un'istanza

Usa il comando reboot-instances.

```
aws ec2 reboot-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Come riavviare un'istanza

Utilizza il cmdlet Restart-EC2Instance.

```
Restart-EC2Instance -InstanceId i-1234567890abcdef0
```

Esecuzione di un esperimento di iniezione di guasti controllati

È possibile AWS Fault Injection Service utilizzarlo per verificare la risposta dell'applicazione al riavvio dell'istanza. Per ulteriori informazioni, consulta la Guida per l'utente AWS Fault Injection Service.

Terminare le istanze Amazon EC2

> **Warning**
>
> La terminazione di un'istanza è permanente e irreversibile.
> Dopo aver terminato un'istanza, non puoi più connetterti a essa e non puoi ripristinarla. Inoltre, tutti i volumi Amazon EBS collegati e configurati per essere eliminati in caso di terminazione vengono eliminati in modo definitivo e non possono essere recuperati. Tutti i dati archiviati nei volumi di archivio dell'istanza vengono persi in modo definitivo. Per ulteriori informazioni, consulta Come funziona la terminazione delle istanze.
> Prima di terminare un'istanza, assicurati di aver eseguito il backup di tutti i dati che devi mantenere dopo la terminazione sull'archivio persistente.

Puoi eliminare un'istanza quando non è più necessaria. Questa operazione viene definita interruzione dell'istanza. Appena lo stato di un'istanza cambia in `shutting-down` o `terminated`, vengono bloccati i rispettivi addebiti.

Dopo averla interrotta, non è più possibile connettersi a un'istanza o avviarla. Tuttavia, puoi avviare nuove istanze utilizzando la stessa AMI.

Invece, se preferisci arrestare o ibernare un'istanza, consulta Avvio e arresto di un'istanza Amazon EC2 o Metti in ibernazione la tua istanza Amazon EC2. Per ulteriori informazioni, consulta Differenze tra gli stati dell'istanza.

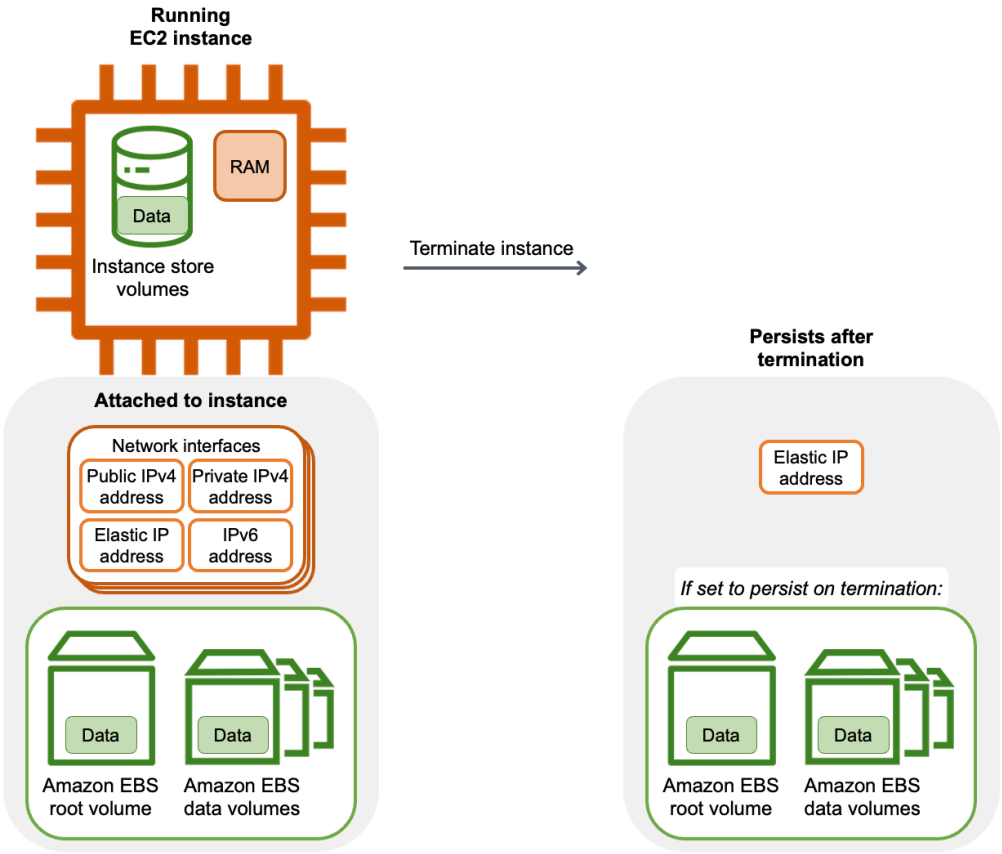
Indice

- Come funziona la terminazione delle istanze
- Metodi per terminare un'istanza
- Terminazione di un'istanza con un corretto spegnimento del sistema operativo
- Terminazione di un'istanza e aggiramento dello spegnimento controllato del sistema operativo
- Risoluzione dei problemi relativi alla terminazione delle istanze
- Modifica della protezione da terminazione dell'istanza
- Modificare il comportamento di arresto avviato dall'istanza
- Conservare i dati quando un'istanza viene terminata

Come funziona la terminazione delle istanze

Quando termini un'istanza, le modifiche sono registrate a livello di sistema operativo (OS) dell'istanza, alcune risorse sono perse e altre persistono.

Il seguente diagramma mostra cosa viene perso e cosa persiste quando un'istanza Amazon EC2 viene terminata. Quando un'istanza è terminata, i dati disponibili sui volumi dell'archivio dell'istanza e i dati memorizzati nella RAM dell'istanza sono cancellati. Eventuali indirizzi IP elastici associati all'istanza vengono scollegati. Per i volumi root e i volumi di dati Amazon EBS, il risultato dipende dall'impostazione Elimina alla terminazione per ciascun volume.



Considerazioni

- Persistenza dei dati
  - Volumi dell'archivio dell'istanza: quando un'istanza termina, tutti i dati sono eliminati in modo definitivo.
  - Volume root EBS:
    - Se collegato al momento dell'avvio, è eliminato per impostazione predefinita quando l'istanza termina.

    - Se collegato dopo l'avvio, persiste per impostazione predefinita quando l'istanza termina.
  - Volumi di dati EBS:
    - Se collegato all'avvio tramite la console: persiste per impostazione predefinita quando l'istanza termina.
    - Se collegato all'avvio utilizzando la CLI: eliminato per impostazione predefinita quando l'istanza termina.
    - Se collegato dopo l'avvio tramite la console o la CLI: persiste per impostazione predefinita quando l'istanza termina.

      > **Note**
      >
      > Continueranno a essere addebitati i costi per volumi che non sono eliminati al momento della terminazione dell'istanza. Puoi modificare l'impostazione in modo che un volume sia eliminato o persista alla terminazione dell'istanza. Per ulteriori informazioni, consulta Conservare i dati quando un'istanza viene terminata.

- Protezione contro la terminazione accidentale
  - Per impedire che un'istanza venga interrotta per errore, è necessario abilitare la protezione da cessazione.
  - Per controllare se un'istanza deve essere arrestata o terminata quando le procedure di arresto vengono avviate dall'istanza, è necessario modificare il comportamento di arresto avviato dall'istanza.
- Script di spegnimento: se esegui uno script durante la terminazione dell'istanza, si potrebbe verificare una terminazione anomala dell'istanza stessa perché non esiste alcun modo per garantire l'esecuzione degli script di arresto. Amazon EC2 tenta di arrestare un'istanza correttamente ed eseguire gli eventuali script di spegnimento del sistema. Tuttavia, alcuni eventi, ad esempio un errore hardware, potrebbero impedire l'esecuzione di questi script di spegnimento del sistema.
- Istanze bare metal: le istanze bare metal x86 non supportano lo spegnimento cooperativo.

Cosa accade se si termina un'istanza

Le modifiche vengono registrate a livello di sistema operativo

- La richiesta dell'API invia un evento di pressione del pulsante al sistema guest.

- Vari servizi di sistema vengono arrestati a seguito dell'evento di pressione del pulsante. L'arresto graceful del sistema è fornito da systemd (Linux) o dal processo di sistema (Windows). L'arresto graceful viene attivato dall'evento di pressione del pulsante di arresto ACPI dall'hypervisor.
- L'arresto ACPI viene avviato.
- L'istanza si spegne dopo l'uscita dal processo di spegnimento controllato. Non c'è un orario di arresto del sistema operativo configurabile. L'istanza rimane visibile nella console per un breve periodo, trascorso il quale la relativa voce viene eliminata automaticamente.

Risorse perse

- I dati archiviati nei volumi dell'instance store.
- Volume root EBS se l'attributo `DeleteOnTermination` è impostato su `true`.
- Volumi di dati EBS (collegati all'avvio o dopo) se l'attributo `DeleteOnTermination` è impostato su `true`.

Risorse mantenute

- Volume root EBS se l'attributo `DeleteOnTermination` è impostato su `false`.
- Volumi di dati EBS (collegati all'avvio o dopo) se l'attributo `DeleteOnTermination` è impostato su `false`.

Testare la risposta dell'applicazione alla terminazione dell'istanza

Puoi usarlo AWS Fault Injection Service per testare come risponde l'applicazione quando l'istanza viene terminata. Per ulteriori informazioni, consulta la Guida per l'utente AWS Fault Injection Service.

Metodi per terminare un'istanza

> **Warning**
>
> La terminazione di un'istanza è permanente e irreversibile.
> Dopo aver terminato un'istanza, non puoi più connetterti a essa e non puoi ripristinarla. Inoltre, tutti i volumi Amazon EBS collegati e configurati per essere eliminati in caso di terminazione vengono eliminati in modo definitivo e non possono essere recuperati. Tutti i dati archiviati nei volumi di archivio dell'istanza vengono persi in modo definitivo. Per ulteriori informazioni, consulta Come funziona la terminazione delle istanze.

Prima di terminare un'istanza, assicurati di aver eseguito il backup di tutti i dati che devi mantenere dopo la terminazione sull'archivio persistente.

Esistono quattro modi per eseguire la terminazione di un'istanza avviata dall'utente: terminazione predefinita, terminazione ignorando lo spegnimento del sistema operativo, terminazione forzata e terminazione forzata ignorando lo spegnimento del sistema operativo. La tabella seguente confronta le differenze chiave tra i due metodi di terminazione:

Note

Non è possibile terminare un'istanza se è abilitata la protezione da cessazione. Per ulteriori informazioni, consulta Change instance termination protection.

Metodo di terminazione	Scopo principale	Caso d'uso	Comando della CLI
Terminazione per impostazione predefinita	Arresto normale dell'istanza con tentativo di spegnimento controllato del sistema operativo.	Tipica terminazione dell'istanza.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0`
Terminazione ignorando lo spegnimento del sistema operativo	Ignora lo spegnimento controllato del sistema operativo quando si termina un'istanza.	Quando si ignora, è necessario lo spegnere il sistema operativo in modo controllato.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0 \ --skip-os-shutdown`

Metodo di terminazione	Scopo principale	Caso d'uso	Comando della CLI
Terminazione forzata	Gestisce le istanze bloccate. Tenta innanzitutto una terminazione predefinita; se l'istanza non riesce a terminare, termina forzatamente l'istanza.	Quando l'istanza è bloccata nello stato `shutting-down` .	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0 \ --force`
Terminazione forzata ignorando lo spegnimento del sistema operativo	La forza termina e ignora lo spegnimento regolare del sistema operativo quando si termina un'istanza.	Quando è necessario terminare forzatamente e ignorare, lo spegnimento controllato del sistema operativo è necessario.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0 \ --force \ --skip-os-shutdown`

Per istruzioni su come utilizzare ogni metodo, consulta quanto segue:

- Terminazione di un'istanza con un corretto spegnimento del sistema operativo
- Terminazione di un'istanza e aggiramento dello spegnimento controllato del sistema operativo
- Termina forzatamente un'istanza

Terminazione di un'istanza con un corretto spegnimento del sistema operativo

Puoi terminare un'istanza utilizzando il metodo di terminazione predefinito, che include un tentativo di spegnimento regolare del sistema operativo. Per ulteriori informazioni, consulta Metodi per terminare un'istanza.

Console

Utilizza il metodo di terminazione predefinita per terminare un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e scegli Stato istanza e Termina (elimina) istanza.
4. Quando viene richiesta la conferma, scegli Termina (elimina).
5. Dopo essere stata terminata, un'istanza rimane visibile per un breve periodo con lo stato `terminated`.

   Se la terminazione non va a buon fine o se un'istanza terminata rimane visibile per più di qualche ora, consulta L'istanza terminata rimane visualizzata.

AWS CLI

Utilizza il metodo di terminazione predefinita per terminare un'istanza

Utilizza il comando terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Utilizza il metodo di terminazione predefinita per terminare un'istanza

Utilizza il cmdlet Remove-EC2Instance.

```
Remove-EC2Instance -InstanceId i-1234567890abcdef0
```

Terminazione di un'istanza e aggiramento dello spegnimento controllato del sistema operativo

Puoi ignorare lo spegnimento controllato del sistema operativo quando si termina un'istanza. Per ulteriori informazioni, consulta Metodi per terminare un'istanza.

Console

Per terminare un'istanza e ignorare lo spegnimento controllato del sistema operativo

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e scegli Stato istanza e Termina (elimina) istanza.
4. In Ignora l'arresto del sistema operativo, seleziona la casella di controllo Ignora lo spegnimento del sistema operativo. Se questa opzione non è mostrata nella console, significa che non è ancora disponibile nella console nell'attuale Regione. Tuttavia, puoi accedere a questa funzionalità utilizzando l'SDK AWS CLI o provare un'altra regione nella console.
5. Scegli Termina (elimina).
6. Dopo essere stata terminata, un'istanza rimane visibile per un breve periodo con lo stato `terminated`.

   Se la terminazione non va a buon fine o se un'istanza terminata rimane visibile per più di qualche ora, consulta L'istanza terminata rimane visualizzata.

AWS CLI

Per terminare un'istanza e ignorare lo spegnimento controllato del sistema operativo

Utilizza il comando terminate-instances con `--skip-os-shutdown`.

```
aws ec2 terminate-instances \
    --instance-ids i-1234567890abcdef0 \
    --skip-os-shutdown
```

PowerShell

Per terminare un'istanza e ignorare lo spegnimento controllato del sistema operativo

Usa il Remove-EC2Instance cmdlet con.. `-SkipOsShutdown $true`

```
Remove-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -SkipOsShutdown $true
```

Risoluzione dei problemi relativi alla terminazione delle istanze

Il richiedente deve disporre dell'autorizzazione per effettuare la chiamata `ec2:TerminateInstances`. Per ulteriori informazioni, consulta Esempi di policy per l'utilizzo delle istanze.

Se termini l'istanza e avvii un'altra istanza, molto probabilmente hai configurato la scalabilità automatica tramite una caratteristica come Parco istanze EC2 o Amazon EC2 Auto Scaling. Per ulteriori informazioni, consulta Istanze avviate o terminate automaticamente.

> **Note**
>
> Non è possibile terminare un'istanza se è abilitata la protezione da cessazione. Per ulteriori informazioni, consulta Change instance termination protection.

Se l'istanza è nello stato `shutting-down` per un periodo più lungo del previsto, puoi tentare di terminarla forzatamente. Se rimane nello stato `shutting-down`, deve essere cancellata (terminata) mediante processi automatizzati all'interno del servizio Amazon EC2. Per ulteriori informazioni, consulta Ritardo della terminazione dell'istanza.

Modifica della protezione da terminazione dell'istanza

Per evitare che la tua istanza sia terminata accidentalmente utilizzando l'API Amazon EC2, indipendentemente dal fatto che tu chiami `TerminateInstances` direttamente o utilizzando un'altra interfaccia come la console Amazon EC2, abilita la protezione dalla terminazione per l'istanza. L'attributo `DisableApiTermination` controlla se l'istanza può essere terminata. Per impostazione di default, la protezione da interruzione è disabilitata per l'istanza. Puoi impostare il valore di questo attributo quando avvii l'istanza, mentre l'istanza è in esecuzione o è arrestata.

L'attributo `DisableApiTermination` non impedisce di terminare un'istanza avviando lo spegnimento dall'istanza stessa (ad esempio, utilizzando un comando del sistema operativo per lo spegnimento del sistema) quando l'attributo `InstanceInitiatedShutdownBehavior` è impostato su `terminate`. Per ulteriori informazioni, consulta Modificare il comportamento di arresto avviato dall'istanza.

Considerazioni

- L'attivazione della protezione dalla terminazione non AWS impedisce la chiusura dell'istanza in caso di evento pianificato per la chiusura dell'istanza.

- L'attivazione della protezione da cessazione non impedisce al Amazon EC2 Auto Scaling di terminare un'istanza quando l'istanza non è integra o durante eventi di riduzione orizzontale. È possibile controllare se un gruppo con dimensionamento automatico può terminare una determinata istanza durante la riduzione utilizzando la protezione per la riduzione delle istanze. È possibile controllare se un gruppo con dimensionamento automatico può terminare istanze non integre sospendendo il processo di dimensionamento ReplaceUnhealthy.
- Non è possibile abilitare la protezione da interruzione per Istanze spot.

Console

Per abilitare la protezione da terminazione per un'istanza all'avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di controllo scegliere Avvia istanza.
3. Espandi Advanced details (Dettagli avanzati). Per la Protezione dalla terminazione, seleziona Abilita.
4. Quando hai finito di specificare i dettagli per l'istanza, scegli Avvia istanza.

Per modificare la protezione da terminazione per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza.
4. Seleziona Azioni, Impostazioni istanza, Modifica protezione da terminazione.
5. Per la Protezione dalla terminazione, seleziona o annulla Abilita.
6. Scegli Save (Salva).

AWS CLI

Per abilitare la protezione da terminazione per un'istanza

Utilizza il comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-termination
```

Per disabilitare la protezione da terminazione per un'istanza

Utilizza il comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-termination
```

PowerShell

Per abilitare la protezione da terminazione per un'istanza

Utilizza il cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiTermination $true
```

Per disabilitare la protezione da terminazione per un'istanza

Utilizza il cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiTermination $false
```

Terminare più istanze con protezione da cessazione

Se si terminano più istanze in più zone di disponibilità nella stessa richiesta e una o più istanze specificate hanno la protezione da cessazione abilitata, la richiesta ha esito negativo con i seguenti risultati:

- Le istanze specificate nella stessa zona di disponibilità dell'istanza protetta non vengono terminate.
- Le istanze specificate che si trovano in zone di disponibilità diverse, in cui non sono protette altre istanze specificate, vengono terminate correttamente.

Esempio

Supponiamo di avere le seguenti quattro istanze in due zone di disponibilità.

Istanza	Zona di disponibilità	Protezione da cessazione
Istanza 1	AZ A	`Disabled`
Istanza 2		`Disabled`
Istanza 3	AZ B	`Enabled`
Istanza 4		`Disabled`

Se si tenta di terminare tutte queste istanze nella stessa richiesta, la richiesta segnala un errore con i seguenti risultati:

- Istanza 1 e Istanza 2 vengono terminate correttamente poiché per nessuna delle due istanze è abilitata la protezione da cessazione.
- È impossibile terminare Istanza 3 e Istanza 4 poiché per Istanza 3 è abilitata la protezione da cessazione.

Modificare il comportamento di arresto avviato dall'istanza

> **Warning**
>
> La terminazione di un'istanza è permanente e irreversibile.
> Dopo aver terminato un'istanza, non puoi più connetterti a essa e non puoi ripristinarla. Inoltre, tutti i volumi Amazon EBS collegati e configurati per essere eliminati in caso di terminazione vengono eliminati in modo definitivo e non possono essere recuperati. Tutti i dati archiviati nei volumi di archivio dell'istanza vengono persi in modo definitivo. Per ulteriori informazioni, consulta Come funziona la terminazione delle istanze.
> Prima di terminare un'istanza, assicurati di aver eseguito il backup di tutti i dati che devi mantenere dopo la terminazione sull'archivio persistente.

Per impostazione predefinita, quando si avvia un arresto da un'istanza supportata da Amazon EBS (utilizzando un comando come shutdown o poweroff), l'istanza viene arrestata. Puoi modificare questo comportamento in modo che l'istanza venga terminata invece di modificare l'attributo `InstanceInitiatedShutdownBehavior` per l'istanza. Puoi modificare questo attributo mentre l'istanza è in esecuzione o quando è arrestata.

Il comando halt non avvia un arresto. Se utilizzato, l'istanza non sarà terminata; al contrario, la CPU verrà messa in stato HLT e l'istanza rimarrà in esecuzione.

> **Note**
>
> L'attributo `InstanceInitiatedShutdownBehavior` si applica solo quando si esegue un arresto dal sistema operativo dell'istanza stessa. Non si applica quando si interrompe un'istanza utilizzando l'API `StopInstances` o la console Amazon EC2.

Console

Modifica del comportamento di arresto avviato dall'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Scegliere Actions (Operazioni), Instance settings (Impostazioni istanza), Change shutdown behavior (Cambia comportamento di arresto).

   Il comportamento di arresto mostra il comportamento corrente.
5. Per modificare il comportamento, in Comportamento di arresto, scegli Arresta o Termina.
6. Scegli Save (Salva).

AWS CLI

Modifica del comportamento di arresto avviato dall'istanza

Utilizza il comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --instance-initiated-shutdown-behavior terminate
```

PowerShell

Modifica del comportamento di arresto avviato dall'istanza

Utilizza il cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -InstanceInitiatedShutdownBehavior terminate
```

Conservare i dati quando un'istanza viene terminata

Quando un'istanza Amazon EC2 è terminata, puoi conservare i dati sui volumi dell'archivio dell'istanza o sui volumi Amazon EBS. Questo argomento descrive come garantire la persistenza dei dati anche dopo la terminazione dell'istanza.

Modalità in cui la terminazione dell'istanza influisce sui volumi di root e di dati

Volumi di archivio dell'istanza

Quando le istanze sono terminate, i volumi dell'archivio dell'istanza sono eliminati automaticamente e i dati sono persi. Per conservare questi dati oltre la durata dell'istanza, prima di terminare l'istanza, devi copiarli manualmente su un'archiviazione più persistente, come un volume Amazon EBS, un bucket Amazon S3 o un file system Amazon EFS. Per ulteriori informazioni, consulta Opzioni di archiviazione per le istanze Amazon EC2.

Volumi Amazon EBS

Quando un'istanza è terminata, i volumi EBS sono eliminati o conservati, a seconda del valore dell'attributo `DeleteOnTermination` per ciascun volume:

- Sì (console)/`true` (CLI): il volume è eliminato quando l'istanza è terminata.
- No (console)/`false`(CLI): il volume è conservato quando l'istanza è terminata. Per i volumi conservati continuano a esserti addebitati i costi.

> **Note**
>
> Una volta terminata un'istanza, puoi acquisire uno snapshot del volume conservato e collegarlo a un'altra istanza. È necessario eliminare un volume per evitare di incorrere in addebiti.

Comportamento di eliminazione predefinito per i volumi EBS

Il valore predefinito `DeleteOnTermination` varia in base al tipo di volume, al fatto che il volume sia stato collegato all'avvio o dopo e al metodo (console o CLI) utilizzato per collegare il volume:

Tipo di volume	Collegato quando	Metodo di collegamento	Comportamento predefinito alla terminazione dell'istanza
Volume root	Al momento dell'avvio	Console o CLI	Elimina
Volume root	Dopo l'avvio	Console o CLI	Preserve
Volume di dati	Al momento dell'avvio	Console	Preserve
Volume di dati	Al momento dell'avvio	CLI	Elimina
Volume di dati	Dopo l'avvio	Console e CLI	Preserve

Verifica delle impostazioni di persistenza del volume

Il valore predefinito all'avvio per un volume EBS è determinato dall'attributo `DeleteOnTermination` impostato sull'AMI. Puoi modificare il valore all'avvio dell'istanza, sovrascrivendo l'impostazione AMI. Consigliamo di verificare l'impostazione predefinita dell'attributo `DeleteOnTermination` dopo l'avvio di un'istanza con un'AMI.

Per verificare se un volume Amazon EBS sarà eliminato al momento della terminazione dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Scegli la scheda Archiviazione.
5. In Blocca dispositivi, scorri verso destra per verificare la colonna Elimina in caso di terminazione.
   - Se l'impostazione è Sì, il volume è eliminato al momento della terminazione dell'istanza.
   - Se l'impostazione è No, il volume non è eliminato al momento della terminazione dell'istanza. Tutti i volumi non eliminati continuano a esserti addebitati i costi.

Modificare il volume root per renderlo persistente all'avvio

Puoi modificare l'attributo `DeleteOnTermination` di un volume root EBS quando avvii un'istanza. Inoltre, puoi utilizzare la procedura seguente per un volume di dati.

Console

Per modificare il volume root di un'istanza per renderlo persistente all'avvio

1. Segui la procedura di avvio di un'istanza, ma non avviare l'istanza finché non avrai completato i seguenti passaggi per modificare il volume root per renderlo persistente.
2. Nel riquadro Configura archiviazione, scegli Avanzate.
3. In Volumi EBS, espandi le informazioni relative al volume root.
4. In Elimina al termine, scegliere No.
5. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

AWS CLI

Per modificare il volume root di un'istanza per renderlo persistente all'avvio

Utilizza il comando run-instances per modificare il valore di `DeleteOnTermination` nella mappatura dei dispositivi a blocchi.

Aggiungere l'opzione `--block-device-mappings`:

```
--block-device-mappings file://mapping.json
```

In `mapping.json`, specifica il nome del dispositivo, ad esempio `/dev/sda1` o `/dev/xvda` e per `DeleteOnTermination` specifica `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
```

```
]
```

PowerShell

Per modificare il volume root di un'istanza per renderlo persistente all'avvio

Utilizzare il New-EC2Instance cmdlet per modificare il valore di `DeleteOnTermination` nella mappatura dei dispositivi a blocchi.

Aggiungere l'opzione `-BlockDeviceMapping`:

```
-BlockDeviceMapping $bdm
```

In `bdm`, specifica il nome del dispositivo, ad esempio `/dev/sda1` o `/dev/xvda` e per `DeleteOnTermination` specifica `false`.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.DeleteOnTermination = false
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "/dev/sda1"
$bdm.Ebs = $ebd
```

Modificare il volume root di un'istanza in esecuzione per renderlo persistente

Puoi modificare il volume root di un'istanza in esecuzione per renderlo persistente. Inoltre, puoi utilizzare la procedura seguente per un volume di dati.

AWS CLI

Per modificare il volume root in modo che persista

Utilizza il comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0  \
    --block-device-mappings file://mapping.json
```

In `mapping.json`, specifica il nome del dispositivo, ad esempio `/dev/sda1` o `/dev/xvda` e per `--DeleteOnTermination` specifica `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

PowerShell

Per modificare il volume root in modo che persista

Utilizza il cmdlet Edit-EC2InstanceAttribute.

Aggiungere l'opzione `-BlockDeviceMapping`:

```
-BlockDeviceMapping $bdm
```

In `bdm`, specifica il nome del dispositivo, ad esempio `/dev/sda1` o `/dev/xvda` e per `DeleteOnTermination` specifica `false`.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.DeleteOnTermination = false
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "/dev/sda1"
$bdm.Ebs = $ebd
```

Ritiro dell'istanza

Un'istanza è pianificata per essere ritirata quando AWS rileva un guasto irreparabile dell'hardware sottostante che ospita l'istanza. Il tipo di volume root dell'istanza determina il comportamento del ritiro dell'istanza:

- Se il volume root dell'istanza è un volume Amazon EBS, l'istanza viene arrestata e puoi avviarla di nuovo in qualsiasi momento. L'avvio di un'istanza arrestata ne comporta la migrazione in un nuovo hardware.
- Se il volume root dell'istanza è un volume di archivio dell'istanza, l'istanza viene terminata e non puoi più utilizzarla di nuovo.

Per ulteriori informazioni sui tipi di eventi relativi alle istanze, consulta Eventi pianificati per le istanze Amazon EC2.

Indice

- Identificazione delle istanze pianificate per il ritiro
- Azioni da intraprendere per i EBS-backed casi previsti per il pensionamento
- Azioni da intraprendere per istanze supportate dall'instance store pianificate per il ritiro

Identificazione delle istanze pianificate per il ritiro

Se l'istanza è pianificata per il ritiro, riceverai un'e-mail prima dell'evento con l'ID dell'istanza e la data del ritiro. Puoi anche verificare se sono presenti istanze pianificate per il ritiro.

> **Important**
>
> Se un'istanza è pianificata per il ritiro, ti consigliamo di intervenire il prima possibile perché l'istanza potrebbe già non essere raggiungibile. Per ulteriori informazioni, consulta Check if your instance is reachable.

Opzioni per identificare le istanze pianificate per il ritiro

- Monitorare l'indirizzo e-mail dei contatti dell'account
- Controllare le istanze

Monitorare l'indirizzo e-mail dei contatti dell'account

Se un'istanza è pianificata per il ritiro, il contatto principale e il contatto operativo dell'account ricevono un'e-mail prima dell'evento che include l'ID dell'istanza e la data in cui è pianificato il ritiro. Per ulteriori informazioni, consulta Aggiornare il contatto principale per il tuo AWS account e Aggiornare i contatti alternativi per il tuo AWS account nella Guida di riferimento. Gestione dell'account AWS

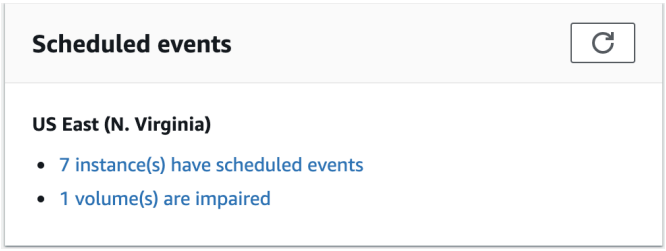
Controllare le istanze

Se usi un account e-mail che non controlli regolarmente, potresti non vedere una notifica di ritiro dell'istanza. Puoi verificare se le istanze sono pianificate per il ritiro in qualsiasi momento.

Console

Per identificare le istanze pianificate per il ritiro

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere EC2 Dashboard (Pannello di controllo EC2). In Scheduled events (Eventi pianificati), è possibile visualizzare gli eventi associati a istanze e volumi Amazon EC2, organizzati per regione.



3. Se nell'elenco viene visualizzata un'istanza con un evento pianificato, selezionare il relativo collegamento sotto il nome della regione per passare alla pagina Events (Eventi).
4. Nella pagina Events (Eventi) sono elencate tutte le risorse e i relativi eventi associati. Per visualizzare le istanze pianificate per il ritiro, selezionare Instance resources (Risorse istanze) nel primo elenco di filtri, quindi Instance stop or retirement (Ritiro o arresto istanze) nel secondo elenco di filtri.
5. Se i risultati dei filtri indicano che un'istanza è pianificata per il ritiro, selezionarla e annotare la data e l'ora riportata nel campo Start time (Ora di avvio) nel riquadro dei dettagli. Questa è la data di ritiro dell'istanza.

AWS CLI

Per individuare le istanze pianificate per il ritiro

Usa il seguente comando describe-instance-status. Ripeti l'operazione in ogni Regione in cui disponi di istanze in esecuzione.

```
aws ec2 describe-instance-status --filters Name=event.code,Values=instance-
retirement
```

PowerShell

Per individuare le istanze pianificate per il ritiro

Utilizza il cmdlet Get-EC2InstanceStatus. Ripeti l'operazione in ogni Regione in cui disponi di istanze in esecuzione.

```
Get-EC2InstanceStatus -Filter @{Name="event.code"; Values="instance-retirement"}
```

Azioni da intraprendere per i EBS-backed casi previsti per il pensionamento

Per conservare i dati sull'istanza pianificata per il ritiro, è possibile eseguire una delle seguenti operazioni. È essenziale che tu esegua questa operazione prima della data di ritiro dell'istanza per evitare tempi di inattività imprevisti o la perdita dei dati.

Per le instanze Linux, Se non hai la certezza che l'istanza sia supportata da EBS o dall'archivio dell'istanza, consulta Volumi root per le tue istanze Amazon EC2.

Controlla se la tua istanza è raggiungibile

Quando si riceve una notifica che l'istanza è pianificata per il ritiro, si consiglia di eseguire le seguenti azioni il prima possibile:

- Controlla se la tua istanza è raggiungibile collegandoti a o eseguendo il ping all'istanza.
- Se la tua istanza è raggiungibile, dovresti stop/start programmarla in un momento opportuno prima della data prevista per il pensionamento, quando l'impatto sarà minimo. Per ulteriori informazioni su arresto e avvio dell'istanza e sulle conseguenze previste in caso di arresto dell'istanza, ad esempio effetti sugli indirizzi IP pubblici, privati ed elastici associati all'istanza, consulta Avvio e arresto di un'istanza Amazon EC2. Si noti che i dati sui volumi instance store vengono persi quando si arresta e si avvia l'istanza.
- Se l'istanza non è raggiungibile, è necessario intervenire immediatamente ed eseguire una procedura stop/start per ripristinare l'istanza.
- In alternativa, se si desidera terminare l'istanza, pianificare di farlo il prima possibile in modo da interrompere gli addebiti per l'istanza.

Creare un backup dell'istanza

Crea un' EBS-backed AMI dalla tua istanza in modo da avere un backup. Per garantire l'integrità dei dati, arrestare l'istanza prima di creare l'AMI. Puoi attendere la data di ritiro pianificato (quando l'istanza viene arrestata) oppure arrestare manualmente l'istanza prima della data di ritiro. Puoi avviare di nuovo l'istanza in qualsiasi momento. Per ulteriori informazioni, consulta Crea un' EBS-backed AMI Amazon.

Avviare un'istanza sostitutiva

Dopo aver creato un'AMI dall'istanza, è possibile utilizzare l'AMI per avviare un'istanza sostitutiva. Dalla console Amazon EC2, seleziona la tua nuova AMI, quindi scegli Avvia istanza dall'AMI. Configura i parametri per la tua istanza, quindi scegli Avvia istanza. Per ulteriori informazioni su ciascun campo, consultare Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

Azioni da intraprendere per istanze supportate dall'instance store pianificate per il ritiro

Per conservare i dati sull'istanza pianificata per il ritiro, è possibile eseguire una delle seguenti operazioni. È essenziale che tu esegua questa operazione prima della data di ritiro dell'istanza per evitare tempi di inattività imprevisti o la perdita dei dati.

> **Warning**
>
> Se l'istanza dispone di un volume root di archivio dell'istanza e supera la data di ritiro, viene terminata e non puoi recuperare l'istanza stessa o i dati in essa archiviati. Indipendentemente dal tipo di volume root dell'istanza, i dati sui volumi di archivio dell'istanza vanno persi quando l'istanza viene ritirata, anche se sono collegati a un'istanza con un volume root EBS.

Controlla se la tua istanza è raggiungibile

Quando si riceve una notifica che l'istanza è pianificata per il ritiro, si consiglia di eseguire le seguenti azioni il prima possibile:

- Controlla se la tua istanza è raggiungibile collegandoti a o eseguendo il ping all'istanza.
- Se la tua istanza è irraggiungibile, probabilmente c'è molto poco che può essere fatto per recuperare la tua istanza. Per ulteriori informazioni, consultaRisoluzione di problemi relativi a un'istanza Amazon EC2 irraggiungibile. AWS terminerà l'istanza alla data di pensionamento prevista, quindi, per un'istanza irraggiungibile, è possibile chiudere immediatamente l'istanza personalmente.

Avviare un'istanza sostitutiva

Crea un'Amazon S3-backed AMI dalla tua istanza utilizzando gli strumenti AMI, come descritto in. Crea un' S3-backed AMI Amazon Dalla console Amazon EC2, seleziona la tua nuova AMI, quindi scegli Avvia istanza dall'AMI. Configura i parametri per la tua istanza, quindi scegli Avvia istanza.

Per ulteriori informazioni su ciascun campo, consultare Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

Converti la tua istanza in un' EBS-backed istanza

Trasferire i dati in un volume EBS, acquisire uno snapshot del volume e quindi creare AMI dallo snapshot. Puoi avviare un'istanza di sostituzione dalla nuova AMI. Per ulteriori informazioni, consulta Converti la tua Amazon AMI in un'AMI S3-backed EBS-backed.

Ripristino automatico dell'istanza

> **Important**
>
> Questa sezione descrive come configurare in modo proattivo i meccanismi di ripristino su un'istanza EC2. Tali meccanismi sono progettati per ripristinare la disponibilità dell'istanza quando AWS rileva un problema hardware o software sottostante a causa del quale un controllo dello stato del sistema ha esito negativo. Se al momento riscontri problemi di accesso all'istanza, consulta Troubleshoot EC2 instances.

Se AWS rileva che un'istanza non è disponibile a causa di un problema hardware o software sottostante, esistono due meccanismi in grado di ripristinare automaticamente la disponibilità dell'istanza: il ripristino automatico semplificato e il ripristino basato sulle azioni di Amazon CloudWatch. Il ripristino della disponibilità dell'istanza è noto anche come ripristino dell'istanza.

Durante il processo di ripristino dell'istanza, AWS tenterà di spostare l'istanza dall'host con il problema hardware o software sottostante a un host diverso. Se viene eseguito correttamente, il processo di ripristino dell'istanza verrà visualizzato dall'istanza come riavvio non programmato. Puoi verificare se è avvenuto un ripristino dell'istanza.

In caso di esito negativo del processo di ripristino, l'istanza potrebbe continuare a essere eseguita sull'host che presenta il problema hardware o software sottostante. In tal caso, è richiesto un intervento manuale. Se l'istanza diventa irraggiungibile o se il controllo dello stato del sistema continua ad avere esito negativo, ti consigliamo di arrestare e avviare manualmente l'istanza. Al momento dell'avvio dell'istanza, viene solitamente effettuata la migrazione a un nuovo computer host sottostante. Tuttavia, a differenza del ripristino automatico dell'istanza, in cui quest'ultima mantiene il proprio indirizzo IPv4 pubblico, un'istanza riavviata riceve un nuovo indirizzo IPv4 pubblico a meno che non disponga di un indirizzo IP elastico.

Per usufruire dei meccanismi di ripristino automatico, devi configurarli su un'istanza in anticipo, prima che un controllo dello stato del sistema abbia esito negativo. Per impostazione predefinita, il ripristino automatico semplificato è abilitato durante l'avvio dell'istanza. Facoltativamente, puoi configurare il ripristino basato su CloudWatch azioni di Amazon dopo il lancio. La configurazione di uno di questi meccanismi rende l'istanza più resiliente.

Il ripristino automatico semplificato e il ripristino basato sulle CloudWatch azioni di Amazon sono disponibili solo nelle istanze supportate. Per ulteriori informazioni, consulta Requisiti per l'abilitazione del ripristino automatico semplificato e Requisiti per abilitare il ripristino basato sull'azione CloudWatch.

> **Warning**
>
> Quando AWS ripristina l'istanza a causa di un problema hardware o software sottostante, tieni presente le seguenti conseguenze: i dati archiviati nella memoria volatile (RAM) andranno persi e il tempo di attività del sistema operativo ricomincerà da zero. Inoltre, con il ripristino basato sull' CloudWatch azione, andranno persi anche i dati sui volumi dell'archivio dell'istanza. Per proteggere i dati importanti, consigliamo di creare regolarmente dei backup. Per ulteriori informazioni sulle best practice di backup e ripristino per le istanze EC2, consulta Best practices for Amazon EC2.
>
> I meccanismi di recupero dell'istanza sono progettati per singole istanze. Per indicazioni su come creare un sistema resiliente, consulta Creare un sistema resiliente.

Argomenti

- Concetti chiave del ripristino automatico dell'istanza
- Differenze tra ripristino automatico semplificato e ripristino basato sull' CloudWatch azione
- Creare un sistema resiliente
- Verificare se è avvenuto il ripristino automatico dell'istanza
- Configurare il ripristino automatico semplificato su un'istanza Amazon EC2
- Configurare il ripristino basato sull' CloudWatch azione su un'istanza EC2

Concetti chiave del ripristino automatico dell'istanza

Il ripristino automatico dell'istanza è una funzionalità di Amazon EC2 che ripristina automaticamente la disponibilità di un'istanza quando si verificano guasti hardware o software sottostanti, migliorando la resilienza e l'affidabilità delle istanze EC2.

Di seguito sono riportati alcuni concetti chiave del ripristino automatico dell'istanza:

Opzioni di configurazione

Puoi configurare due meccanismi per supportare il ripristino automatico dell'istanza:

- Ripristino automatico semplificato: abilitato per impostazione predefinita sulle istanze supportate.
- CloudWatch ripristino basato sull'azione: richiede una configurazione manuale sulle istanze supportate.

Verifiche dello stato del sistema

I controlli dello stato del sistema monitorano automaticamente l' AWS infrastruttura su cui viene eseguita l'istanza EC2.

- Se un controllo dello stato del sistema fallisce, AWS avvia il ripristino automatico dell'istanza, che tenta di migrare l'istanza interessata su un hardware diverso.
- Un controllo dello stato del sistema che ha esito negativo indica un problema hardware o software dell'host, non un problema dell'istanza stessa. Il ripristino automatico può ripristinare un'istanza con un controllo dello stato del sistema con esito negativo. Tuttavia, il ripristino automatico non viene eseguito se il solo controllo dello stato dell'istanza ha esito negativo.
- Per informazioni sulle differenze tra i controlli dello stato dell'istanza e del sistema, consulta Types of status checks.

Esempi di problemi hardware o software sottostanti

I problemi hardware o software che possono causare controlli dello stato del sistema con esito negativo includono la perdita di connettività di rete, la perdita di alimentazione del sistema e problemi di software e hardware sull'host fisico che compromettono la possibilità di raggiungere la rete.

Caratteristiche delle istanze ripristinate

Un'istanza ripristinata è identica all'istanza originale, a eccezione degli elementi persi.

Elementi mantenuti:

- ID istanza
- Indirizzi IP pubblici, privati ed elastici
- Metadati delle istanze
- Gruppo di posizionamento
- Volumi EBS collegati
- Zona di disponibilità

Elementi persi:

- Dati archiviati nella memoria volatile (RAM)
- Dati archiviati nei volumi di archiviazione delle istanze (applicabile solo al ripristino basato sull' CloudWatch azione)
- Il tempo di attività del sistema operativo si azzera

Monitoraggio dei controlli dello stato del sistema con CloudWatch

La metrica StatusCheckFailed _System in CloudWatch indica se un controllo dello stato del sistema è stato superato o non è riuscito.

Valore della metrica:

- 0: il controllo dello stato del sistema ha avuto esito positivo.
- 1: il controllo dello stato del sistema ha avuto esito negativo.

Eventi in Health Dashboard

Durante i tentativi di ripristino automatico dell'istanza, AWS invia eventi all'utente in Health Dashboard base al meccanismo di ripristino configurato e al relativo risultato:

- Ripristino automatico semplificato
  - Evento con esito positivo: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`
  - Evento con esito negativo: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`
- CloudWatch ripristino basato sull'azione
  - Evento con esito positivo: `AWS_EC2_INSTANCE_AUTO_RECOVERY_SUCCESS`
  - Evento con esito negativo: `AWS_EC2_INSTANCE_AUTO_RECOVERY_FAILURE`

Differenze tra ripristino automatico semplificato e ripristino basato sull' CloudWatch azione

La tabella seguente confronta le principali differenze tra il ripristino automatico semplificato e il ripristino basato sull' CloudWatch azione.

Punto di confronto	Ripristino automatico semplificato	CloudWatch ripristino basato sull'azione
Configurazione	Abilitato per impostazione predefinita sulle istanze supportate	Richiede la configurazione manuale di CloudWatch allarmi e azioni
Flessibilità	Comportamento di ripristino fisso gestito da AWS	Operazioni e condizioni personalizzabili
Notification	Notifiche di base tramite Health Dashboard	Notifiche personalizzabili tramite SNS
Dimensione istanze metal	Esclusa	Incluso
Volumi di archivio dell'istanza collegati all'avvio	Non supportato per le istanze che collegano volumi di archivio dell'istanza all'avvio	Supportato su tipi di istanze selezionati. Tieni presente che tutti i dati presenti sui volumi di archivio dell'istanza vengono persi durante il recupero dell'istanza.
Tempo di ripristino	Tentativo di ripristino standard	Tentativi di ripristino più veloci rispetto al ripristino automatico semplificato
Risoluzione del problema dell'host durante la migrazione	La migrazione potrebbe essere annullata e l'istanza rimane sull'host originale	La migrazione potrebbe essere annullata e l'istanza rimane sull'host originale
Costo	Nessun costo aggiuntivo	Potrebbe comportare addebiti CloudWatch

Creare un sistema resiliente

Sebbene il ripristino automatico semplificato e il ripristino basato su CloudWatch azioni siano efficaci per mantenere la disponibilità delle singole istanze, AWS consiglia di implementare un'architettura ad alta disponibilità che consenta il failover del traffico verso istanze integre.

Per raggiungere questo obiettivo, prendi in considerazione l'utilizzo di AWS servizi come Elastic Load Balancing (che distribuisce il traffico in entrata su più istanze EC2) e Amazon EC2 Auto Scaling (che regola automaticamente il numero di istanze in base alla domanda e allo stato).

Per ulteriori informazioni sulla creazione di un sistema resiliente e con tolleranza ai guasti basato su istanze EC2, consulta le seguenti risorse:

- Ritorno alle basi: Designing for Failure con EC2 sul canale AWS YouTube
- Disaster Recovery (DR) Architecture on AWS, parte I: Strategie per il ripristino nel cloud sul sito AWS Architecture Blog
- Application Load Balancers User Guide
- Guida per l'utente di Amazon EC2 Auto Scaling
- REL11-BP02 Affidati a risorse affidabili nel Reliability Pillar Framework AWS Well-Architected

Verificare se è avvenuto il ripristino automatico dell'istanza

Se l'istanza sembra essere stata offline e poi riavviata in modo imprevisto, è possibile che sia stata sottoposta al ripristino automatico dell'istanza in risposta a un problema hardware o software sottostante. Puoi verificarlo controllando se sono presenti eventi di ripristino automatico dell'istanza nella Health Dashboard. Puoi anche verificare se è stato rilevato un problema hardware o software sottostante per la tua istanza controllando la metrica StatusCheckFailed _System Amazon CloudWatch .

Controlla gli eventi in Health Dashboard

Quando si verifica un tentativo di ripristino automatico dell'istanza, AWS invia eventi al tuo Health Dashboard. L'evento specifico dipende dal meccanismo di ripristino configurato e dall'esito positivo o negativo del tentativo.

Per verificare la presenza di eventi di ripristino automatico dell'istanza nel Health Dashboard

1. Apri l' Health Dashboard indirizzo https://phd.aws.amazon.com/phd/home #/.

2. Cerca gli eventi associati al ripristino automatico dell'istanza. La presenza di questi eventi può confermare se si è verificato un tentativo di ripristino automatico dell'istanza e con quale risultato.

   - Ripristino automatico semplificato
     - Evento con esito positivo: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`
     - Evento con esito negativo: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`
   - CloudWatch ripristino basato sull'azione
     - Evento con esito positivo: `AWS_EC2_INSTANCE_AUTO_RECOVERY_SUCCESS`
     - Evento con esito negativo: `AWS_EC2_INSTANCE_AUTO_RECOVERY_FAILURE`

Monitora i controlli dello stato del sistema con CloudWatch

Puoi verificare se è stato rilevato un problema hardware o software sottostante per la tua istanza archiviando la metrica StatusCheckFailed _System. CloudWatch Il valore della metrica indica se un controllo dello stato del sistema ha avuto esito positivo (nessun problema hardware o software) o negativo (problema hardware o software).

Per verificare se è stato rilevato un problema hardware o software sottostante

1. Apri la pagina delle metriche CloudWatch della console all'indirizzo? https://console.aws.amazon.com/cloudwatch/home #metricsV2.
2. Verifica di trovarti nella stessa Regione dell'istanza EC2.
3. Incolla la seguente metrica nel campo di ricerca della pagina Metriche e premi Invio.

   ```
   StatusCheckFailed_System
   ```

4. Scegli EC2 > Per-Instance Metriche.
5. Nella tabella, seleziona la casella di controllo accanto all'istanza che desideri verificare.
6. Modifica il periodo di query al periodo in cui sospetti si sia verificato l'evento di recupero.
7. Scegli la scheda Metriche grafiche e, per StatusCheckFailed _System, procedi come segue:

   a. In Statistica, seleziona un'opzione tra Media, Massimo o Minimo.

   b. Per Periodo, scegli 1 minuto.

8. Controllate il valore per _System. StatusCheckFailed

- Valore 0: il controllo dello stato del sistema ha avuto esito positivo, che indica l'assenza di un problema hardware o software sottostante.
- Valore 1: il controllo dello stato del sistema ha avuto esito negativo, che indica la presenza di un problema hardware o software sottostante.

Per ulteriori informazioni, consulta Ripristino automatico dell'istanza.

Configurare il ripristino automatico semplificato su un'istanza Amazon EC2

> **Important**
>
> Questa sezione descrive come configurare in modo proattivo i meccanismi di ripristino su un'istanza EC2. Tali meccanismi sono progettati per ripristinare la disponibilità dell'istanza quando AWS rileva un problema hardware o software sottostante a causa del quale un controllo dello stato del sistema ha esito negativo. Se al momento riscontri problemi di accesso all'istanza, consulta Troubleshoot EC2 instances.

Se AWS rileva che un'istanza non è disponibile a causa di un problema hardware o software sottostante, il ripristino automatico semplificato può ripristinare automaticamente la disponibilità dell'istanza spostando l'istanza dall'host con il problema sottostante a un host diverso.

Se si verifica un ripristino automatico semplificato, AWS invia uno dei seguenti eventi al tuo Dashboard AWS Health, a seconda del risultato:

- Evento con esito positivo: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`
- Evento con esito negativo: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`

Per ricevere un avviso per questi eventi, puoi configurare le notifiche. Per ulteriori informazioni, consulta Creating your first notification configuration in Notifiche all'utente AWS nella Guida per l'utente di Notifiche all'utente AWS . Puoi anche utilizzare EventBridge le regole di Amazon per monitorare gli eventi di ripristino automatico semplificati.

Il ripristino automatico semplificato è abilitato per impostazione predefinita all'avvio di tutte le istanze supportate. Tuttavia, può funzionare solo se un'istanza si trova nello `running` stato, non sono elencati eventi di servizio e c'è capacità disponibile per il tipo di istanza. Dashboard AWS Health In alcune situazioni, per esempio nel caso di interruzioni significative, i limiti di capacità potrebbero

comportare l'esito negativo dei tentativi di recupero. Per ulteriori informazioni, consulta the section called "Risoluzione dei problemi relativi al ripristino automatico semplificato".

Puoi disabilitare il ripristino automatico semplificato durante o dopo il lancio e riabilitarlo in seguito, se necessario.

> **Warning**
>
> Quando AWS ripristina l'istanza a causa di un problema hardware o software sottostante, tieni presente le seguenti conseguenze: i dati archiviati nella memoria volatile (RAM) andranno persi e l'uptime del sistema operativo ricomincerà da zero. Per proteggere i dati importanti, consigliamo di creare regolarmente dei backup. Per ulteriori informazioni sulle best practice di backup e ripristino per le istanze EC2, consulta Best practices for Amazon EC2.
> I meccanismi di recupero dell'istanza sono progettati per singole istanze. Per indicazioni su come creare un sistema resiliente, consulta Creare un sistema resiliente.

Indice

- Requisiti per l'abilitazione del ripristino automatico semplificato
- Configurazione del ripristino automatico semplificato
- Risoluzione dei problemi relativi al ripristino automatico semplificato

Requisiti per l'abilitazione del ripristino automatico semplificato

Il ripristino automatico semplificato può essere abilitato sulle istanze che soddisfano i seguenti criteri:

Tipi di istanza

- Uso generale: A1, M3, M4, M5, M5a, M5n, M5zn, M6a, M6g, M6i, M6in, M7a, M7g, M7i,, M8a, M8aZn M7i-flex, M8g, M8gb, M8gN, M8i, M8in, M8ine, M8ib M8i-flex, M8ib, M8i 9g, T1, T2, T3, T3a, T4g
- Ottimizzato per l'elaborazione: C3, C4, C5, C5a, C5n, C6a, C6g, C6gn, C6i, C6in, C7a, C7g, C7gn, C7i C7i-flex,, C8a, C8g, C8gb, C8gn, C8i C8i-flex, C8in, C8ine, C8ib, C9g
- Memoria ottimizzata: R3, R4, R5, R5a, R5b, R5n, R6a, R6g, R6i, R6in, R7a, R7g, R7i, R7iz, R8a, R8g, R8gb, R8gn, R8i,, R8i-flex, R8in, R8ib, R9g, U-3tb1, U-6tb1, U-9tb1, U-12tb1, U-18tb1, U-24tb1, U7i-6tb, U7i-8tb, U7i-12tb, U7in-16tb, U7in-24tb, U7in-32tb, U7inh-32tb, X1, X1e, X2iZn, X8g, X8i

- Calcolo accelerato: G3, G5g, Inf1, P3, VT1
- High-performance elaborazione: HPC6a, HPC7a, HPC7g, HPC8a

Tenancy

- Condiviso
- Dedicated Instance

  Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2.

Limitazioni

Il ripristino automatico semplificato non è supportato per le istanze con le seguenti caratteristiche:

- Dimensione dell'istanza: istanze `metal`
- Tenancy: host dedicato. Per gli host dedicati, usa il ripristino automatico dell'host dedicato.
- Archiviazione: istanze con volumi di archivio dell'istanza
- Rete: istanze che utilizzano un Elastic Fabric Adapter
- Dimensionamento automatico: istanze appartenenti a un gruppo Auto Scaling
- Manutenzione: istanze attualmente sottoposte a un evento di manutenzione programmato

Configurazione del ripristino automatico semplificato

Il ripristino automatico semplificato è abilitato per impostazione predefinita all'avvio di un'istanza supportata. Puoi impostare il comportamento del ripristino automatico su `disabled` durante o dopo l'avvio dell'istanza.

La configurazione `default` non consente il ripristino automatico semplificato per un'istanza non supportata.

Console

Disabilitare il ripristino automatico semplificato all'avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze), quindi seleziona Launch instance (Avvia istanza).
3. Nella sezione Dettagli avanzati, in Ripristino automatico dell'istanza, scegli Disabilitato.

4. Configura le impostazioni di avvio dell'istanza rimanenti secondo necessità e quindi avvia l'istanza.

Per disabilitare il ripristino automatico semplificato dopo il lancio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e scegli Actions (Operazioni), Instance Settings (Impostazioni istanza), Change auto-recovery behavior (Modifica comportamento di ripristino automatico).
4. Selezionare Off (Disattiva), quindi Save (Salva URL).

Per abilitare il ripristino automatico semplificato dopo il lancio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e scegli Actions (Operazioni), Instance Settings (Impostazioni istanza), Change auto-recovery behavior (Modifica comportamento di ripristino automatico).
4. Scegli Predefinito (attivo), quindi Salva.

AWS CLI

Disabilitare il ripristino automatico semplificato all'avvio

Usa il comando run-instances con l'opzione `--maintenance-options`.

```
--maintenance-options AutoRecovery=Disabled
```

Per disabilitare il ripristino automatico semplificato dopo il lancio

Utilizza il comando modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
    --instance-id i-1234567890abcdef0 \
    --auto-recovery disabled
```

Per abilitare il ripristino automatico semplificato dopo il lancio

Utilizza il comando modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
    --instance-id i-1234567890abcdef0 \
    --auto-recovery default
```

PowerShell

Disabilitare il ripristino automatico semplificato all'avvio

Utilizza il cmdlet New-EC2Instance.

```
-MaintenanceOptions_AutoRecovery Disabled
```

Per disabilitare il ripristino automatico semplificato dopo il lancio

Utilizza il cmdlet Edit-EC2InstanceMaintenanceOption.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId i-1234567890abcdef0 `
    -AutoRecovery Disabled
```

Per abilitare il ripristino automatico semplificato dopo il lancio

Utilizza il cmdlet Edit-EC2InstanceMaintenanceOption.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId i-1234567890abcdef0 `
    -AutoRecovery Enabled
```

Risoluzione dei problemi relativi al ripristino automatico semplificato

Se il recupero dell'istanza tramite ripristino automatico semplificato ha esito negativo, considera i seguenti problemi:

- AWS gli eventi di servizio sono in corso

  Il ripristino automatico semplificato non funziona durante gli eventi di servizio in Dashboard AWS Health. Potresti non ricevere notifiche di errore di ripristino per tali eventi. Consulta la pagina sullo stato di integrità del servizio per informazioni aggiornate sulla disponibilità dei servizi.

- Capacità insufficiente

  L'hardware sostitutivo è temporaneamente insufficiente per eseguire la migrazione dell'istanza.
- Numero massimo di tentativi giornalieri di ripristino raggiunto

  L'istanza ha raggiunto il limite massimo giornaliero consentito di tentativi di ripristino. Successivamente, l'istanza potrebbe venire ritirata se il ripristino automatico ha esito negativo e se viene determinato che la causa principale del controllo dello stato del sistema con esito negativo originale è un deterioramento dell'hardware.

Se l'errore di controllo dello stato del sistema dell'istanza persiste nonostante diversi tentativi di ripristino, consulta Troubleshoot instances with failed status checks per ulteriori indicazioni.

Configurare il ripristino basato sull' CloudWatch azione su un'istanza EC2

> **Important**
>
> Questa sezione descrive come configurare in modo proattivo i meccanismi di ripristino su un'istanza EC2. Tali meccanismi sono progettati per ripristinare la disponibilità dell'istanza quando AWS rileva un problema hardware o software sottostante a causa del quale un controllo dello stato del sistema ha esito negativo. Se al momento riscontri problemi di accesso all'istanza, consulta Troubleshoot EC2 instances.

Se AWS rileva che un'istanza non è disponibile a causa di un problema hardware o software sottostante, il ripristino basato sull'CloudWatch azione può ripristinare automaticamente la disponibilità dell'istanza spostando l'istanza dall'host con il problema sottostante a un host diverso.

Se si verifica un ripristino basato sull' CloudWatch azione, AWS invia uno dei seguenti eventi al tuo Dashboard AWS Health, a seconda del risultato:

- Evento con esito positivo: `AWS_EC2_INSTANCE_AUTO_RECOVERY_SUCCESS`
- Evento con esito negativo: `AWS_EC2_INSTANCE_AUTO_RECOVERY_FAILURE`

Puoi configurare il ripristino basato sull' CloudWatch azione per aggiungere azioni di ripristino agli CloudWatch allarmi Amazon. CloudWatch il ripristino basato sull'azione funziona con la `StatusCheckFailed_System` metrica. CloudWatchil ripristino basato sulle azioni fornisce una granularità dei tempi di risposta al minuto e notifiche Amazon Simple Notification Service (Amazon

SNS) sulle azioni e sui risultati del ripristino. Queste opzioni di configurazione consentono tentativi di ripristino più rapidi con un controllo più granulare sulla risposta agli eventi di errore del controllo dello stato del sistema rispetto al ripristino automatico semplificato. Per ulteriori informazioni sulle CloudWatch opzioni disponibili, consulta Controlli dello stato delle tue istanze.

Tuttavia, il ripristino basato sull' CloudWatch azione può funzionare solo se un'istanza è nello `running` stato, non sono elencati eventi di servizio e c'è capacità disponibile per il tipo di istanza. Dashboard AWS Health In alcune situazioni, per esempio nel caso di interruzioni significative, i limiti di capacità potrebbero comportare l'esito negativo dei tentativi di recupero. Per ulteriori informazioni, consulta the section called "Risoluzione dei problemi".

> **Warning**
>
> Quando AWS ripristina l'istanza a causa di un problema hardware o software sottostante, tieni presente le seguenti conseguenze: i dati archiviati nella memoria volatile (RAM) e nei volumi di archiviazione dell'istanza andranno persi e l'uptime del sistema operativo ricomincerà da zero. Per proteggere i dati importanti, consigliamo di creare regolarmente dei backup. Per ulteriori informazioni sulle best practice di backup e ripristino per le istanze EC2, consulta Best practices for Amazon EC2.
>
> I meccanismi di recupero dell'istanza sono progettati per singole istanze. Per indicazioni su come creare un sistema resiliente, consulta Creare un sistema resiliente.

Indice

- Requisiti per abilitare il ripristino basato sull'azione CloudWatch
- Configurare il ripristino basato CloudWatch sull'azione
- Risolvi gli errori di ripristino basati su CloudWatch azioni

Requisiti per abilitare il ripristino basato sull'azione CloudWatch

CloudWatch il ripristino basato sull'azione può essere abilitato su istanze che soddisfano i seguenti criteri:

Tipi di istanza

- Uso generale: A1, M3, M4, M5, M5a, M5n, M5zn, M6a, M6g, M6i, M6in, M7a, M7g, M7i,, M8a, M8aZn, M8g, M8gb, M8gN, M8i, M8in M7i-flex, M8ine, M8ib, M8ib, M8i 9g, T1, T2, T3, T3a, T4g M8i-flex

- Ottimizzato per l'elaborazione: C3, C4, C5, C5a, C5n, C6a, C6g, C6gn, C6i, C6in, C7a, C7g, C7gn, C7i C7i-flex,, C8a, C8g, C8gb, C8gn, C8i C8i-flex, C8in, C8ine, C8ib, C9g
- Memoria ottimizzata: R3, R4, R5, R5a, R5b, R5n, R6a, R6g, R6i, R6in, R7a, R7g, R7i, R7iz, R8a, R8g, R8gb, R8gn, R8i,,, R8in R8i-flex, R8ib, R9g,,,,,, U-3tb1, U-6tb1, U-9tb1, U-12tb1, U-18tb1, U-24tb1, U7i-6tb, U7i-8tb, X1 U7i-12tb U7in-16tb U7in-24tb U7in-32tb, X1e U7inh-32tb, X2idn, X2iEDN, X2iZn, X8g, X8i
- Calcolo accelerato: G3, G5g, Inf1, P3, VT1
- High-performance elaborazione: HPC6a, HPC7a, HPC7g, HPC8a
- Istanze metal: uno qualsiasi dei tipi di istanza precedenti con la dimensione di istanza metal.
- Se i volumi di archivio dell'istanza vengono aggiunti all'avvio: in tal caso, sono supportati solo i tipi di istanza M3, C3, R3, X1, X1e, X2idn, X2iedn

Tenancy

- Condiviso
- Dedicated Instance

  Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2.

Limitazioni

CloudWatch il ripristino basato sull'azione non è supportato per i casi con le seguenti caratteristiche:

- Tenancy: host dedicato. Per gli host dedicati, usa il ripristino automatico dell'host dedicato.
- Rete: istanze che utilizzano un Elastic Fabric Adapter
- Dimensionamento automatico: istanze appartenenti a un gruppo Auto Scaling
- Manutenzione: istanze attualmente sottoposte a un evento di manutenzione programmato

Individuare un tipo di istanza supportato

È possibile visualizzare i tipi di istanza che supportano il ripristino basato sull' CloudWatch azione.

Console

Per visualizzare i tipi di istanza che supportano il ripristino basato sull' CloudWatch azione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel pannello di navigazione a sinistra, scegli Instance Types (Tipi di istanza).
3. Nella barra del filtro, aggiungi il filtro Supporto ripristino automatico = true. La tabella Tipi di istanza mostra tutti i tipi di istanza che supportano il ripristino basato sull' CloudWatch azione.
4. (Facoltativo) Aggiungi filtri per approfondire l'ambito di specifici tipi di istanze di interesse.

AWS CLI

Per visualizzare i tipi di istanza che supportano il ripristino basato sull' CloudWatch azione

Utilizza il comando describe-instance-types con il filtro `auto-recovery-supported`.

```
aws ec2 describe-instance-types \
    --filters Name=auto-recovery-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Per visualizzare i tipi di istanza che supportano il ripristino basato sull' CloudWatch azione

Utilizzare il Get-EC2InstanceType cmdlet con il `auto-recovery-supported` filtro.

```
Get-EC2InstanceType `
    -Filter @{Name="auto-recovery-supported";Values="true"} | `
    Select InstanceType | Sort-Object InstanceType
```

Configurare il ripristino basato CloudWatch sull'azione

Per configurare il ripristino basato sull' CloudWatch azione per un'istanza EC2, crea un CloudWatch allarme che monitora la `StatusCheckFailed_System` metrica per l'istanza specificata. Imposta l'attivazione dell'avviso quando il valore della metrica è 1, che indica un controllo dello stato del sistema con esito negativo. Configura l'operazione dell'allarme affinché recuperi automaticamente l'istanza quando viene attivato.

Puoi configurare l'allarme utilizzando la console Amazon EC2 o la console. CloudWatch Per le istruzioni, consulta Aggiungi azioni di ripristino agli CloudWatch allarmi Amazon questa guida per l'utente o Adding recovery actions to Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.

Risolvi gli errori di ripristino basati su CloudWatch azioni

Se il ripristino basato sull' CloudWatch azione non riesce a ripristinare l'istanza, considera i seguenti problemi:

- AWS gli eventi di servizio sono in esecuzione

  CloudWatch il ripristino basato sulle azioni non funziona durante gli eventi di servizio in Dashboard AWS Health. Potresti non ricevere notifiche di errore di ripristino per tali eventi. Consulta la pagina sullo stato di integrità del servizio per informazioni aggiornate sulla disponibilità dei servizi.

- Capacità insufficiente

  L'hardware sostitutivo è temporaneamente insufficiente per eseguire la migrazione dell'istanza.

- Numero massimo di tentativi giornalieri di ripristino raggiunto

  L'istanza ha raggiunto il limite massimo giornaliero consentito di tentativi di ripristino. Successivamente, l'istanza potrebbe venire ritirata se il ripristino automatico ha esito negativo e se viene determinato che la causa principale del controllo dello stato del sistema con esito negativo originale è un deterioramento dell'hardware.

Se l'errore di controllo dello stato del sistema dell'istanza persiste nonostante diversi tentativi di ripristino, consulta Troubleshoot instances with failed status checks per ulteriori indicazioni.

Utilizzo dei metadati dell'istanza per gestire l'istanza EC2

I metadati dell'istanza sono dati relativi all'istanza che puoi utilizzare per configurare o gestire un'istanza in esecuzione. I metadati dell'istanza includono quanto segue:

Proprietà dei metadati dell'istanza

I metadati dell'istanza sono suddivisi in categorie, ad esempio, nome host, eventi e gruppi di sicurezza.

Dati dinamici

I dati dinamici sono metadati generati all'avvio dell'istanza, ad esempio un documento di identità dell'istanza. Per ulteriori informazioni, consulta Categorie dei dati dinamici.

Dati utente

Puoi anche utilizzare i metadati dell'istanza per accedere ai dati utente da te specificati quando un'istanza viene avviata. Ad esempio, puoi specificare i parametri per configurare l'istanza o includere un semplice script. Inoltre, puoi creare AMI generiche e utilizzare i dati utente per modificare i file di configurazione forniti all'avvio. Ad esempio, se esegui server Web per delle piccole attività commerciali, tutte potranno utilizzare la stessa AMI generica e recuperare i loro contenuti dal bucket Amazon S3 specificato nei dati utente all'avvio. Per aggiungere un nuovo cliente in qualsiasi momento, crea un bucket per il cliente, aggiungi il relativo contenuto e avvia l'AMI con il nome bucket univoco fornito al codice nel dati utente. Se avvii più di un'istanza alla volta utilizzando la stessa chiamata `RunInstances`, i dati utente sono disponibili per tutte le istanze presenti all'interno della prenotazione. Ogni istanza che fa parte della stessa prenotazione dispone di un numero `ami-launch-index` univoco che consente di scrivere il codice che controlla ciò che fa l'istanza. Ad esempio, il primo host potrebbe scegliere se stesso come nodo originale in un cluster. Per un esempio di avvio dell'AMI dettagliato, consulta Identificazione di ciascuna istanza lanciata in una singola richiesta.

Important

Anche se puoi accedere ai metadati dell'istanza e ai dati utente solo dall'interno dell'istanza stessa, i dati non sono protetti mediante metodi di autenticazione o crittografia. Chiunque disponga dell'accesso diretto all'istanza, e potenzialmente qualsiasi software in esecuzione sull'istanza, può visualizzare i propri metadati. Pertanto, è opportuno non memorizzare dati sensibili, ad esempio password o chiavi di crittografia di lunga durata, come dati utente.

Indice

- Categorie di metadati dell'istanza
- Categorie dei dati dinamici
- Accesso ai metadati dell'istanza per un'istanza EC2
- Configurazione delle opzioni del servizio di metadati di istanza
- Esegui i comandi quando avvii un'istanza EC2 con l'input dei dati utente
- Identificazione di ciascuna istanza lanciata in una singola richiesta

Categorie di metadati dell'istanza

Le proprietà dei metadati dell'istanza sono suddivise in categorie. Per recuperare le proprietà dei metadati dell'istanza, specifica la categoria nella richiesta e i metadati verranno restituiti nella risposta.

Quando vengono rilasciate nuove categorie, viene creata una nuova build di metadati di istanza con un nuovo numero di versione. Nella tabella che segue, la colonna Version when category was released (Versione in cui è stata rilasciata la categoria) specifica la versione di build quando è stata rilasciata una categoria di metadati dell'istanza. Per evitare di dover aggiornare il codice ogni volta che Amazon EC2 rilascia una nuova build di metadati dell'istanza, utilizza `latest` invece del numero di versione nelle richieste di metadati. Per ulteriori informazioni, consulta Recupero delle versioni disponibili dei metadati dell'istanza.

Quando Amazon EC2 rilascia una nuova categoria di metadati dell'istanza, i metadati dell'istanza per la nuova categoria potrebbero non essere disponibili per le istanze esistenti. Con Nitro-based le istanze, puoi recuperare i metadati delle istanze solo per le categorie disponibili al momento del lancio. Per le istanze con l'hypervisor Xen, è possibile arrestare e avviare l'istanza per aggiornare le categorie disponibili.

Nella tabella seguente sono elencate le categorie di metadati dell'istanza. Alcuni dei nomi delle categorie includono segnaposti per i dati univoci dell'istanza. Ad esempio, *`mac`* rappresenta l'indirizzo MAC per l'interfaccia di rete. Quando richiami i metadati dell'istanza, devi sostituire i segnaposti con i valori effettivi.

Categoria	Description	Versione in cui è stata rilasciata la categoria
`ami-id`	ID dell'AMI utilizzata per avviare l'istanza.	1.0
`ami-launch-index`	Se si avviano più istanze utilizzando la stessa chiamata `RunInstances`, questo valore indica l'ordine di avvio per ciascuna istanza. Il valore della prima istanza avviata è 0. Se avvii istanze utilizzando il dimensionamento automatico	1.0

Categoria	Description	Versione in cui è stata rilasciata la categoria
	o il parco EC2, questo valore è sempre 0.	
`ami-manifest-path`	Percorso del file manifest dell'AMI in Amazon S3. Se hai utilizzato un'Amazon EBS-backed AMI per avviare l'istanza, il risultato restituit o è`unknown`.	1.0
`ancestor-ami-ids`	ID dell'AMI di qualsiasi istanza raggruppata per creare l'AMI corrente. Questo valore esiste solo se il file manifest dell'AMI contiene una chiave `ancestor-amis` .	10-10-2007
`autoscaling/target-lifecycle-state`	Valore che mostra lo stato del ciclo di vita di Auto Scaling di destinazi one a cui sta passando un'istanza di Auto Scaling. Presente quando l'istanza passa a uno degli stati del ciclo di vita di destinazione dopo il 10 marzo 2022. Valori possibili: `Detached` | `InService` | `Standby` | `Terminated` | `Warmed:Hibernated` | `Warmed:Running` | `Warmed:St opped` | `Warmed:Terminated` . Consulta la sezione Recupero dello stato del ciclo di vita tramite i metadati dell'istanza nella Guida per l'utente di Amazon EC2 Auto Scaling.	15/07/2021
`block-device-mapping/ ami`	Il dispositivo virtuale che contiene il file system. root/boot	15-12-2007

Categoria	Description	Versione in cui è stata rilasciata la categoria
`block-device-mapping/ebsN`	Dispositivi virtuali associati a qualsiasi volume Amazon EBS. I volumi Amazon EBS sono disponibili solo nei metadati se erano presenti al momento dell'avvio o quando l'istanza è stata avviata per l'ultima volta. N indica il valore di indice del volume Amazon EBS (ad esempio `ebs1` o `ebs2`).	15-12-2007
`block-device-mapping/ephemeral N`	I dispositivi virtuali per qualsiasi volume instance store non NVMe. La N indica l'indice di ogni volume. Il numero di volumi instance store nella mappatura del dispositivo a blocchi potrebbero non corrispon dere al numero effettivo dei volumi instance store per l'istanza. Il tipo di istanza determina il numero di volumi instance store disponibi li per un'istanza. Se il numero di volumi instance store in una mappatura dei dispositivi a blocchi supera il numero disponibile per un'istanza, i volumi instance store aggiuntivi vengono ignorati.	15-12-2007
`block-device-mapping/root`	Dispositivi o partizioni virtuali associati ai dispositivi o alle partizioni radice sul dispositivo virtuale, dove il file system radice (/ o C:) è associato all'istanza specificata.	15-12-2007

Categoria	Description	Versione in cui è stata rilasciata la categoria
`block-device-mapping/swap`	Dispositivi virtuali associati a `swap`. Non sempre presenti.	15-12-2007
`events/maintenance/history`	Se sono presenti eventi di manutenzione completati o cancellati per l'istanza, contiene una stringa JSON con informazioni sugli eventi.	17-08-2018
`events/maintenance/scheduled`	Se sono presenti eventi di manutenzione attivi per l'istanza , contiene una stringa JSON con informazioni sugli eventi. Per ulteriori informazioni, consulta Visualizzare gli eventi pianificati che influiscono sulle istanze Amazon EC2.	17-08-2018
`events/recommendations/rebalance`	Ora approssimativa, in UTC, in cui viene emessa la notifica della raccomandazione di ribilanciamento dell'istanza EC2 per l'istanza. Di seguito è riportato un esempio dei metadati per questa categoria: `{"noticeTime": "2020-11-05T08:22:00Z"}` . Questa categoria è disponibile solo dopo che la notifica è stata emessa. Per ulteriori informazioni, consulta Raccomandazioni per il ribilanciamento delle istanze EC2.	27-10-2020

Categoria	Description	Versione in cui è stata rilasciata la categoria
`hostname`	Se l'istanza EC2 utilizza la IP-based denominazione (IPBN), questo è il nome host DNS IPv4 privato dell'istanza. Se l'istanza EC2 utilizza la Resource-based denominazione (RBN), si tratta dell'RBN. Se sono presenti più interfacce di rete, fa riferimento al dispositivo eth0 (il dispositivo per il quale il numero di dispositivo è 0). Per ulteriori informazioni su IPBN e RBN, consultare Hostname e domini delle istanze EC2.	1.0
`iam/info`	Se all'istanza è associato un ruolo IAM, contiene informazioni sull'ultimo aggiornamento del profilo dell'istanza, inclusa la LastUpdated data dell'istanza e. InstanceProfileArn InstanceProfileId In caso contrario, non presente.	12-01-2012
`iam/security-credentials/role-name`	Se è associato un ruolo IAM all'istanza, *`role-name`* è il nome del ruolo e *`role-name`* contiene le credenziali di sicurezza temporanee associate al ruolo (per ulteriori informazioni, consultaRecupero delle credenziali di sicurezza dai metadati delle istanze). In caso contrario, non presente.	12-01-2012

Categoria	Description	Versione in cui è stata rilasciata la categoria
`identity-credentials/ec2/info`	Informazioni sulle credenziali in `identity-credentials/ec2/security-credentials/ec2-instance` .	23/05/2018
`identity-credentials/ec2/security-credentials/ec2-instance`	Credenziali per il ruolo di identità dell'istanza che consentono al software sull'istanza di AWS identificarsi per supportare funzionalità come EC2 Instance Connect e AWS Systems Manager Default Host Management Configuration. A queste credenziali non sono associate politiche, quindi non dispongono di autorizzazioni AWS API aggiuntive oltre all'identificazione dell'istanza della funzionalità. AWS Per ulteriori informazioni, consulta Ruoli di identità dell'istanza per le istanze Amazon EC2.	23/05/2018
`instance-action`	Comunica all'istanza la necessità di un riavvio in preparazione del processo di raggruppamento. Valori validi: `none` | `shutdown` | `bundle-pending` .	01-09-2008
`instance-id`	ID dell'istanza corrente.	1.0
`instance-life-cycle`	L'opzione di acquisto di questa istanza. Per ulteriori informazioni, consulta Opzioni di fatturazione e acquisto di Amazon EC2.	01-10-2019

Categoria	Description	Versione in cui è stata rilasciata la categoria
`instance-type`	Tipo di istanza. Per ulteriori informazioni, consulta Tipi di istanza Amazon EC2.	29-08-2007
`ipv6`	L'indirizzo IPv6 dell'istanza. Se sono presenti più interfacce di rete, fa riferimento all'interfaccia di rete del dispositivo eth0 (il dispositivo per il quale il numero di dispositivo è 0) e al primo indirizzo IPv6 assegnato. Se non esiste un indirizzo IPv6 sull'interfaccia di rete [0], questo elemento non viene impostato e viene restituita una risposta HTTP 404.	03/01/2021
`kernel-id`	ID del kernel avviato con questa istanza, se applicabile.	01-02-2008
`local-hostname`	Se sono presenti più interfacce di rete, fa riferimento al dispositivo eth0 (il dispositivo per il quale il numero di dispositivo è 0). Se l'istanza EC2 utilizza la IP-based denominazione (IPBN), questo è il nome host DNS IPv4 privato dell'istanza. Se l'istanza EC2 utilizza la Resource-based denominazione (RBN), si tratta dell'RBN. Per ulteriori informazioni sulla denominazione delle istanze IPBN, RBN ed EC2, consultare Hostname e domini delle istanze EC2.	19-01-2007

Categoria	Description	Versione in cui è stata rilasciata la categoria
`local-ipv4`	Indirizzo IPv4 privato dell'istanza. Se sono presenti più interfacce di rete, fa riferimento al dispositivo eth0 (il dispositivo per il quale il numero di dispositivo è 0). Se si tratta di un' IPv6-onlyistanza, questo elemento non è impostato e genera una risposta HTTP 404.	1.0
`mac`	Indirizzo MAC (Media Access Control) dell'istanza. Se sono presenti più interfacce di rete, fa riferimento al dispositivo eth0 (il dispositivo per il quale il numero di dispositivo è 0).	01-01-2011
`metrics/vhostmd`	Non più disponibile.	2011-05-01
`network/interfaces/macs/mac/device-number`	Numero di dispositivo univoco associato all'interfaccia specificata. Il numero di dispositivo corrisponde al nome del dispositivo, ad esempio `device-number` pari a 2 indica il dispositivo eth2. Questa categoria corrisponde ai campi `DeviceIndex` e `device-index` utilizzati dall'API Amazon EC2 e ai comandi EC2 per AWS CLI.	01-01-2011
`network/interfaces/macs/mac/interface-id`	L'ID dell'interfaccia di rete.	01-01-2011

Categoria	Description	Versione in cui è stata rilasciata la categoria
`network/interfaces/macs/mac/ipv4-associations/public-ip`	Indirizzi IPv4 privati associati a ogni indirizzo IP pubblico e assegnati all'interfaccia specificata.	01-01-2011
`network/interfaces/macs/mac/ipv6s`	Indirizzi IPv6 associati all'interfaccia.	30-06-2016
`network/interfaces/macs/mac/ipv6-prefix`	Prefissi IPv6 assegnati all'interfaccia di rete.	
`network/interfaces/macs/mac/local-hostname`	Il nome host DNS IPv4 privato dell'interfaccia di rete. Questo valore non è impostato per le interfacce senza alcun indirizzo IP, come le interfacce. EFA-only Se si tratta di un'IPv6-only interfaccia, questo è il nome basato sulla risorsa. Per ulteriori informazioni su IPBN e RBN, consultare Hostname e domini delle istanze EC2.	19-01-2007
`network/interfaces/macs/mac/local-ipv4s`	Indirizzi IPv4 privati associati all'interfaccia. Se si tratta di un'interfaccia IPv6-only di rete, questo elemento non è impostato e genera una risposta HTTP 404.	01-01-2011
`network/interfaces/macs/mac/mac`	Indirizzo MAC dell'istanza.	01-01-2011
`network/interfaces/macs/`*`mac`*`/network-card`	L'indice della scheda di rete. Alcuni tipi di istanza supportano più schede di rete.	2020-11-01

Categoria	Description	Versione in cui è stata rilasciata la categoria
`network/interfaces/macs/mac/owner-id`	ID del proprietario dell'interfaccia di rete. In ambienti con più interfacce, un'interfaccia può essere collegata mediante una terza parte, ad esempio Elastic Load Balancing . Il traffico di un'interfaccia viene sempre addebitato al proprietario dell'interfaccia.	01-01-2011
`network/interfaces/macs/mac/public-hostname`	DNS pubblico (IPv4) dell'interfaccia. Questa categoria viene restituita solo se l'attributo `enableDnsHostnames` è impostato su `true`. Per ulteriori informazioni, consulta Attributi DNS per il VPC nella Guida per l'utente di Amazon VPC. Se l'istanza ha solo un indirizzo IPv6 pubblico e nessun indirizzo IPv4 pubblico, questo elemento non è impostato e restituisce una risposta HTTP 404.	01-01-2011
`network/interfaces/macs/mac/public-ipv4s`	L'indirizzo IP pubblico o gli indirizzi IP elastici associati all'interfaccia. In un'istanza possono essere presenti più indirizzi IPv4.	01-01-2011
`network/interfaces/macs/mac/security-groups`	Gruppi di sicurezza a cui appartiene l'interfaccia di rete.	01-01-2011

Categoria	Description	Versione in cui è stata rilasciata la categoria
`network/interfaces/macs/mac/security-group-ids`	ID dei gruppi di sicurezza a cui appartiene l'interfaccia di rete.	01-01-2011
`network/interfaces/macs/mac/subnet-id`	ID della sottorete in cui si trova l'interfaccia di rete.	01-01-2011
`network/interfaces/macs/mac/subnet-ipv4-cidr-block`	Blocco CIDR IPv4 della sottorete in cui si trova l'interfaccia di rete.	01-01-2011
`network/interfaces/macs/mac/subnet-ipv6-cidr-blocks`	Blocco CIDR IPv6 della sottorete in cui si trova l'interfaccia di rete.	30-06-2016
`network/interfaces/macs/mac/vpc-id`	ID del VPC in cui si trova l'interfaccia di rete.	01-01-2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-block`	Blocco CIDR IPv4 primario del VPC.	01-01-2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-blocks`	Blocchi CIDR IPv4 del VPC.	30-06-2016
`network/interfaces/macs/mac/vpc-ipv6-cidr-blocks`	Blocco CIDR IPv6 del VPC in cui si trova l'interfaccia di rete.	30-06-2016
`placement/availability-zone`	zona di disponibilità in cui l'istanza è stata avviata.	01-02-2008

Categoria	Description	Versione in cui è stata rilasciata la categoria
`placement/availability-zone-id`	ID dell'area di disponibilità statica in cui viene avviata l'istanza. L'ID dell'area di disponibilità è coerente tra gli account. Tuttavia, potrebbe essere diverso dall'area di disponibilità, che può variare in base all'account.	01-10-2019
`placement/group-name`	Nome del gruppo di posiziona mento in cui viene avviata l'istanza.	2020-08-24
`placement/host-id`	ID dell'host su cui viene avviata l'istanza. Applicabile solo a Host dedicati.	2020-08-24
`placement/partition-number`	Il numero della partizione in cui viene avviata l'istanza.	2020-08-24
`placement/region`	La AWS regione in cui viene avviata l'istanza.	2020-08-24
`product-codes`	Marketplace AWS codici di prodotto associati all'istanza, se presenti.	01-03-2007

Categoria	Description	Versione in cui è stata rilasciata la categoria
`public-hostname`	Il DNS pubblico dell'istanza (IPv4). Questa categoria viene restituit a solo se l'attributo `enableDns Hostnames` è impostato su `true`. Per ulteriori informazi oni, consulta Attributi DNS per il VPC nella Guida per l'utente di Amazon VPC. Se l'istanza ha solo un indirizzo IPv6 pubblico e nessun indirizzo IPv4 pubblico, questo elemento non è impostato e restituisce una risposta HTTP 404.	19-01-2007
`public-ipv4`	Indirizzo IPv4 pubblico. Se un indirizzo IP elastico è associato all'istanza, il valore restituito è l'indirizzo IP elastico.	19-01-2007
`public-keys/0/openssh-key`	Chiave pubblica. Disponibile solo se viene specificato in fase di avvio dell'istanza.	1.0
`ramdisk-id`	ID del disco RAM specificato in fase di avvio, se applicabile.	10-10-2007
`reservation-id`	ID della prenotazione.	1.0
`security-groups`	Nomi dei gruppi di sicurezza applicati all'istanza. Dopo l'avvio puoi modificare i gruppi di sicurezza delle istanze. Tali modifiche sono riportate qui e in network/interfaces /macs/ / security-groups. *mac*	1.0

Categoria	Description	Versione in cui è stata rilasciata la categoria
`services/domain`	Il dominio delle risorse per la Regione. AWS	25-2-2014
`services/partition`	Partizione in cui si trova la risorsa. Per AWS le regioni standard, la partizione è`aws`. Se sono presenti risorse in altre partizioni, la partizione è `aws-`*`partition name`* . Ad esempio, la partizione per le risorse nella regione Cina (Pechino) è `aws-cn`.	20-10-2015
`spot/instance-action`	Operazione (ibernazione, arresto o terminazione) e orario indicativo, in UTC, in cui si verificherà l'operazione. Questo elemento è presente solo se l'istanza spot è stata contrassegnata per essere ibernata, arrestata o terminata. Per ulteriori informazioni, consulta instance-action.	15-11-2016

Categoria	Description	Versione in cui è stata rilasciata la categoria
`spot/termination-time`	Ora approssimativa, in formato UTC, in cui il sistema operativo dell'istanza spot riceverà il segnale di arresto. Questo elemento è presente e contiene un valore temporale (ad esempio, 2015-01-05T18:02:00Z) solo se l'istanza Spot è stata contrassegnata per la terminazione da Amazon EC2. L'elemento "termination-time" non è impostato su un'ora se termini manualmente l'istanza spot. Per ulteriori informazioni, consulta termination-time.	05-11-2014
`system`	Il tipo di virtualizzazione sottostante (hypervisor) dell'istanza.	24/09/2022
`tags/instance`	I tag istanza associati all'istanza. Disponibile solo se permetti esplicitamente l'accesso ai tag nei metadati dell'istanza. Per ulteriori informazioni, consulta Abilita l'accesso ai tag nei metadati dell'istanza.	2021-03-23

Categorie dei dati dinamici

Nella tabella seguente sono elencate le categorie dei dati dinamici.

Categoria	Description	Versione in cui è stata rilasciata la categoria
`fws/instance-monitoring`	Valore che indica se il cliente ha abilitato il monitoraggio dettagliato di un minuto in. CloudWatch Valori validi: `enabled | disabled`	04-04-2009
`instance-identity/document`	JSON contenente attributi di istanza, come instance-id, indirizzo IP privato e altro. Per informazioni, consulta Documenti di identità dell'istanza per le istanze Amazon EC2.	04-04-2009
`instance-identity/pkcs7`	Utilizzato per verificare l'autenticità e i contenuti del documento in base alla firma. Per informazioni, consulta Documenti di identità dell'istanza per le istanze Amazon EC2.	04-04-2009
`instance-identity/signature`	Dati che possono essere utilizzati da altre parti per verificare la relativa origine e autenticità. Per informazioni, consulta Documenti di identità dell'istanza per le istanze Amazon EC2.	04-04-2009

Accesso ai metadati dell'istanza per un'istanza EC2

Puoi accedere ai metadati delle istanze EC2 dall'interno dell'istanza stessa o dalla console EC2, dall'API, dagli SDK o dalla AWS CLI. Per ottenere le impostazioni correnti dei metadati dell'istanza per un'istanza dalla console o dalla riga di comando, consulta Esegui una query sulle opzioni dei metadati dell'istanza per le istanze esistenti.

Puoi anche modificare i dati utente per le istanze con un volume root EBS. L'istanza deve essere nello stato stopped (arrestato). Per le indicazioni per la console, consulta Aggiornamento dei dati utente dell'istanza. Per un esempio Linux che utilizza l'attributo AWS CLIhttps://docs.aws.amazon.com/cli/latest/reference/ec2/modify-instance-attribute.html modify-instance-attribute. Per un esempio di Windows che utilizza gli Strumenti per Windows, vedi. PowerShell the section called "Dati utente e strumenti per Windows PowerShell"

> **Note**
>
> Non verrà addebitato alcun costo per le richieste HTTP utilizzate per recuperare i metadati dell'istanza e i dati utente.

Considerazioni sull'accesso ai metadati dell'istanza

Per evitare problemi con i metadati delle istanze, considerate quanto segue.

Errori di avvio dell'istanza dovuti all'applicazione di IMDSv2 () **`HttpTokensEnforced=enabled`**

Prima di abilitare l'applicazione di IMDSv2, è necessario che tutto il software sull'istanza supporti IMDSv2, dopodiché è possibile modificare l'impostazione predefinita per disabilitare IMDSv1 (), dopodiché è possibile abilitare l'applicazione. `httpTokens=required` Per ulteriori informazioni, consulta Passaggio all'utilizzo di Servizio di metadati dell'istanza Versione 2.

Formato comando

Il formato del comando varia a seconda che utilizzi il servizio metadati di istanza versione 1 (IMDSv1) o versione 2 (IMDSv2). Per impostazione predefinita, puoi utilizzare entrambi i servizi di metadati dell'istanza. Per richiedere l'utilizzo di IMDSv2, consulta Utilizzo del servizio di metadati di istanza per accedere ai metadati dell'istanza.

Se IMDSv2 è obbligatorio, IMDSv1 non funziona

Se utilizzi IMDSv1 e non ricevi alcuna risposta, è probabile che IMDSv2 sia obbligatorio. Per verificare se IMDSv2 è obbligatorio, seleziona l'istanza per visualizzarne i dettagli. Il valore IMDSv2 indica Obbligatorio (devi utilizzare IMDSv2) o Facoltativo (puoi utilizzare IMDSv2 o IMDSv1).

(IMDSv2) Utilizza /latest/api/token per recuperare il token

L'emissione di richieste PUT a qualsiasi percorso specifico della versione, ad esempio `/2021-03-23/api/token`, farà sì che il servizio dei metadati restituisca errori 403 Accesso negato. Questo è il comportamento previsto.

Versione dei metadati

Per evitare di dover aggiornare il codice ogni volta che Amazon EC2 rilascia una nuova build di metadati dell'istanza, ti consigliamo di utilizzare `latest` nel percorso e non nel numero di versione.

Supporto IPv6

Per recuperare i metadati dell'istanza utilizzando un indirizzo IPv6, assicurati di abilitare e utilizzare l'indirizzo IPv6 dell'IMDS `[fd00:ec2::254]` anziché l'indirizzo IPv4 `169.254.169.254`. L'istanza deve essere un'istanza avviata in una Nitro-based sottorete che supporta IPv6. https://docs.aws.amazon.com/vpc/latest/userguide/configure-subnets.html#subnet-ip-address-range

(Windows) Creazione di AMI personalizzate utilizzando Windows Sysprep

Per assicurarti che l'IMDS funzioni quando avvii un'istanza da un'AMI Windows personalizzata, l'AMI deve essere un'immagine standardizzata creata mediante Windows Sysprep. In caso contrario, l'IMDS non funzionerà. Per ulteriori informazioni, consulta Creare un'AMI Amazon EC2 utilizzando Windows Sysprep.

In un ambiente container, prendi in considerazione la riconfigurazione o l'aumento del limite di hop a 2

Gli AWS SDK utilizzano le chiamate IMDSv2 per impostazione predefinita. Se la chiamata IMDSv2 non riceve risposta, alcuni AWS SDK riprovano la chiamata e, se ancora non riesce, utilizzano IMDSv1. Ciò può comportare un ritardo, soprattutto in un ambiente del container. Per AWS gli SDK che richiedono IMDSv2, se il limite di hop è 1 in un ambiente container, la chiamata potrebbe non ricevere alcuna risposta perché l'accesso al container è considerato un hop di rete aggiuntivo.

Per mitigare questi problemi in un ambiente container, valuta la possibilità di modificare la configurazione in modo da trasferire le impostazioni (ad esempio Regione AWS) direttamente al contenitore o di aumentare il limite di hop a 2. Per ulteriori informazioni, consulta Add defense in depth against open firewalls, reverse proxies, and SSRF vulnerabilities with enhancements to the EC2 Instance Metadata Service. Per informazioni sulla modifica del limite di hop, consulta Modifica del limite di hop di risposta PUT.

Limite di pacchetti al secondo (PPS)

Esiste un limite di 1024 pacchetti al secondo (PPS) per i servizi che utilizzano indirizzi locali del collegamento. Questo limite include l'aggregato di query DNS del risolutore Route 53, richieste del servizio di metadati di istanza (IMDS), richieste Network Time Protocol (NTP) del servizio orario di Amazon e richieste Windows Licensing Service (per istanze basate su Microsoft Windows).

Considerazioni aggiuntive sull'accesso ai dati utente

- I dati utente vengono considerati dati opachi: ciò che indichi è ciò che risulta durante il recupero. È l'istanza a interpretare i dati utente e a intervenire su di essi.
- I dati utente devono essere codificati con base64. A seconda dello strumento o dell'SDK che stai utilizzando, la codifica base64 potrebbe essere eseguita automaticamente. Ad esempio:
  - La console Amazon EC2 può eseguire automaticamente la codifica con base64 oppure accettare input codificati con base64.
  - AWS CLI per impostazione predefinita, la versione 2 esegue automaticamente la codifica base64 dei parametri binari. AWS CLI la versione 1 esegue la codifica base64 del parametro per te. `--user-data`
  - AWS SDK per Python (Boto3) Esegue la codifica in base 64 del parametro per te. `UserData`
- I dati dell'utente sono limitati a 16 KB, in formato raw, prima della codifica base 64. La dimensione di una stringa di lunghezza n dopo la codifica base64 è ceil(n/3)*4.
- I dati utente devono essere decodificati con base64 quando li recuperi. Se recuperi i dati utilizzando i metadati dell'istanza o la console, vengono decodificati automaticamente.
- Se arresti un'istanza, ne modifichi i dati utente e quindi avvii l'istanza, i dati utente aggiornati non vengono eseguiti automaticamente quando si avvia l'istanza. Con le istanze Windows puoi configurare le impostazioni in modo che gli script dei dati utente aggiornati vengano eseguiti una volta all'avvio dell'istanza oppure ogni volta che avvii o riavvii l'istanza.
- I dati utente sono un attributo dell'istanza. Se si crea un'AMI da un'istanza, i dati utente dell'istanza non vengono inclusi nell'AMI.

Accesso ai metadati dell'istanza dall'interno di un'istanza EC2

Dal momento che i metadati dell'istanza sono disponibili dall'istanza in esecuzione, non devi utilizzare la console Amazon EC2 o AWS CLI. Ciò può risultare utile quando sta scrivendo script da eseguire dall'istanza. Ad esempio, puoi accedere all'indirizzo IP locale dell'istanza dai metadati dell'istanza per gestire una connessione a un'applicazione esterna.

Quelli riportati di seguito sono considerati tutti metadati dell'istanza, ma vi si accede in modi diversi. Seleziona la scheda che rappresenta il tipo di metadati dell'istanza a cui desideri accedere per visualizzare ulteriori informazioni.

Metadata

Le proprietà dei metadati dell'istanza sono suddivise in categorie. Per una descrizione di ciascuna categoria di metadati dell'istanza, consulta Categorie di metadati dell'istanza.

Per accedere alle proprietà dei metadati dell'istanza dall'interno di un'istanza in esecuzione, recupera i dati dai seguenti URI IPv4 o IPv6. Gli indirizzi IP sono indirizzi locali di collegamento e sono validi solo dall'istanza. Per ulteriori informazioni, consulta Link-local indirizzi.

IPv4

```
http://169.254.169.254/latest/meta-data/
```

IPv6

```
http://[fd00:ec2::254]/latest/meta-data/
```

Dynamic data

Per recuperare i dati dinamici dall'interno di un'istanza in esecuzione, utilizza i seguenti URI.

IPv4

```
http://169.254.169.254/latest/dynamic/
```

IPv6

```
http://[fd00:ec2::254]/latest/dynamic/
```

Esempi: accesso con cURL

Gli esempi seguenti utilizzano cURL per recuperare le categorie di identità di alto livello dell'istanza.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
```

```
document
signature
dsa2048
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

Esempi: Accesso con PowerShell

Gli esempi seguenti vengono utilizzati PowerShell per recuperare le categorie di identità delle istanze di alto livello.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

Per ulteriori informazioni sui dati dinamici e per esempi di come recuperarli, consulta Documenti di identità dell'istanza per le istanze Amazon EC2.

User data

Per recuperare i dati utente da un'istanza, utilizza i seguenti URI. Per recuperare i dati utente utilizzando l'indirizzo IPv6, è necessario abilitarlo e l'istanza deve essere un'Nitro-based istanza in una sottorete che supporta IPv6.

IPv4

```
http://169.254.169.254/latest/user-data
```

IPv6

```
http://[fd00:ec2::254]/latest/user-data
```

Una richiesta di dati utente restituisce i dati nel formato originale (tipo di contenuto `application/octet-stream`). Se l'istanza non dispone di dati utente, la richiesta restituisce `404 - Not Found`.

Esempi: accesso con cURL per recuperare testo separato da virgola

Gli esempi seguenti utilizzano cURL per recuperare i dati utente specificati come testo separato da virgola.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Esempi: Accedere con per recuperare il testo separato da virgole PowerShell

Gli esempi seguenti vengono utilizzati PowerShell per recuperare i dati utente specificati come testo separato da virgole.

IMDSv2

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri
 http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = Invoke-RestMethod -Headers
 @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
-Method PUT -Uri http://169.254.169.254/latest/api/token} -Method GET -uri
 http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Esempi: accesso con cURL per recuperare uno script

Gli esempi seguenti utilizzano cURL per recuperare i dati utente specificati come script.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-
data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

IMDSv1

```
curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Esempi: Accedere con PowerShell per recuperare uno script

Gli esempi seguenti vengono utilizzati PowerShell per recuperare i dati utente specificati come script.

IMDSv2

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri
 http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

IMDSv1

```
Invoke-RestMethod -uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Esegui una query sulle opzioni dei metadati dell'istanza per le istanze esistenti

Puoi eseguire query sulle opzioni dei metadati dell'istanza per le istanze esistenti.

Console

Per eseguire una query sulle opzioni dei metadati dell'istanza per un'istanza esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona la tua istanza e verifica i seguenti campi:
   - IMDSv2: il valore è Obbligatorio o Facoltativo.
   - Consenti tag nei metadati dell'istanza: il valore è Abilitato o Disabilitato.

4. Dopo aver selezionato l'istanza, scegli Operazioni, Impostazioni istanza, Modifica opzioni dei metadati dell'istanza.

   La finestra di dialogo mostra se il servizio di metadati di istanza è abilitato o disabilitato per l'istanza selezionata.

AWS CLI

Per eseguire una query sulle opzioni dei metadati dell'istanza per un'istanza esistente

Utilizzare il comando describe-instances.

```
aws ec2 describe-instances \
    --instance-id i-1234567898abcdef0 \
    --query 'Reservations[].Instances[].MetadataOptions'
```

PowerShell

Per interrogare le opzioni di metadati dell'istanza per un'istanza esistente utilizzando gli Strumenti per PowerShell

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567898abcdef0).Instances.MetadataOptions
```

Risposte e messaggi di errore

Tutti i metadati dell'istanza vengono restituiti come testo (tipo di contenuto HTTP `text/plain`).

Una richiesta relativa a una risorsa di metadati specifica restituisce il valore appropriato o un codice di errore HTTP `404 - Not Found` se la risorsa non è disponibile.

Una richiesta relativa a una risorsa di metadati generica (l'URI termina con /) restituisce l'elenco delle risorse disponibili o un codice di errore HTTP `404 - Not Found` se la risorsa specificata non è disponibile. Le voci dell'elenco si trovano su righe distinte che terminano con caratteri di avanzamento riga (ASCII 10).

Se una richiesta IMDSv1 non riceve alcuna risposta, è probabile che IMDSv2 sia obbligatorio.

Per richieste effettuate mediante IMDSv2, possono essere restituiti i seguenti codici di errore HTTP:

- `400 - Missing or Invalid Parameters` – La richiesta PUT non è valida.
- `401 - Unauthorized` – La richiesta `GET` utilizza un token non valido. L'operazione consigliata è quella di generare un nuovo token.
- `403 - Forbidden`: la richiesta non è consentita o l'IMDS è disattivato.
- `404 - Not Found`: la risorsa non è disponibile o non esiste alcuna risorsa di questo tipo.
- `503`: Non è stato possibile completare la richiesta. Riprova la richiesta .

Se l'IMDS restituisce un errore, curl stampa il messaggio di errore nell'output e restituisce un codice di stato di operazione riuscita. Il messaggio di errore viene memorizzato nella variabile `TOKEN`, il che causa l'esito negativo dei comandi curl che utilizzano il token. Se chiami curl con l'opzione -f, restituisce un codice di stato di errore in caso di errore del server HTTP. Se abiliti la gestione degli errori, la shell può rilevare l'errore e fermare lo script.

Throttling delle query

La limitazione (della larghezza di banda della rete) delle query viene applicata in base all'istanza, ovvero vengono applicate restrizioni al numero di connessioni simultanee da un'istanza all'IMDS.

Se stai utilizzando l'IMDS per recuperare le credenziali AWS di sicurezza, evita di richiederle durante ogni transazione o contemporaneamente da un numero elevato di thread o processi, poiché ciò potrebbe comportare limitazioni. Consigliamo invece di memorizzare le credenziali nella cache fino all'approssimarsi della relativa data di scadenza. Per ulteriori informazioni sul ruolo IAM e sulle credenziali di sicurezza associate al ruolo, consulta Recupero delle credenziali di sicurezza dai metadati delle istanze.

Se si verifica tale limitazione (della larghezza di banda della rete) durante l'accesso all'IMDS, riprova a eseguire la query con un approccio basato sul backoff esponenziale.

Utilizzo del servizio di metadati di istanza per accedere ai metadati dell'istanza

Puoi accedere ai metadati dell'istanza da un'istanza in esecuzione utilizzando uno dei metodi seguenti:

- Servizio di metadati dell'istanza Versione 2 (IMDSv2): un metodo orientato alla sessione

  Per alcuni esempi, consulta Esempi per IMDSv2.
- Instance Metadata Service Version 1 (IMDSv1): un metodo request/response

  Per alcuni esempi, consulta Esempi per IMDSv1.

Per impostazione predefinita, puoi utilizzare IMDSv1 o IMDSv2 oppure entrambi.

È possibile configurare l'Instance Metadata Service (IMDS) su ciascuna istanza in modo che accetti solo chiamate IMDSv2, il che causerà il fallimento delle chiamate IMDSv1. Per informazioni su come configurare l'istanza per l'utilizzo di IMDSv2, consulta Configurazione delle opzioni del servizio di metadati di istanza.

Le intestazioni `PUT` o `GET` sono esclusive di IMDSv2. Se queste intestazioni sono presenti nella richiesta, la richiesta è destinata a IMDSv2. Se non sono presenti intestazioni, si presume che la richiesta sia destinata a IMDSv1.

Per un'analisi approfondita di IMDSv2, consulta Aggiungere protezione in profondità contro firewall aperti, proxy inversi e vulnerabilità SSRF con miglioramenti al servizio di metadati dell'istanza EC2.

Argomenti

- Funzionamento di Servizio di metadati dell'istanza Versione 2
- Usa un supporto AWS SDK
- Esempi per IMDSv2
- Esempi per IMDSv1

Funzionamento di Servizio di metadati dell'istanza Versione 2

IMDSv2 utilizza richieste orientate alla sessione. Con richieste orientate alla sessione, puoi creare un token di sessione che definisce la durata della sessione, che può essere compresa tra un minimo di un secondo e un massimo di sei ore. Durante la specifica della durata, puoi utilizzare lo stesso token di sessione per le richieste successive. Al termine della durata specificata, è necessario creare un nuovo token di sessione da utilizzare per richieste future.

> **Note**
>
> Negli esempi riportati in questa sezione viene utilizzato l'indirizzo IPv4 del servizio di metadati dell'istanza (IMDS): `169.254.169.254`. Se si recuperano i metadati per le istanze EC2 tramite l'indirizzo IPv6, accertarsi invece di abilitare e utilizzare l'indirizzo IPv6: `[fd00:ec2::254]`. L'indirizzo IPv6 del servizio di metadati dell'istanza (IMDS) è compatibile con i comandi IMDSv2. L'indirizzo IPv6 è accessibile solo sulle Nitro-based istanze di una sottorete (dual stack o solo IPv6). IPv6-supported

L'esempio seguente utilizza uno script della shell e IMDSv2 per recuperare gli elementi di metadati dell'istanza di livello superiore. Ogni esempio:

- Crea un token di sessione della durata di sei ore (21.600 secondi) utilizzando la richiesta PUT
- Memorizza l'intestazione del token di sessione in una variabile denominata `TOKEN` (istanze Linux) oppure `token` (istanze Windows)
- Richiede gli elementi di metadati di livello superiore utilizzando il token

Esempio per Linux

È possibile eseguire due comandi separati o combinarli.

Comandi separati

Innanzitutto, generare un token utilizzando il comando riportato di seguito.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"`
```

Quindi, utilizzare il token per generare elementi di metadati di primo livello utilizzando il seguente comando.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/
```

Comandi combinati

È possibile memorizzare il token e combinare i comandi. L'esempio seguente combina i due comandi precedenti e memorizza l'intestazione del token di sessione in una variabile denominata TOKEN.

> **Note**
>
> Se si verifica un errore nella creazione del token, invece di un token valido nella variabile viene memorizzato un messaggio di errore e il comando avrà esito negativo.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
 && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Dopo aver creato un token, puoi riutilizzarlo finché non scade. Nel comando di esempio seguente, che ottiene l'ID dell'AMI utilizzata per avviare l'istanza, viene riutilizzato il token archiviato memorizzato in `$TOKEN` nell'esempio precedente.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/ami-id
```

Esempio per Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -
Uri http://169.254.169.254/latest/meta-data/
```

Dopo aver creato un token, puoi riutilizzarlo finché non scade. Nel comando di esempio seguente, che ottiene l'ID dell'AMI utilizzata per avviare l'istanza, viene riutilizzato il token archiviato memorizzato in `$token` nell'esempio precedente.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
 -Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Quando utilizzi IMDSv2 per richiedere i metadati dell'istanza, la richiesta deve includere quanto segue:

1. Utilizza una richiesta PUT per inizializzare una sessione al servizio di metadati dell'istanza. La richiesta PUT restituisce un token che deve essere incluso nelle richieste GET successive al servizio di metadati dell'istanza. Il token è obbligatorio per accedere ai metadati utilizzando IMDSv2.
2. Includi il token in tutte le richieste GET inviate all'IMDS. Quando l'uso del token è impostato su `required`, le richieste senza una token valido o con un token scaduto ricevono un codice di errore HTTP `401 - Unauthorized`.
   - Il token è una chiave specifica dell'istanza. Il token non è valido su altre istanze EC2 e verrà rifiutato se si tenta di utilizzarlo all'esterno dell'istanza su cui è stato generato.
   - La richiesta PUT deve includere un'intestazione che specifica il Time To Live (TTL) per il token, in secondi, fino a un massimo di sei ore (21.600 secondi). Il token rappresenta una sessione logica. Il TTL specifica la durata di validità del token e, pertanto, la durata della sessione.

- Dopo che un token scade, per continuare ad accedere ai metadati dell'istanza, è necessario creare una nuova sessione utilizzando un altro PUT.
- Puoi scegliere di riutilizzare un token o creare un nuovo token con ogni richiesta. Per un piccolo numero di richieste, potrebbe essere più semplice generare e utilizzare immediatamente un token ogni volta che devi accedere al servizio di metadati dell'istanza (IMDS). Per maggior efficienza, tuttavia, puoi specificare una durata maggiore per il token e riutilizzarlo, piuttosto che dover riscrivere una richiesta PUT ogni volta che devi richiedere metadati dell'istanza. Non esiste un limite effettivo al numero di token simultanei, ciascuno dei quali rappresenta la propria sessione. Tuttavia, IMDSv2 è ancora vincolato ai normali limiti di connessione e limitazione (della larghezza di banda della rete) di IMDS. Per ulteriori informazioni, consulta Throttling delle query.

HTTP GET e HEAD metodi sono consentiti nelle richieste di metadati delle istanze IMDSv2. PUTle richieste vengono rifiutate se contengono un'intestazione. X-Forwarded-For

Per impostazione predefinita, la risposta alle richieste PUT dispone di un limite di hop della risposta (time-to-live) di 1 a livello del protocollo IP. Se hai bisogno di un limite di hop maggiore, puoi modificarlo usando il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-instance-metadata-options.html AWS CLI modify-instance-metadata-options. Ad esempio, potrebbe essere necessario un limite di hop maggiore per la compatibilità con le versioni precedenti dei servizi container in esecuzione sull'istanza. Per ulteriori informazioni, consulta Modifica delle opzioni dei metadati dell'istanza per le istanze esistenti.

Usa un supporto AWS SDK

Per utilizzare IMDSv2, le istanze EC2 devono utilizzare una versione AWS SDK che supporti l'uso di IMDSv2. Le versioni più recenti di tutti gli SDK supportano l'utilizzo di IMDSv2. AWS

> **Important**
>
> Ti consigliamo di rimanere al passo con i nuovi rilasci degli SDK per poter usufruire delle funzionalità, degli aggiornamenti di sicurezza e delle dipendenze sottostanti più recenti. L'uso continuato di una versione SDK non supportata è sconsigliato ed è a tua discrezione. Per ulteriori informazioni, consulta la pagina Policy di manutenzione degli SDK e degli strumenti AWS nella Guida di riferimento degli SDK e degli strumenti AWS .

Le seguenti sono le versioni minime che supportano l'uso di IMDSv2:

- AWS CLI - 1.16.289
- AWS Tools for Windows PowerShell – 4,0.1.0
- AWS SDK per .NET - 3.3.634.1
- AWS SDK per C++ - 1.7.229
- AWS SDK per Go - 1.25.38
- AWS SDK per Go v2 — 0.19.0
- AWS SDK per Java - 1.11.678
- AWS SDK for Java 2.x - 2.10.21
- AWS SDK per in — 2.722.0 JavaScript Node.js
- AWS SDK per Kotlin - 1.1.4
- AWS SDK per PHP - 3.147.7
- AWS SDK per Python (Botocore) — 1.13.25
- AWS SDK per Python (Boto3) - 1.12.6
- AWS SDK per Ruby - 3.79.0

Esempi per IMDSv2

Esegui i seguenti esempi sull'istanza Amazon EC2 per recuperare i metadati dell'istanza per IMDSv2.

Nelle istanze Windows, puoi usare Windows PowerShell oppure puoi installare cURL o wget. Se installi uno strumento di terze parti su un'istanza Windows, assicurati di leggere attentamente la relativa documentazione, dal momento che le chiamate e l'output potrebbero essere diversi da quanto documentato in questa sede.

Esempi

- Recupero delle versioni disponibili dei metadati dell'istanza
- Recupero degli elementi di metadati di primo livello
- Ottenimento dei valori per gli elementi di metadati
- Recupero dell'elenco di chiavi pubbliche disponibili
- Visualizzazione dei formati in cui è disponibile la chiave pubblica 0
- Recupero della chiave pubblica 0 (nel formato di chiave OpenSSH)
- Recupero dell'ID della sottorete per un'istanza
- Ottenere i tag dell'istanza per un'istanza

Recupero delle versioni disponibili dei metadati dell'istanza

Questo esempio recupera le versioni disponibili dei metadati dell'istanza. Ogni versione fa riferimento a una build dei metadati dell'istanza quando sono state rilasciate nuove categorie di metadati dell'istanza. Le versioni di build dei metadati dell'istanza non sono correlate alle versioni dell'API di Amazon EC2. Le versioni precedenti sono disponibili in presenza di script basati sulla struttura e sulle informazioni presenti in una versione precedente.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
```

```
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Recupero degli elementi di metadati di primo livello

Questo esempio recupera gli elementi di metadati di primo livello. Per ulteriori informazioni sugli elementi nella risposta, consulta Categorie di metadati dell'istanza.

Tieni presente che i tag sono inclusi in questo output solo se hai consentito l'accesso. Per ulteriori informazioni, consulta the section called "Abilita l'accesso ai tag nei metadati dell'istanza".

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
```

```
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
```

```
services/
tags/
```

Ottenimento dei valori per gli elementi di metadati

Gli esempi seguenti consentono di recuperare i valori di alcuni degli elementi di metadati di primo livello che sono stati ottenuti nell'esempio precedente. Queste richieste utilizzano il token memorizzato che è stato creato utilizzando il comando nell'esempio precedente. Il token non deve essere scaduto.

cURL

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Recupero dell'elenco di chiavi pubbliche disponibili

Questo esempio recupera l'elenco delle chiavi pubbliche disponibili.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

Visualizzazione dei formati in cui è disponibile la chiave pubblica 0

Questo esempio mostra i formati in cui è disponibile la chiave pubblica 0.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/
```

```
openssh-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

Recupero della chiave pubblica 0 (nel formato di chiave OpenSSH)

Questo esempio recupera la chiave pubblica 0 (nel formato di chiave OpenSSH).

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Recupero dell'ID della sottorete per un'istanza

In questo esempio viene recuperato l'ID della sottorete per un'istanza.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -
Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Ottenere i tag dell'istanza per un'istanza

Se l'accesso ai tag dell'istanza nei metadati dell'istanza è abilitato, puoi ottenere i tag per un'istanza dai metadati dell'istanza. Per ulteriori informazioni, consulta Recupero dei tag dai metadati dell'istanza.

Esempi per IMDSv1

Esegui i seguenti esempi sull'istanza Amazon EC2 per recuperare i metadati dell'istanza per IMDSv1.

Nelle istanze Windows, puoi usare Windows PowerShell oppure puoi installare cURL o wget. Se installi uno strumento di terze parti su un'istanza Windows, assicurati di leggere attentamente la relativa documentazione, dal momento che le chiamate e l'output potrebbero essere diversi da quanto documentato in questa sede.

Esempi

- Recupero delle versioni disponibili dei metadati dell'istanza
- Recupero degli elementi di metadati di primo livello
- Ottenimento dei valori per gli elementi di metadati
- Recupero dell'elenco di chiavi pubbliche disponibili
- Visualizzazione dei formati in cui è disponibile la chiave pubblica 0
- Recupero della chiave pubblica 0 (nel formato di chiave OpenSSH)
- Recupero dell'ID della sottorete per un'istanza
- Ottenere i tag dell'istanza per un'istanza

Recupero delle versioni disponibili dei metadati dell'istanza

Questo esempio recupera le versioni disponibili dei metadati dell'istanza. Ogni versione fa riferimento a una build dei metadati dell'istanza quando sono state rilasciate nuove categorie di metadati dell'istanza. Le versioni di build dei metadati dell'istanza non sono correlate alle versioni dell'API di Amazon EC2. Le versioni precedenti sono disponibili in presenza di script basati sulla struttura e sulle informazioni presenti in una versione precedente.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/
```

```
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Recupero degli elementi di metadati di primo livello

Questo esempio recupera gli elementi di metadati di primo livello. Per ulteriori informazioni sugli elementi nella risposta, consulta Categorie di metadati dell'istanza.

Tieni presente che i tag sono inclusi in questo output solo se hai consentito l'accesso. Per ulteriori informazioni, consulta the section called "Abilita l'accesso ai tag nei metadati dell'istanza".

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
```

```
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

Ottenimento dei valori per gli elementi di metadati

Questi esempi consentono di recuperare i valori di alcuni degli elementi di metadati di primo livello che sono stati ottenuti nell'esempio precedente.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Recupero dell'elenco di chiavi pubbliche disponibili

Questo esempio recupera l'elenco delle chiavi pubbliche disponibili.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/ 0=my-public-key
```

Visualizzazione dei formati in cui è disponibile la chiave pubblica 0

Questo esempio mostra i formati in cui è disponibile la chiave pubblica 0.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
```

```
openssh-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
openssh-key
```

Recupero della chiave pubblica 0 (nel formato di chiave OpenSSH)

Questo esempio recupera la chiave pubblica 0 (nel formato di chiave OpenSSH).

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
```

```
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Recupero dell'ID della sottorete per un'istanza

In questo esempio viene recuperato l'ID della sottorete per un'istanza.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/network/
interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Ottenere i tag dell'istanza per un'istanza

Se l'accesso ai tag dell'istanza nei metadati dell'istanza è abilitato, puoi ottenere i tag per un'istanza dai metadati dell'istanza. Per ulteriori informazioni, consulta Recupero dei tag dai metadati dell'istanza.

Passaggio all'utilizzo di Servizio di metadati dell'istanza Versione 2

Se desideri configurare le tue istanze in modo che accettino solo chiamate Instance Metadata Service Version 2 (IMDSv2), ti consigliamo di utilizzare i seguenti strumenti e il percorso di transizione.

Argomenti

- Strumenti per la transizione a IMDSv2
- Percorso consigliato per richiedere IMDSv2

Strumenti per la transizione a IMDSv2

I seguenti strumenti possono aiutarvi a identificare, monitorare e gestire la transizione del vostro software da IMDSv1 a IMDSv2. Per le istruzioni su come utilizzare questi strumenti, vedere. Percorso consigliato per richiedere IMDSv2

AWS software

Le versioni più recenti di AWS CLI e gli AWS SDK supportano IMDSv2. Per usare IMDSv2, aggiorna le tue istanze EC2 per utilizzare le versioni più recenti. Per le versioni minime dell' AWS SDK che supportano IMDSv2, consulta. Usa un supporto AWS SDK

Tutti i pacchetti software Amazon Linux 2 e Amazon Linux 2023 supportano IMDSv2. Amazon Linux 2023 disabilita IMDSv1 per impostazione predefinita.

IMDS Packet Analyzer

IMDS Packet Analyzer è uno strumento open source che identifica e registra le chiamate IMDSv1 durante la fase di avvio e le operazioni di runtime dell'istanza. Analizzando questi log, potete identificare con precisione il software che effettua chiamate IMDSv1 sulle vostre istanze e determinare cosa deve essere aggiornato per supportare IMDSv2 solo sulle vostre istanze. Puoi eseguire IMDS Packet Analyzer da una riga di comando o installarlo come servizio. AWS ImdsPacketAnalyzerPer GitHub ulteriori informazioni, consulta su.

CloudWatch

CloudWatch fornisce le due metriche seguenti per il monitoraggio delle istanze:

`MetadataNoToken`— IMDSv2 utilizza sessioni supportate da token, mentre IMDSv1 no. La `MetadataNoToken` metrica tiene traccia del numero di chiamate all'Instance Metadata Service (IMDS) che utilizzano IMDSv1. Monitorando questo parametro a zero, puoi determinare se e quando tutto il software è stato aggiornato per utilizzare IMDSv2.

`MetadataNoTokenRejected`— Dopo aver disabilitato IMDSv1, puoi utilizzare la `MetadataNoTokenRejected` metrica per tenere traccia del numero di volte in cui una chiamata IMDSv1 è stata tentata e rifiutata. Monitorando questa metrica puoi verificare se il software deve essere aggiornato per utilizzare IMDSv2.

Per ogni istanza EC2, queste metriche si escludono a vicenda. Quando IMDSv1 è abilitato (), emette solo. `httpTokens = optional` `MetadataNoToken` Quando IMDSv1 è disabilitato (), emette solo. `httpTokens = required` `MetadataNoTokenRejected` Per sapere quando utilizzare queste metriche, consulta. Percorso consigliato per richiedere IMDSv2

Per ulteriori informazioni, consulta Parametri dell'istanza.

Avvia le API

Nuove istanze: utilizza l'RunInstancesAPI per avviare nuove istanze che richiedono l'uso di IMDSv2. Per ulteriori informazioni, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.

Istanze esistenti: utilizza l'ModifyInstanceMetadataOptionsAPI per richiedere l'uso di IMDSv2 su istanze esistenti. Per ulteriori informazioni, consulta Modifica delle opzioni dei metadati dell'istanza per le istanze esistenti.

Nuove istanze lanciate dai gruppi Auto Scaling: per richiedere l'uso di IMDSv2 su tutte le nuove istanze lanciate dai gruppi Auto Scaling, i gruppi Auto Scaling possono utilizzare un modello di avvio o una configurazione di avvio. Quando crei un modello di avvio o una configurazione di avvio, devi configurare i parametri `MetadataOptions` per richiedere l'utilizzo di IMDSv2. Il gruppo con scalabilità automatica avvia le nuove istanza tramite il nuovo modello di avvio o configurazione di avvio, senza coinvolgere le istanze esistenti.

Istanze esistenti in un gruppo Auto Scaling: utilizza l'ModifyInstanceMetadataOptionsAPI per richiedere l'uso di IMDSv2 su istanze esistenti o termina le istanze e il gruppo Auto Scaling avvierà nuove istanze sostitutive con le impostazioni delle opzioni dei metadati delle istanze definite nel nuovo modello di avvio o nella nuova configurazione di avvio.

AMI

Le AMI configurate con il parametro impostato per avvieranno le istanze che richiedono IMDSv2 per impostazione predefinita. `ImdsSupport v2.0` Amazon Linux 2023 è configurato con. `ImdsSupport = v2.0`

Nuove AMI: utilizza il comando register-image CLI per impostare il `ImdsSupport` parametro su `v2.0` quando crei una nuova AMI.

AMI esistenti: utilizzate il comando CLI modify-image-attribute per impostare il parametro su quando modificate un'AMI esistente. `ImdsSupport v2.0`

Per ulteriori informazioni, consulta Configurazione dell'AMI.

Account-level controlli

È possibile configurare i valori predefiniti per tutte le opzioni di metadati delle istanze a livello di account. I valori predefiniti vengono applicati automaticamente all'avvio di un'istanza. Per ulteriori informazioni, vedere. Configurazione di IMDSv2 come impostazione predefinita per l'account

È inoltre possibile imporre l'obbligo di utilizzare IMDSv2 a livello di account. Quando l'applicazione di IMDSv2 è abilitata:

- Nuove istanze: le istanze configurate per l'avvio con IMDSv1 abilitato non verranno avviate
- Istanze esistenti con IMDSv1 disabilitato: i tentativi di abilitare IMDSv1 su istanze esistenti saranno impediti.
- Istanze esistenti con IMDSv1 abilitato: le istanze esistenti con IMDSv1 già abilitato non saranno interessate.

Per ulteriori informazioni, consulta Applica IMDSv2 a livello di account.

Policy IAM e SCP

Puoi utilizzare una policy IAM o una policy di controllo del AWS Organizations servizio (SCP) per controllare gli utenti come segue:

- Non è possibile avviare un'istanza utilizzando l'RunInstancesAPI a meno che l'istanza non sia configurata per utilizzare IMDSv2.
- Non è possibile modificare un'istanza esistente utilizzando l'ModifyInstanceMetadataOptionsAPI per riattivare IMDSv1.

La policy IAM o SCP deve contenere le chiavi di condizione IAM indicate di seguito:

- `ec2:MetadataHttpEndpoint`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpTokens`

Se un parametro nella chiamata API o CLI non corrisponde allo stato specificato nella policy che contiene la chiave di condizione, la chiamata all'API o alla CLI ha esito negativo con una risposta. `UnauthorizedOperation`

Inoltre, puoi scegliere un livello aggiuntivo di protezione per imporre la modifica da IMDSv1 a IMDSv2. A livello di gestione degli accessi rispetto alle API chiamate tramite le credenziali del ruolo EC2, puoi utilizzare una chiave di condizione nelle policy IAM o nelle policy di controllo dei AWS Organizations servizi (SCP). In particolare, utilizzando la chiave di condizione della policy `ec2:RoleDelivery` con il valore `2.0` nelle policy IAM, le chiamate dell'API effettuate con le credenziali del ruolo EC2 ottenute da IMDSv1 riceveranno una risposta `UnauthorizedOperation`. Lo stesso può essere ottenuto su scala più ampia con tale condizione richiesta da un SCP. Ciò garantisce che le credenziali fornite tramite IMDSv1 non possano essere effettivamente utilizzate per chiamare le API perché qualsiasi chiamata API che non corrisponde alla condizione specificata riceverà un errore. `UnauthorizedOperation`

Per esempi di policy IAM, consulta Utilizzo dei metadati delle istanze. Per ulteriori informazioni sulle policy di controllo dei servizi (SCP), consulta Service control policies nella Guida per l'utente di AWS Organizations .

Politiche dichiarative

Utilizza le politiche dichiarative (una funzionalità di AWS Organizations) per impostare centralmente le impostazioni predefinite degli account IMDS, inclusa l'applicazione di IMDSv2, in tutta l'organizzazione. Per un esempio di policy, consulta la scheda Metadati delle istanze nella sezione Politiche dichiarative supportate della Guida per l'utente. AWS Organizations

Percorso consigliato per richiedere IMDSv2

Utilizzando gli strumenti sopra riportati, consigliamo il seguente percorso per la transizione a IMDSv2:

- Fase 1: Identifica le istanze con IMDSv2=opzionale e verifica l'utilizzo di IMDSv1
- Fase 2: Aggiorna il software a IMDSv2
- Passaggio 3: richiedi IMDSv2 sulle istanze
- Passaggio 4: imposta IMDSV2=Required come predefinito
- Fase 5: Imporre alle istanze di richiedere IMDSv2

Fase 1: Identifica le istanze con IMDSv2=opzionale e verifica l'utilizzo di IMDSv1

Per valutare l'ambito della migrazione a IMDSv2, identifica le istanze configurate per consentire IMDSv1 o IMDSv2 e verifica le chiamate IMDSv1.

1. Identifica le istanze configurate per consentire IMDSv1 o IMDSv2:

   Amazon EC2 console

   1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
   2. Nel riquadro di navigazione, scegliere Instances (Istanze).
   3. Per visualizzare solo le istanze configurate per consentire IMDSv1 o IMDSv2, aggiungi il filtro IMDSv2 = opzionale.
   4. In alternativa, per vedere se IMDSv2 è opzionale o obbligatorio per tutte le istanze, apri la finestra Preferenze (icona a forma di ingranaggio), attiva IMDSv2 e scegli Conferma. Questo aggiunge la colonna IMDSv2 alla tabella Istanze.

AWS CLI

Utilizzate il comando describe-instances e filtrate per, come segue: `metadata-options.http-tokens = optional`

```
aws ec2 describe-instances --filters "Name=metadata-options.http-
tokens,Values=optional" --query "Reservations[*].Instances[*].[InstanceId]" --
output text
```

2. Controlla le chiamate IMDSv1 su ogni istanza:

   Usa la metrica. CloudWatch `MetadataNoToken` Tale parametro mostra il numero di chiamate IMDSv1 al servizio di metadati dell'istanza (IMDS) nelle istanze. Per ulteriori informazioni, consulta Parametri dell'istanza.

3. Identifica il software sulle tue istanze che effettuano chiamate IMDSv1:

   Utilizzate l'IMDS Packet Analyzer open source per identificare e registrare le chiamate IMDSv1 durante la fase di avvio e le operazioni di runtime dell'istanza. Usa queste informazioni per identificare il software da aggiornare e preparare le tue istanze all'uso solo di IMDSv2. Puoi eseguire IMDS Packet Analyzer da una riga di comando o installarlo come servizio.

Fase 2: Aggiorna il software a IMDSv2

Aggiorna tutti gli SDK, le CLI e il software che utilizzano le credenziali di ruolo sulle tue istanze alle versioni. IMDSv2-compatible Per ulteriori informazioni sull'aggiornamento dell'interfaccia a riga di comando (CLI), consulta Installing or updating to the latest version of the AWS CLI nella Guida per l'utente di AWS Command Line Interface .

Passaggio 3: richiedi IMDSv2 sulle istanze

Dopo aver confermato zero chiamate IMDSv1 tramite la `MetadataNoToken` metrica, configura le istanze esistenti in modo che richiedano IMDSv2. Inoltre, configura tutte le nuove istanze in modo che richiedano IMDSv2. In altre parole, disabilita IMDSv1 su tutte le istanze esistenti e nuove.

1. Configura le istanze esistenti per richiedere IMDSv2:

   Amazon EC2 console

   1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza.
4. Seleziona Operazioni, Impostazioni istanza, Modifica opzioni dei metadati dell'istanza.
5. Per IMDSv2, scegli Obbligatorio.
6. Scegli Save (Salva).

AWS CLI

Usa il comando CLI https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/modify-instance-metadata-options.html modify-instance-metadata-options per specificare che deve essere usato solo IMDSv2.

> **Note**
>
> È possibile modificare questa impostazione sulle istanze in esecuzione. La modifica ha effetto immediato senza che sia necessario riavviare l'istanza.

Per ulteriori informazioni, consulta Richiesta dell'uso di IMDSv2.

2. Monitora i problemi dopo aver disabilitato IMDSv1:
   1. Tieni traccia del numero di volte in cui una chiamata IMDSv1 è stata tentata e rifiutata con la metrica. `MetadataNoTokenRejected` CloudWatch
   2. Se la `MetadataNoTokenRejected` metrica registra le chiamate IMDSv1 su un'istanza che presenta problemi software, ciò indica che il software deve essere aggiornato per utilizzare IMDSv2.
3. Configura le nuove istanze in modo che richiedano IMDSv2:

   Amazon EC2 console

   1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
   2. Segui i passaggi per avviare un'istanza.
   3. Espandi i dettagli avanzati e, per la versione dei metadati, scegli solo V2 (token richiesto).

4. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza).

   Per ulteriori informazioni, consulta Configurazione dell'istanza all'avvio.

AWS CLI

AWS CLI: utilizza il comando run-instances e specifica l'utilizzo esclusivo di IMDSv2.

Passaggio 4: imposta IMDSV2=Required come predefinito

È possibile impostare IMDSV2=Required come configurazione predefinita a livello di account o organizzazione. Ciò garantisce che tutte le istanze appena avviate siano configurate automaticamente per richiedere IMDSv2.

1. Imposta l'impostazione predefinita a livello di account:

   Amazon EC2 console

   1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
   2. Nel pannello di navigazione seleziona Pannello di controllo.
   3. Nella scheda Attributi dell'account, in Impostazioni, scegli Protezione e sicurezza dei dati.
   4. In Impostazioni predefinite IMDS, scegli Gestisci.
   5. Per il servizio di metadati di Instance, scegli Abilitato.
   6. Per la versione dei metadati, scegli solo la versione V2 (token richiesto).
   7. Scegliere Aggiorna.

   AWS CLI

   Utilizzate il comando CLI https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/modify-instance-metadata-defaults.html modify-instance-metadata-defaults e specificate e. `--http-tokens required` `--http-put-response-hop-limit 2`

   Per ulteriori informazioni, consulta Configurazione di IMDSv2 come impostazione predefinita per l'account.

2. In alternativa, imposta l'impostazione predefinita a livello di organizzazione utilizzando una politica dichiarativa:

   Utilizza una politica dichiarativa per impostare l'impostazione predefinita dell'organizzazione per IMDSv2 su obbligatoria. Per un esempio di policy, consulta la scheda Metadati dell'istanza nella sezione Politiche dichiarative supportate della Guida per l'utente. AWS Organizations

Fase 5: Imporre alle istanze di richiedere IMDSv2

Dopo aver verificato che non c'è dipendenza da IMDSv1 su nessuna delle tue istanze, ti consigliamo di applicare IMDSv2 su tutte le nuove istanze.

Usa una delle seguenti opzioni per applicare IMDSv2:

1. Applica IMDSv2 con una proprietà dell'account

   È possibile imporre l'uso di IMDSv2 a livello di account per ciascuno. Regione AWS Una volta applicate, le istanze possono essere avviate solo se sono configurate per richiedere IMDSv2. Questa applicazione si applica indipendentemente dalla configurazione dell'istanza o dell'AMI. Per ulteriori informazioni, consulta Applica IMDSv2 a livello di account. Per applicare questa impostazione a livello di organizzazione, imposta una politica dichiarativa. Per un esempio di policy, consulta la scheda Metadati dell'istanza nella sezione Politiche dichiarative supportate della Guida per l'utente. AWS Organizations

   Per evitare un'inversione dell'applicazione, è necessario utilizzare una policy IAM per impedire l'accesso all'API. ModifyInstanceMetadataDefaults Per ulteriori informazioni, consulta Utilizzo di una policy IAM.

   > **Note**
   >
   > Questa impostazione non modifica la versione IMDS delle istanze esistenti, ma blocca l'abilitazione di IMDSv1 sulle istanze esistenti che attualmente hanno IMDSv1 disabilitato.

   > **Warning**
   >
   > Se l'imposizione di IMDSv2 è abilitata e non `httpTokens` è impostata nella configurazione dell'istanza all'avvio, `required` nelle impostazioni dell'account o nella configurazione AMI,

l'avvio dell'istanza fallirà. Per informazioni sulla risoluzione dei problemi, consulta L'avvio di un' IMDSv1-enabled istanza non riesce.

2. In alternativa, applica IMDSv2 utilizzando le seguenti chiavi di condizione IAM o SCP:
   - `ec2:MetadataHttpTokens`
   - `ec2:MetadataHttpPutResponseHopLimit`
   - `ec2:MetadataHttpEndpoint`

   Queste chiavi di condizione controllano l'uso delle API RunInstances e delle CLI ModifyInstanceMetadataOptions corrispondenti. Se viene creata una policy e un parametro nella chiamata API non corrisponde allo stato specificato nella policy utilizzando la chiave di condizione, la chiamata all'API o alla CLI non va a buon e viene restituita la risposta `UnauthorizedOperation`.

   Per esempi di policy IAM, consulta Utilizzo dei metadati delle istanze.

Limitazione dell'accesso al servizio di metadati di istanza

Puoi valutare se utilizzare regole firewall locali per disabilitare l'accesso al servizio di metadati di istanza (IMDS) da alcuni processi o da tutti.

Ad Nitro-based esempio, l'IMDS può essere raggiunto dalla propria rete quando un dispositivo di rete all'interno del VPC, come un router virtuale, inoltra i pacchetti all'indirizzo IMDS e il controllo predefinito sull'istanza è disabilitato. source/destination Per evitare che un'origine esterna al VPC raggiunga l'IMDS, si consiglia di modificare la configurazione dell'appliance di rete per eliminare i pacchetti con l'indirizzo IPv4 di destinazione dell'IMDS `169.254.169.254` e, se hai abilitato l'endpoint IPv6, l'indirizzo IPv6 dell'IMDS `[fd00:ec2::254]`.

Limitazione dell'accesso all'IMDS per le istanze Linux

Utilizzo di iptables per limitare l'accesso

L'esempio seguente utilizza iptables Linux e il relativo modulo `owner` per impedire al server Web Apache (basato sul suo ID utente di installazione predefinito di `apache`) di accedere a 169.254.169.254. Utilizza una regola di rifiuto per rifiutare tutte le richieste dei metadati dell'istanza (IMDSv1 o IMDSv2) da qualsiasi processo in esecuzione come tale utente.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner
 --uid-owner apache --jump REJECT
```

Oppure, puoi valutare di consentire l'accesso solo a utenti o gruppi particolari, utilizzando regole che autorizzano. Le regole che autorizzano potrebbero essere più facili da gestire dal punto di vista della sicurezza, perché richiedono di prendere una decisione sul software che deve poter accedere ai metadati dell'istanza. Se utilizzi regole che autorizzano, è meno probabile che venga accidentalmente concesso al software l'accesso al servizio di metadati (a cui non intendevi accedere) se in seguito modifichi il software o la configurazione su un'istanza. Puoi anche combinare l'utilizzo dei gruppi con le regole che autorizzano, in modo da poter aggiungere e rimuovere utenti da un gruppo autorizzato senza la necessità di modificare la regola firewall.

L'esempio seguente impedisce a tutti i processi di accedere all'IMDS, tranne a quelli in esecuzione nell'account utente `trustworthy-user`.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match
 owner ! --uid-owner trustworthy-user --jump REJECT
```

> **Note**
>
> - Per utilizzare regole firewall locali, è necessario adattare i comandi dell'esempio precedente in base alle proprie esigenze.
> - Per impostazione predefinita, le regole iptables non vengono mantenute tra riavvii del sistema. Possono essere rese persistenti utilizzando funzionalità del sistema operativo non descritte in questo argomento.
> - Il modulo `owner` iptables corrisponde all'appartenenza al gruppo solo se il gruppo è quello primario di un determinato utente locale. Altri gruppi non corrispondono.

Utilizzo di PF o IPFW per limitare l'accesso

Se utilizzi FreeBSD o OpenBSD, puoi anche considerare l'utilizzo di PF o IPFW. Gli esempi seguenti limitano l'accesso all'IMDS al solo utente root.

PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

> **Note**
>
> L'ordine dei comandi PF e IPFW è importante. PF è preimpostato sull'ultima regola corrispondente e IPFW è preimpostato sulla prima regola corrispondente.

Limitazione dell'accesso all'IMDS per le istanze Windows

Utilizzo del firewall Windows per limitare l'accesso

L' PowerShell esempio seguente utilizza il firewall integrato di Windows per impedire al server web di Internet Information Server (in base all'ID utente di installazione predefinito di) di accedere a 169.254.169.254. `NT AUTHORITY\IUSR` Utilizza una regola di rifiuto per rifiutare tutte le richieste dei metadati dell'istanza (IMDSv1 o IMDSv2) da qualsiasi processo in esecuzione come tale utente.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("NT
 AUTHORITY\IUSR")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $BlockPrincipalSDDL = "D:(A;;CC;;;$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service from IIS" -Action
 block -Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $BlockPrincipalSDDL
```

Oppure, puoi valutare di consentire l'accesso solo a utenti o gruppi particolari, utilizzando regole che autorizzano. Le regole che autorizzano potrebbero essere più facili da gestire dal punto di vista della sicurezza, perché richiedono di prendere una decisione sul software che deve poter accedere ai metadati dell'istanza. Se utilizzi regole che autorizzano, è meno probabile che venga accidentalmente concesso al software l'accesso al servizio di metadati (a cui non intendevi accedere) se in seguito modifichi il software o la configurazione su un'istanza. Puoi anche combinare l'utilizzo dei gruppi con

le regole che autorizzano, in modo da poter aggiungere e rimuovere utenti da un gruppo autorizzato senza la necessità di modificare la regola firewall.

L'esempio seguente impedisce l'accesso ai metadati dell'istanza da tutti i processi in esecuzione su un gruppo OS specificato nella variabile `blockPrincipal` (in questo esempio, il gruppo Windows `Everyone`), ad eccezione dei processi specificati in `exceptionPrincipal` (in questo esempio, un gruppo denominato `trustworthy-users`). È necessario specificare entrambi i principali di rifiuto e di autorizzazione perché Windows Firewall, a differenza della regola `! --uid-owner trustworthy-user` in iptables Linux, non fornisce un meccanismo di scelta rapida per consentire solo un principale particolare (utente o gruppo) rifiutando tutti gli altri.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("Everyone")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $exceptionPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("trustworthy-users")
PS C:\> $ExceptionPrincipalSID =
 $exceptionPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptionPrincipalSID)(A;;CC;;;
$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service for
 $($blockPrincipal.Value), exception: $($exceptionPrincipal.Value)" -Action block -
Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $PrincipalSDDL
```

> **Note**
>
> Per utilizzare regole firewall locali, è necessario adattare i comandi dell'esempio precedente in base alle proprie esigenze.

Utilizzo di regole netsh per limitare l'accesso

Puoi considerare di bloccare tutto il software utilizzando regole `netsh`, ma queste sono molto meno flessibili.

```
C:\> netsh advfirewall firewall add rule name="Block metadata service altogether"
 dir=out protocol=TCP remoteip=169.254.169.254 action=block
```

Note

- Per utilizzare regole firewall locali, è necessario adattare i comandi dell'esempio precedente in base alle proprie esigenze.
- Le regole `netsh` devono essere impostate da un prompt dei comandi con privilegi elevati e non possono essere impostate per rifiutare o autorizzare principali particolari.

Configurazione delle opzioni del servizio di metadati di istanza

Il servizio di metadati di istanza (IMDS) viene eseguito localmente su ogni istanza EC2. Le opzioni relative ai metadati dell'istanza si riferiscono a un insieme di configurazioni che controllano l'accessibilità e il comportamento dell'IMDS su un'istanza EC2.

Per ciascuna istanza puoi configurare le seguenti opzioni dei metadati di istanza:

Servizio di metadati di istanza (IMDS): `enabled` | `disabled`

È possibile abilitare o disabilitare l'IMDS su un'istanza. Se disabilitato, né tu né alcun codice sarete in grado di accedere ai metadati di istanza dell'istanza.

L'IMDS ha due endpoint su un'istanza: IPv4 (`169.254.169.254`) e IPv6 (`[fd00:ec2::254]`). Quando abiliti l'IMDS, l'endpoint IPv4 viene abilitato automaticamente. Se desideri abilitare l'endpoint IPv6, è necessario farlo in modo esplicito.

Endpoint IPv6 dell'IMDS: `enabled` | `disabled`

È possibile abilitare in modo esplicito l'endpoint IPv6 dell'IMDS su un'istanza. Quando l'endpoint IPv6 è abilitato, l'endpoint IPv4 rimane abilitato. L'endpoint IPv6 è supportato solo sulle Nitro-based istanze nelle IPv6-supported sottoreti (dual stack o solo IPv6).

Versione dei metadati: `IMDSv1 or IMDSv2 (token optional)` | `IMDSv2 only (token required)`

Quando richiedi i metadati di istanza è necessario un token per le chiamate IMDSv2. Le chiamate IMDSv1 non richiedono un token. È possibile configurare un'istanza per consentire le chiamate IMDSv1 o IMDSv2 (per cui un token è facoltativo) o per consentire solo le chiamate IMDSv2 (per cui è richiesto un token).

Limite di hop di risposta dei metadati: 1–64

Il limite di hop è il numero di hop di rete che la risposta PUT può effettuare. È possibile impostare il limite di hop su un minimo di 1 e un massimo di 64. In un ambiente container, un limite di hop di 1 può causare problemi. Per informazioni su come mitigare questi problemi, consulta le informazioni sugli ambienti container in Considerazioni sull'accesso ai metadati dell'istanza.

Accesso ai tag nei metadati di istanza: `enabled` | `disabled`

È possibile abilitare o disabilitare l'accesso ai tag di un'istanza dai metadati dell'istanza. Per ulteriori informazioni, consulta Visualizza i tag per le istanze EC2 utilizzando i metadati dell'istanza.

Per visualizzare la configurazione corrente di un'istanza, consulta Esegui una query sulle opzioni dei metadati dell'istanza per le istanze esistenti.

Dove configurare le opzioni dei metadati di istanza

Le opzioni dei metadati di istanza possono essere configurate a diversi livelli, come segue:

- Account: è possibile impostare valori predefiniti per le opzioni dei metadati di istanza a livello di account per ciascuna Regione AWS. All'avvio di un'istanza, le opzioni dei metadati dell'istanza vengono impostate automaticamente sui valori a livello di account. È possibile modificare questi valori all'avvio. Account-level i valori predefiniti non influiscono sulle istanze esistenti.
- AMI: quando registri o modifichi un'AMI, puoi impostare il parametro `imds-support` su `v2.0`. Quando un'istanza viene avviata con questa AMI, la versione dei metadati dell'istanza viene impostata automaticamente su IMDSv2 e il limite di hop è impostato su 2.
- Istanza: puoi modificare tutte le opzioni dei metadati dell'istanza su un'istanza all'avvio, ignorando le impostazioni predefinite. È inoltre possibile modificare le opzioni dei metadati dell'istanza dopo l'avvio su un'istanza in esecuzione o interrotta. Tieni presente che le modifiche possono essere limitate da una policy IAM o SCP.

Per ulteriori informazioni, consultare Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze e Modifica delle opzioni dei metadati dell'istanza per le istanze esistenti.

Ordine di precedenza per le opzioni dei metadati di istanza

Il valore per ciascuna opzione dei metadati di istanza viene determinato all'avvio dell'istanza, seguendo un ordine gerarchico di precedenza. La gerarchia, con la precedenza più alta nella parte superiore, è la seguente:

- Precedenza 1: configurazione dell'istanza all'avvio: i valori possono essere specificati nel modello di avvio o nella configurazione dell'istanza. Tutti i valori qui specificati sostituiscono i valori specificati a livello di account o nell'AMI.
- Precedenza 2: impostazioni dell'account: se un valore non viene specificato all'avvio dell'istanza, viene determinato dalle impostazioni a livello di account (che sono impostate per ciascuna istanza). Regione AWS Account-levelle impostazioni includono un valore per ogni opzione di metadati o non indicano alcuna preferenza.
- Precedenza 3: configurazione dell'AMI: se un valore non è specificato all'avvio dell'istanza o a livello di account, viene determinato dalla configurazione dell'AMI. Questo vale solo per gli eventi `HttpTokens` e `HttpPutResponseHopLimit`.

Ciascuna opzione di metadati viene valutata separatamente. L'istanza può essere configurata con una combinazione di configurazione diretta dell'istanza, impostazioni predefinite a livello di account e configurazione dall'AMI.

È possibile modificare il valore di qualsiasi opzione di metadati dopo l'avvio su un'istanza in esecuzione o interrotta, a meno che le modifiche non siano limitate da una policy IAM o SCP.

> **Note**
>
> L'impostazione di imposizione IMDSv2 a livello di account viene valutata dopo che l'ordine di precedenza ha determinato le impostazioni IMDS dell'istanza. Quando l'imposizione di IMDSv2 è abilitata, le istanze abilitate con IMDSv1 falliranno. Per ulteriori informazioni sull'applicazione, vedere. Applica IMDSv2 a livello di account

> **Warning**
>
> Se l'applicazione di IMDSv2 è abilitata e non è stata impostata `required` nella configurazione dell'istanza all'avvio, nelle impostazioni dell'account o nella configurazione AMI, l'avvio `httpTokens` avrà esito negativo.

Esempio 1 — Determinare i valori per le opzioni di metadati

In questo esempio, un'istanza EC2 viene avviata in una regione in cui `HttpPutResponseHopLimit` è impostato su `1` a livello di account. L'AMI specificata ha `ImdsSupport` impostato su `v2.0`. Nessuna opzione di metadati viene specificata direttamente sull'istanza al momento dell'avvio. L'istanza viene avviata con le seguenti opzioni di metadati:

```
"MetadataOptions": {
    ...
    "HttpTokens": "required",
    "HttpPutResponseHopLimit": 1,
    ...
```

Questi valori sono stati determinati nel modo seguente:

- Nessuna opzione di metadati specificata all'avvio: durante l'avvio dell'istanza, i valori specifici per le opzioni di metadati non sono stati forniti né nei parametri di avvio dell'istanza né nel modello di avvio.
- Le impostazioni dell'account hanno priorità successiva: in assenza di valori specifici indicati all'avvio, le impostazioni a livello di account all'interno della Regione hanno la precedenza. Ciò significa che vengono applicati i valori predefiniti configurati a livello di account. In questo caso, `HttpPutResponseHopLimit` era impostato su `1`.
- Le impostazioni AMI hanno priorità per ultime: in assenza di un valore specifico indicato all'avvio o a livello di account per `HttpTokens` (la versione dei metadati di istanza), viene applicata l'impostazione dell'AMI. In questo caso, l'impostazione `ImdsSupport: v2.0` dell'AMI ha determinato che `HttpTokens` era impostato su `required`. Tieni presente che, sebbene l'impostazione `ImdsSupport: v2.0` dell'AMI sia progettata per essere impostata su `HttpPutResponseHopLimit: 2`, è stata sostituita dall'impostazione `HttpPutResponseHopLimit: 1` a livello di account, che ha una priorità più alta.

Esempio 2 — Determinare i valori per le opzioni di metadati

In questo esempio, l'istanza EC2 viene avviata con le stesse impostazioni del precedente Esempio 1, ma con `HttpTokens` impostato su `optional` direttamente sull'istanza al momento dell'avvio. L'istanza viene avviata con le seguenti opzioni di metadati:

```
"MetadataOptions": {
    ...
```

```
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    ...
```

Il valore di `HttpPutResponseHopLimit` è determinato nello stesso modo dell'Esempio 1. Tuttavia, il valore di `HttpTokens` è determinato come segue: le opzioni di metadati configurate sull'istanza al momento dell'avvio hanno la priorità. Anche se l'AMI era configurata con `ImdsSupport: v2.0` (in altre parole, `HttpTokens` è impostato su `required`), il valore specificato nell'istanza all'avvio (`HttpTokens` impostato su `optional`) aveva la precedenza.

Esempio 3: determina i valori per le opzioni di metadati con abilitato HttpTokensEnforced

In questo esempio, l'account nella Regione ha `HttpTokens = required` e. `HttpTokensEnforced = enabled`

Considera i seguenti tentativi di avvio dell'istanza EC2:

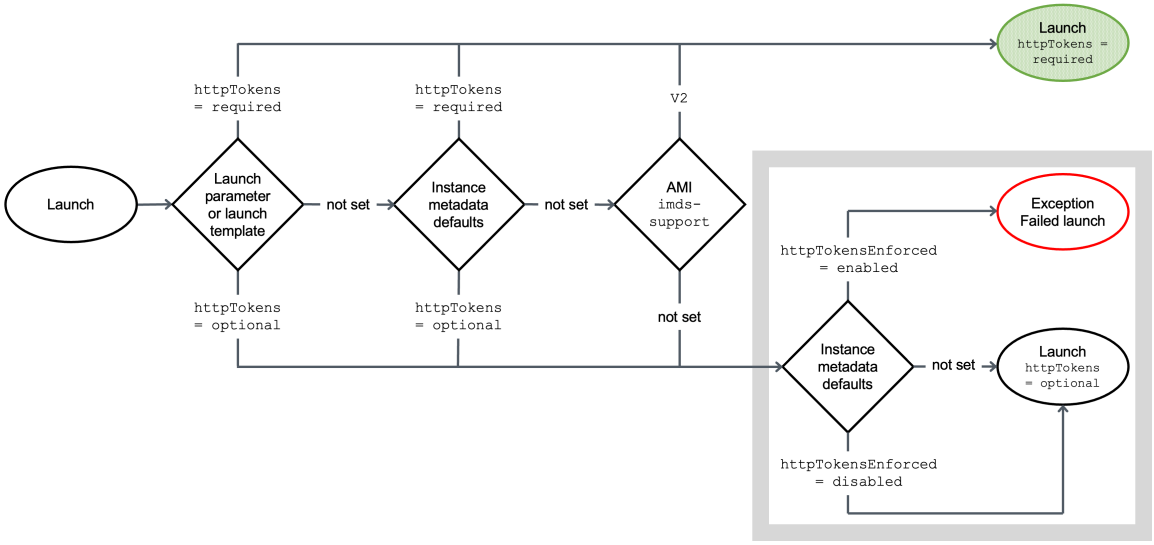
- Tentativo di avvio con `HttpTokens` impostazione su`optional`: l'avvio non riesce perché l'applicazione a livello di account è abilitata (`HttpTokensEnforced = enabled`) e il parametro di avvio ha la precedenza sull'impostazione predefinita dell'account.
- Tentativo di avvio con `HttpTokens` impostazione impostata su`required`: il lancio ha esito positivo perché è conforme all'applicazione a livello di account.
- Tentativo di avvio senza `HttpTokens` valore specificato: l'avvio ha esito positivo perché il valore predefinito è basato sulle impostazioni dell'account. `required`

Configurazione della versione dei metadati di istanza

Quando viene avviata un'istanza, il valore per la versione dei metadati dell'istanza è IMDSv1 o IMDSv2 (token opzionale) () o solo IMDSv2 (token richiesto) (`httpTokens=optional`). **`httpTokens=required`**

All'avvio dell'istanza, è possibile specificare manualmente il valore per la versione dei metadati o utilizzare il valore predefinito. Se specifichi manualmente il valore, esso sostituisce qualsiasi valore predefinito. Se scegli di non specificare manualmente il valore, verrà determinato da una combinazione di impostazioni predefinite.

Il seguente diagramma di flusso mostra come la versione dei metadati per un'istanza all'avvio sia determinata dalle impostazioni ai diversi livelli della configurazione e da dove viene valutata l'applicazione. La tabella che segue fornisce le impostazioni specifiche a ciascun livello.



La tabella mostra come la versione dei metadati per un'istanza all'avvio (indicata dalla Configurazione dell'istanza risultante nella colonna 4) è determinata dalle impostazioni ai diversi livelli di configurazione. L'ordine di precedenza va da sinistra a destra, dove la prima colonna ha la priorità più alta, come segue:

- Colonna 1: parametro di avvio: rappresenta l'impostazione sull'istanza specificata manualmente all'avvio.
- Colonna 2: livello di account predefinito: rappresenta l'impostazione dell'account.
- Colonna 3: AMI predefinita: rappresenta l'impostazione sull'AMI.

Parametro di avvio	Livello di account predefinito	AMI predefinita	Configurazione dell'istanza risultante
Solo V2 (token richiesto)	Nessuna preferenza	Solo V2	Solo V2
Solo V2 (token richiesto)	Solo V2	Solo V2	Solo V2
Solo V2 (token richiesto)	V1 o V2	Solo V2	Solo V2
V1 o V2 (token facoltativo)	Nessuna preferenza	Solo V2	V1 o V2

Parametro di avvio	Livello di account predefinito	AMI predefinita	Configurazione dell'istanza risultante
V1 o V2 (token facoltativo)	Solo V2	Solo V2	V1 o V2
V1 o V2 (token facoltativo)	V1 o V2	Solo V2	V1 o V2
Non impostato	Nessuna preferenza	Solo V2	Solo V2
Non impostato	Solo V2	Solo V2	Solo V2
Non impostato	V1 o V2	Solo V2	V1 o V2
Solo V2 (token richiesto)	Nessuna preferenza	null	Solo V2
Solo V2 (token richiesto)	Solo V2	null	Solo V2
Solo V2 (token richiesto)	V1 o V2	null	Solo V2
V1 o V2 (token facoltativo)	Nessuna preferenza	null	V1 o V2
V1 o V2 (token facoltativo)	Solo V2	null	V1 o V2
V1 o V2 (token facoltativo)	V1 o V2	null	V1 o V2
Non impostato	Nessuna preferenza	null	V1 o V2
Non impostato	Solo V2	null	Solo V2
Non impostato	V1 o V2	null	V1 o V2

Utilizza le chiavi di condizione IAM per limitare le opzioni dei metadati di istanza

È possibile utilizzare le chiavi di condizione IAM in una policy IAM o SCP come riportato di seguito:

- Consentire il lancio di un'istanza solo se è configurata per richiedere l'uso di IMDSv2
- Limitare il numero di hop consentiti
- Disattivazione dell'accesso ai metadati dell'istanza

Processi

- Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze
- Modifica delle opzioni dei metadati dell'istanza per le istanze esistenti

> **Note**
>
> È opportuno procedere con cautela e condurre test accurati prima di apportare qualsiasi modifica. Prendi nota di quanto segue:
>
> - Se imponi l'uso di IMDSv2, applicazioni o agenti che utilizzano IMDSv1 per l'accesso ai metadati dell'istanza verranno interrotti.
> - Se disattivi tutto l'accesso ai metadati dell'istanza, applicazioni o agenti il cui funzionamento si basa sull'accesso ai metadati dell'istanza verranno interrotti.
> - Per IMDSv2, devi utilizzare `/latest/api/token` durante il recupero del token.
> - (Solo Windows) Se la PowerShell versione è precedente alla 4.0, è necessario eseguire l'aggiornamento a Windows Management Framework 4.0 per richiedere l'uso di IMDSv2.

Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze

Puoi configurare le seguenti opzioni dei metadati di istanza per le nuove istanze.

Opzioni

- Richiesta dell'uso di IMDSv2
- Abilitazione degli endpoint IPv4 e IPv6 dell'IMDS
- Disattivazione dell'accesso ai metadati dell'istanza
- Per consentire l'accesso ai tag nei metadati delle istanze

> **Note**
>
> Le impostazioni per queste opzioni sono configurate a livello di account, direttamente nell'account o utilizzando una policy dichiarativa. Devono essere configurate in ogni Regione AWS in cui si desidera configurare le opzioni dei metadati di istanza. L'utilizzo di una policy dichiarativa consente di applicare le impostazioni contemporaneamente su più regioni, nonché su più account. Quando viene utilizzata una policy dichiarativa, non è possibile modificare le impostazioni direttamente all'interno di un account. Questo argomento illustra la modalità di configurazione delle impostazioni direttamente all'interno di un account. Per informazioni sull'utilizzo delle policy dichiarative, consulta Policy dichiarative nella Guida per l'utente di AWS Organizations .

Richiesta dell'uso di IMDSv2

Puoi utilizzare uno dei metodi seguenti per richiedere l'utilizzo di IMDSv2 sulle nuove istanze.

Richiesta di IMDSv2

- Configurazione di IMDSv2 come impostazione predefinita per l'account
- Applica IMDSv2 a livello di account
- Configurazione dell'istanza all'avvio
- Configurazione dell'AMI
- Utilizzo di una policy IAM

Configurazione di IMDSv2 come impostazione predefinita per l'account

È possibile impostare la versione predefinita per l'Instance Metadata Service (IMDS) a livello di account per ciascuna. Regione AWS Ciò significa che quando si avvia una nuova istanza, la versione dei metadati dell'istanza viene impostata automaticamente sul valore predefinito a livello di account. Tuttavia, è possibile sovrascrivere manualmente il valore all'avvio o dopo l'avvio. Per ulteriori informazioni su come le impostazioni a livello di account e le sostituzioni manuali influiscono su un'istanza, consulta Ordine di precedenza per le opzioni dei metadati di istanza.

> **Note**
>
> La configurazione dell'impostazione predefinita a livello di account non ripristina le istanze esistenti. Ad esempio, se configuri l'impostazione predefinita a livello di account su IMDSv2,

ciò non influisce sulle eventuali istanze esistenti impostate su IMDSv1. Se desideri modificare il valore sulle istanze esistenti, devi modificare manualmente il valore sulle istanze stesse.

Puoi impostare l'account predefinito per la versione dei metadati di istanza su IMDSv2 in modo che tutte le nuove istanze nell'account vengano avviate con IMDSv2 obbligatorio e l'IMDSv1 viene disabilitato. Con questa impostazione predefinita dell'account, all'avvio un'istanza, i valori predefiniti dell'istanza sono i seguenti:

- Console: la versione dei metadati è impostata su Solo V2 (è richiesto il token) e il limite di hop di risposta dei metadati è impostato su 2.
- AWS CLI: `HttpTokens` è impostato su `required` e `HttpPutResponseHopLimit` è impostato su 2.

Note

Prima di impostare l'account predefinito su IMDSv2, assicurati che le istanze non dipendano da IMDSv1. Per ulteriori informazioni, consulta Percorso consigliato per richiedere IMDSv2.

Console

Per impostare IMDSv2 come predefinito per l'account per la regione specificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Per modificare il Regione AWS, usa il selettore di regione nell'angolo in alto a destra della pagina.
3. Nel pannello di navigazione seleziona Pannello di controllo.
4. Nella scheda Attributi dell'account, in Impostazioni, scegli Protezione e sicurezza dei dati.
5. Accanto a Impostazioni IMDS predefinite, scegli Gestisci.
6. Nella pagina Gestisci impostazioni IMDS predefinite procedi come segue:
   a. In Servizio di metadati dell'istanza scegli Abilitato.
   b. Per Metadata version (Versione metadati), seleziona V2 only (token required) (Solo V2 [token richiesto]).

c. Per il Limite di hop di risposta ai metadati, specifica 2 se le istanze ospiteranno container. Altrimenti, seleziona Nessuna preferenza. Quando non viene specificata alcuna preferenza, il valore predefinito all'avvio è 2 se l'AMI dispone dell'impostazione `ImdsSupport: v2.0`; in caso contrario, il valore predefinito è 1.

d. Scegliere Aggiorna.

AWS CLI

Per impostare IMDSv2 come predefinito per l'account per la regione specificata

Utilizza il comando modify-instance-metadata-defaults e specifica la regione in cui modificare le impostazioni IMDS a livello di account. Includi `--http-tokens` impostato su `required` e `--http-put-response-hop-limit` impostato su 2 se le istanze ospiteranno container. Altrimenti, specifica `-1` per non indicare alcuna preferenza. Quando `-1` (nessuna preferenza) viene specificato, il valore predefinito all'avvio è 2 se l'AMI dispone dell'impostazione `ImdsSupport: v2.0`; in caso contrario, il valore predefinito è 1.

```
aws ec2 modify-instance-metadata-defaults \
    --region us-east-1 \
    --http-tokens required \
    --http-put-response-hop-limit 2
```

Di seguito è riportato un output di esempio.

```
{
    "Return": true
}
```

Per visualizzare le impostazioni predefinite dell'account per le opzioni dei metadati dell'istanza per la regione specificata

Utilizza il comando get-instance-metadata-defaults e specifica la regione.

```
aws ec2 get-instance-metadata-defaults --region us-east-1
```

Di seguito è riportato un output di esempio.

```
{
```

```
    "AccountLevel": {
        "HttpTokens": "required",
        "HttpPutResponseHopLimit": 2
    },
    "ManagedBy": "account"
}
```

Il campo `ManagedBy` indica l'entità che ha configurato le impostazioni. In questo esempio, `account` indica che le impostazioni sono state configurate direttamente nell'account. Il valore di `declarative-policy` indicherebbe che le impostazioni sono state configurate in base a una policy dichiarativa. Per ulteriori informazioni, consulta Policy dichiarative nella Guida per l'utente di AWS Organizations .

Per impostare IMDSv2 come predefinito per l'account per tutte le regioni

Utilizza il comando modify-instance-metadata-defaults per modificare le impostazioni IMDS a livello di account per tutte le regioni. Includi `--http-tokens` impostato su `required` e `--http-put-response-hop-limit` impostato su 2 se le istanze ospiteranno container. Altrimenti, specifica `-1` per non indicare alcuna preferenza. Quando `-1` (nessuna preferenza) viene specificato, il valore predefinito all'avvio è 2 se l'AMI dispone dell'impostazione `ImdsSupport: v2.0`; in caso contrario, il valore predefinito è 1.

```
echo -e "Region          \t Modified" ; \
echo -e "--------------  \t ---------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 modify-instance-metadata-defaults \
            --region $region \
            --http-tokens required \
            --http-put-response-hop-limit 2 \
            --output text)
        echo -e "$region        \t $output"
    );
done
```

Di seguito è riportato un output di esempio.

```
Region                  Modified
--------------          ---------
ap-south-1              True
eu-north-1              True
eu-west-3               True
...
```

Per visualizzare le impostazioni predefinite dell'account per le opzioni dei metadati dell'istanza per tutte le regioni

Utilizza il comando get-instance-metadata-defaults.

```
echo -e "Region   \t Level          Hops    HttpTokens" ; \
echo -e "-------------- \t ------------   ----    ----------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-instance-metadata-defaults \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Di seguito è riportato un output di esempio.

```
Region           Level          Hops    HttpTokens
--------------   ------------   ----    ----------
ap-south-1       ACCOUNTLEVEL   2       required
eu-north-1       ACCOUNTLEVEL   2       required
eu-west-3        ACCOUNTLEVEL   2       required
...
```

PowerShell

Per impostare IMDSv2 come predefinito per l'account per la regione specificata

Utilizza il Edit-EC2InstanceMetadataDefault cmdlet e specifica la regione in cui modificare le impostazioni a livello di account IMDS. Includi `-HttpToken` impostato su `required` e `-HttpPutResponseHopLimit` impostato su 2 se le istanze ospiteranno container. Altrimenti, specifica `-1` per non indicare alcuna preferenza. Quando `-1` (nessuna preferenza) viene specificato, il valore predefinito all'avvio è 2 se l'AMI dispone dell'impostazione `ImdsSupport: v2.0`; in caso contrario, il valore predefinito è 1.

```
Edit-EC2InstanceMetadataDefault `
    -Region us-east-1 `
    -HttpToken required `
    -HttpPutResponseHopLimit 2
```

Di seguito è riportato un output di esempio.

```
True
```

Per visualizzare le impostazioni predefinite dell'account per le opzioni dei metadati dell'istanza per la regione specificata

Utilizzare il Get-EC2InstanceMetadataDefault cmdlet e specificare la regione.

```
Get-EC2InstanceMetadataDefault -Region us-east-1 | Format-List
```

Di seguito è riportato un output di esempio.

```
HttpEndpoint            :
HttpPutResponseHopLimit : 2
HttpTokens              : required
InstanceMetadataTags    :
```

Per impostare IMDSv2 come predefinito per l'account per tutte le regioni

Utilizzare il Edit-EC2InstanceMetadataDefault cmdlet per modificare le impostazioni a livello di account IMDS per tutte le regioni. Includi `-HttpToken` impostato su `required` e `-HttpPutResponseHopLimit` impostato su 2 se le istanze ospiteranno container. Altrimenti, specifica `-1` per non indicare alcuna preferenza. Quando `-1` (nessuna preferenza) viene specificato, il valore predefinito all'avvio è 2 se l'AMI dispone dell'impostazione `ImdsSupport: v2.0`; in caso contrario, il valore predefinito è 1.

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region   = $_
        Modified = (Edit-EC2InstanceMetadataDefault `
                -Region $_ `
                -HttpToken required `
                -HttpPutResponseHopLimit 2)
    }
} | `
Format-Table Region, Modified -AutoSize
```

Output previsto

```
Region         Modified
------         --------
ap-south-1         True
eu-north-1         True
eu-west-3          True
...
```

Per visualizzare le impostazioni predefinite dell'account per le opzioni dei metadati dell'istanza per tutte le regioni

Utilizza il cmdlet Get-EC2InstanceMetadataDefault.

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region = $_
        HttpPutResponseHopLimit = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpPutResponseHopLimit
        HttpTokens              = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpTokens
    }
} | `
Format-Table -AutoSize
```

Output di esempio

```
Region         HttpPutResponseHopLimit HttpTokens
------         ----------------------- ----------
```

```
ap-south-1                          2 required
eu-north-1                          2 required
eu-west-3                           2 required
...
```

Applica IMDSv2 a livello di account

È possibile imporre l'uso di IMDSv2 a livello di account per ciascuno. Regione AWS Una volta applicate, le istanze possono essere avviate solo se sono configurate per richiedere IMDSv2. Questa applicazione si applica indipendentemente dalla configurazione dell'istanza o dell'AMI.

> **Note**
>
> Prima di abilitare l'applicazione di IMDSv2 a livello di account, assicurati che le tue applicazioni e AMI supportino IMDSv2. Per ulteriori informazioni, consulta Percorso consigliato per richiedere IMDSv2. Se l'imposizione di IMDSv2 è abilitata e non `httpTokens` è impostata nella configurazione dell'istanza all'avvio, `required` nelle impostazioni dell'account o nella configurazione AMI, l'avvio dell'istanza fallirà. Per informazioni sulla risoluzione dei problemi, consulta L'avvio di un' IMDSv1-enabled istanza non riesce.

> **Note**
>
> Questa impostazione non modifica la versione IMDS delle istanze esistenti, ma blocca l'abilitazione di IMDSv1 sulle istanze esistenti che attualmente hanno IMDSv1 disabilitato.

Console

Per applicare IMDSv2 per l'account nella regione specificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Per cambiarlo Regione AWS, usa il selettore di regione nell'angolo in alto a destra della pagina.
3. Nel pannello di navigazione seleziona Pannello di controllo.
4. Nella scheda Attributi dell'account, in Impostazioni, scegli Protezione e sicurezza dei dati.
5. Accanto a Impostazioni IMDS predefinite, scegli Gestisci.

6. Nella pagina Gestisci impostazioni IMDS predefinite procedi come segue:

   a. Per Metadata version (Versione metadati), seleziona V2 only (token required) (Solo V2 [token richiesto]).

   b. Per Enforce IMDSv2, scegli Abilitato.

   c. Scegliere Aggiorna.

AWS CLI

Per applicare IMDSv2 per l'account nella regione specificata

Usa il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-instance-metadata-defaults.html modify-instance-metadata-defaults e specifica la regione in cui applicare IMDSv2.

```
aws ec2 modify-instance-metadata-defaults \
    --region us-east-1 \
    --http-tokens required \
    --http-tokens-enforced enabled
```

Di seguito è riportato un output di esempio.

```
{
"Return": true
}
```

Per visualizzare le impostazioni di imposizione di IMDSv2 per l'account in una regione specifica

Utilizza il comando get-instance-metadata-defaults e specifica la regione.

```
aws ec2 get-instance-metadata-defaults --region us-east-1
```

Di seguito è riportato un output di esempio.

```
{
    "AccountLevel": {
        "HttpTokens": "required",
        "HttpTokensEnforced": "enabled"
    },
    "ManagedBy": "account"
```

```
}
```

Il campo `ManagedBy` indica l'entità che ha configurato le impostazioni. In questo esempio, `account` indica che le impostazioni sono state configurate direttamente nell'account. Il valore di `declarative-policy` indicherebbe che le impostazioni sono state configurate in base a una policy dichiarativa. Per ulteriori informazioni, consulta le politiche dichiarative nella Guida per l'utente delle AWS organizzazioni.

Per applicare IMDSv2 per l'account per tutte le regioni

Usa il comando modify-instance-metadata-defaults per applicare IMDSv2 in tutte le regioni.

```
echo -e "Region          \t Modified" ; \
echo -e "--------------  \t ---------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 modify-instance-metadata-defaults \
            --region $region \
            --http-tokens-enforced enabled \
            --output text)
        echo -e "$region        \t $output"
    );
done
```

Di seguito è riportato un output di esempio.

```
Region                  Modified
--------------          ---------
ap-south-1              True
eu-north-1              True
eu-west-3               True
...
```

Per visualizzare le impostazioni di imposizione di IMDSv2 per l'account in tutte le regioni

Utilizza il comando get-instance-metadata-defaults.

```
echo -e "Region   \t Level           HttpTokensEnforced" ; \
echo -e "-------------- \t ------------   ----------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-instance-metadata-defaults \
            --region $region \
            --query 'AccountLevel.HttpTokensEnforced' \
            --output text)
        echo -e "$region \t ACCOUNTLEVEL $output"
    );
done
```

Di seguito è riportato un output di esempio.

```
Region           Level          HttpTokensEnforced
--------------   ------------   ------------------
ap-south-1       ACCOUNTLEVEL   enabled
eu-north-1       ACCOUNTLEVEL   enabled
eu-west-3        ACCOUNTLEVEL   enabled
...
```

PowerShell

Per applicare IMDSv2 per l'account nella regione specificata

Usa il Edit-EC2InstanceMetadataDefault cmdlet e specifica la regione in cui applicare IMDSv2.

```
Edit-EC2InstanceMetadataDefault `
    -Region us-east-1 `
    -HttpToken required `
    -HttpPutResponseHopLimit 2
```

Di seguito è riportato un output di esempio.

```
@{
    Return = $true
```

```
}
```

Per visualizzare l'impostazione di imposizione di IMDSv2 per l'account in una regione specifica

Usa il Get-EC2InstanceMetadataDefault comando e specifica la regione.

```
Get-EC2InstanceMetadataDefault -Region us-east-1
```

Di seguito è riportato un output di esempio.

```
@{
    AccountLevel = @{
        HttpTokens = "required"
        HttpTokensEnforced = "enabled"
    }
    ManagedBy = "account"
}
```

Il campo `ManagedBy` indica l'entità che ha configurato le impostazioni. In questo esempio, `account` indica che le impostazioni sono state configurate direttamente nell'account. Il valore di `declarative-policy` indicherebbe che le impostazioni sono state configurate in base a una policy dichiarativa. Per ulteriori informazioni, vedere Politiche dichiarative nella Guida per l'utente AWS delle organizzazioni.

Per applicare IMDSv2 per l'account per tutte le regioni

Usa il comando modify-instance-metadata-defaults per applicare IMDSv2 in tutte le regioni.

```
echo -e "Region          \t Modified" ; \
echo -e "--------------  \t ---------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 modify-instance-metadata-defaults \
            --region $region \
            --http-tokens-enforced enabled \
            --output text)
```

```
        echo -e "$region        \t $output"
    );
done
```

Di seguito è riportato un output di esempio.

```
Region                  Modified
--------------          ---------
ap-south-1              True
eu-north-1              True
eu-west-3               True
...
```

Per impostare IMDSv2 come predefinito per l'account per tutte le regioni

Utilizza il Edit-EC2InstanceMetadataDefault cmdlet per modificare le impostazioni a livello di account IMDS per tutte le regioni. Includi `-HttpToken` impostato su `required` e `-HttpPutResponseHopLimit` impostato su 2 se le istanze ospiteranno container. Altrimenti, specifica `-1` per non indicare alcuna preferenza. Quando `-1` (nessuna preferenza) viene specificato, il valore predefinito all'avvio è 2 se l'AMI dispone dell'impostazione `ImdsSupport: v2.0`; in caso contrario, il valore predefinito è 1.

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region   = $_
        Modified = (Edit-EC2InstanceMetadataDefault `
                -Region $_ `
                -HttpToken required `
                -HttpPutResponseHopLimit 2)
    }
} | `
Format-Table Region, Modified -AutoSize
```

Output previsto

```
Region         Modified
------         --------
ap-south-1         True
eu-north-1         True
eu-west-3          True
```

```
...
```

Per visualizzare le impostazioni predefinite dell'account per le opzioni dei metadati dell'istanza per tutte le regioni

Utilizza il cmdlet Get-EC2InstanceMetadataDefault.

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region = $_
        HttpPutResponseHopLimit = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpPutResponseHopLimit
        HttpTokens              = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpTokens
    }
} | `
Format-Table -AutoSize
```

Output di esempio

```
Region         HttpPutResponseHopLimit HttpTokens
------         ----------------------- ----------
ap-south-1                           2 required
eu-north-1                           2 required
eu-west-3                            2 required
...
```

Configurazione dell'istanza all'avvio

Quando avvii un'istanza, puoi configurare l'istanza in modo che richieda l'uso di IMDSv2 configurando i campi seguenti:

- Console di Amazon EC2: imposta Metadata version (Versione metadati) su V2 only (token required) (Solo V2 [token richiesto]).
- AWS CLI: imposta `HttpTokens` su `required`.

Quando specifichi che IMDSv2 è obbligatorio, devi abilitare anche l'endpoint del servizio di metadati dell'istanza (IMDS) impostando Metadati accessibili su Abilitato (console) o `HttpEndpoint` su `enabled` (AWS CLI).

In un ambiente container, quando è obbligatorio IMDSv2, consigliamo di impostare il limite di hop su 2. Per ulteriori informazioni, consulta Considerazioni sull'accesso ai metadati dell'istanza.

Console

Per richiedere l'uso di IMDSv2 su una nuova istanza

- Quando avvii una nuova istanza nella console Amazon EC2, espandi Advanced details (Dettagli avanzati) e procedi come segue:
  - Per Metadata accessible (Metadati accessibili), scegli Enabled (Abilitato).
  - Per Metadata version (Versione metadati), seleziona V2 only (token required) (Solo V2 [token richiesto]).
  - (Ambiente container) Per il Limite di hop di risposta ai metadati, scegliere 2.

  Per ulteriori informazioni, consulta Dettagli avanzati.

AWS CLI

Per richiedere l'uso di IMDSv2 su una nuova istanza

L'esempio run-instances avvia un'istanza `c6i.large` con `--metadata-options` impostato su `HttpTokens=required`. Quando si specifica un valore per `HttpTokens`, è necessario impostare `HttpEndpoint` anche su `enabled`. Poiché l'intestazione del token sicuro è impostata su `required` per le richieste di recupero dei metadati, l'istanza deve utilizzare IMDSv2 quando si richiedono i metadati dell'istanza.

In un ambiente container, quando è obbligatorio IMDSv2, consigliamo di impostare il limite di hop su 2 con `HttpPutResponseHopLimit=2`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
 ...
    --metadata-options
 "HttpEndpoint=enabled,HttpTokens=required,HttpPutResponseHopLimit=2"
```

PowerShell

Per richiedere l'uso di IMDSv2 su una nuova istanza

Il seguente esempio di New-EC2Instance cmdlet avvia un'`c6i.large`istanza con `MetadataOptions_HttpEndpoint` set to e il parametro to. `enabled` `MetadataOptions_HttpTokens` `required` Quando si specifica un valore per `HttpTokens`, è necessario impostare `HttpEndpoint` anche su `enabled`. Poiché l'intestazione del token sicuro è impostata su `required` per le richieste di recupero dei metadati, l'istanza deve utilizzare IMDSv2 quando si richiedono i metadati dell'istanza.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpTokens required
```

CloudFormation

Per specificare le opzioni di metadati per l'utilizzo di un'istanza CloudFormation, consulta la proprietà AWS: :EC2:: nella Guida per l'utente. LaunchTemplate MetadataOptions AWS CloudFormation

Configurazione dell'AMI

Quando registri una nuova AMI o modifichi un'AMI esistente, puoi impostare il parametro `imds-support` su `v2.0`. Per le istanze avviate da questa AMI, Versione metadati sarà impostato su Solo V2 (token obbligatorio) (console) o `HttpTokens` sarà impostato su `required` (AWS CLI). Con queste impostazioni, l'istanza richiede l'uso di IMDSv2 quando vengono chiesti i metadati dell'istanza.

Tieni presente che quando imposti `imds-support` su `v2.0`, anche per le istanze avviate da questa AMI Metadata response hop limit (Limite hop risposta metadati) (console) o `http-put-response-hop-limit` (AWS CLI) sarà impostato su 2.

> **Important**
>
> Non utilizzate questo parametro a meno che il software AMI non supporti IMDSv2. Dopo aver impostato il valore su `v2.0`, non è possibile annullare l'operazione. L'unico modo per "reimpostare" l'AMI consiste nel creare una nuova AMI dallo snapshot sottostante.

Per configurare una nuova AMI per IMDSv2

Utilizza uno dei metodi seguenti per configurare una nuova AMI per IMDSv2.

AWS CLI

L'esempio register-image seguente registra un'AMI utilizzando lo snapshot specificato di un volume root EBS come dispositivo `/dev/xvda`. Specifica `v2.0` per il parametro `imds-support`, in modo che le istanze avviate da tale AMI richiedano l'utilizzo di IMDSv2 quando si richiedono i metadati dell'istanza.

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0123456789example} \
    --architecture x86_64 \
    --imds-support v2.0
```

PowerShell

Il seguente esempio di Register-EC2Image cmdlet registra un'AMI utilizzando l'istantanea specificata di un volume radice EBS come dispositivo. `/dev/xvda` Specifica `v2.0` per il parametro `ImdsSupport`, in modo che le istanze avviate da tale AMI richiedano l'utilizzo di IMDSv2 quando si richiedono i metadati dell'istanza.

```
Register-EC2Image `
    -Name 'my-image' `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping  (
    New-Object `
        -TypeName Amazon.EC2.Model.BlockDeviceMapping `
        -Property @{
        DeviceName = '/dev/xvda';
        EBS        = (New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property
 @{
                SnapshotId = 'snap-0123456789example'
                VolumeType = 'gp3'
                } )
        }  ) `
    -Architecture X86_64 `
    -ImdsSupport v2.0
```

Per configurare un'AMI esistente per IMDSv2

Utilizza uno dei metodi seguenti per configurare una nuova AMI per IMDSv2.

AWS CLI

Il seguente comando modify-image-attribute modifica un'AMI esistente solo per IMDSv2. Specifica `v2.0` per il parametro `imds-support`, in modo che le istanze avviate da tale AMI richiedano l'utilizzo di IMDSv2 quando si richiedono i metadati dell'istanza.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --imds-support v2.0
```

PowerShell

Il seguente esempio di Edit-EC2ImageAttribute cmdlet modifica un'AMI esistente solo per IMDSv2. Specifica `v2.0` per il parametro `imds-support`, in modo che le istanze avviate da tale AMI richiedano l'utilizzo di IMDSv2 quando si richiedono i metadati dell'istanza.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -ImdsSupport 'v2.0'
```

Utilizzo di una policy IAM

È possibile creare una policy IAM che esegua una delle seguenti operazioni:

- Impedisce agli utenti di avviare nuove istanze a meno che non richiedano IMDSv2 sulla nuova istanza.
- Impedisce agli utenti di chiamare l' ModifyInstanceMetadataOptions API per modificare le opzioni di metadati di un'istanza in esecuzione. Limita l'accesso alla proprietà ModifyInstanceMetadataOptions HttpTokens per impedire aggiornamenti involontari delle istanze in esecuzione.
- Impedisci agli utenti di chiamare l' ModifyInstanceMetadataDefaults API per modificare le impostazioni predefinite dell'account sia di HttpTokens che di http. TokensEnforced La limitazione dell'accesso a queste due proprietà garantirà che solo i ruoli autorizzati possano modificare le impostazioni predefinite dell'account.

Uso forzato di IMDSv2 su tutte le nuove istanze tramite una policy IAM

Per garantire che gli utenti possano avviare solo le istanze che richiedono l'uso di IMDSv2 quando richiedono i metadati delle istanze, procedi come segue:

- Limita l'accesso a entrambe le `ModifyInstanceMetadataDefaults` API, `ModifyInstanceMetadataOptions` e più specificamente alle proprietà and. `httpTokens` `httpTokensEnforced`
- Quindi, imposta l'account predefinito su `httpTokens = required` e`httpTokensEnforced = enabled`.

  Per un esempio di policy IAM, consulta Utilizzo dei metadati delle istanze.

Abilitazione degli endpoint IPv4 e IPv6 dell'IMDS

L'IMDS ha due endpoint su un'istanza: IPv4 (`169.254.169.254`) e IPv6 (`[fd00:ec2::254]`). Quando abiliti l'IMDS, l'endpoint IPv4 viene abilitato automaticamente. L'endpoint IPv6 rimane disabilitato anche se si avvia un'istanza in una sottorete. IPv6-only Per abilitare l'endpoint IPv6 è necessario farlo in modo esplicito. Quando abiliti l'endpoint IPv6, l'endpoint IPv4 rimane abilitato.

Puoi abilitare l'endpoint IPv6 all'avvio dell'istanza o dopo.

Requisiti per l'abilitazione dell'endpoint IPv6

- Il tipo di istanza selezionato è un'istanza. Nitro-based
- La sottorete selezionata supporta IPv6, in cui la sottorete è dual-stack o solo IPv6.

Utilizza uno dei seguenti metodi per avviare un'istanza con l'endpoint IPv6 dell'IMDS abilitato.

Console

Per abilitare l'endpoint IPv6 dell'IMDS al lancio dell'istanza

- Avvia l'istanza nella console di Amazon EC2 con le opzioni specificate di seguito in Advanced details (Dettagli avanzati):
  - Per l'endpoint IPv6 dei metadati, scegli Abilitato.

Per ulteriori informazioni, consulta Dettagli avanzati.

AWS CLI

Per abilitare l'endpoint IPv6 dell'IMDS al lancio dell'istanza

L'esempio run-instances seguente avvia un'istanza `c6i.large` con l'endpoint IPv6 abilitato per IMDS. Per abilitare l'endpoint IPv6, per il parametro `--metadata-options` specifica `HttpProtocolIpv6=enabled`. Quando si specifica un valore per `HttpProtocolIpv6`, è necessario impostare `HttpEndpoint` anche su `enabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=enabled,HttpProtocolIpv6=enabled"
```

PowerShell

Per abilitare l'endpoint IPv6 dell'IMDS al lancio dell'istanza

Il seguente esempio di New-EC2Instance cmdlet avvia un'`c6i.large`istanza con l'endpoint IPv6 abilitato per l'IMDS. Per abilitare l'endpoint IPv6, specifica `MetadataOptions_HttpProtocolIpv6` come `enabled`. Quando si specifica un valore per `MetadataOptions_HttpProtocolIpv6`, è necessario impostare `MetadataOptions_HttpEndpoint` anche su `enabled`.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpProtocolIpv6 enabled
```

Disattivazione dell'accesso ai metadati dell'istanza

È possibile disattivare l'accesso ai metadati dell'istanza disabilitando l'IMDS all'avvio di un'istanza. È possibile attivare l'accesso in un secondo momento riabilitando l'IMDS. Per ulteriori informazioni, consulta Attivazione dell'accesso ai metadati dell'istanza.

Important

È possibile scegliere di disabilitare l'IMDS all'avvio o dopo l'avvio. Se disabiliti l'IMDS all'avvio, quanto segue potrebbe non funzionare:

- Potresti non disporre dell'accesso SSH all'istanza. La `public-keys/0/openssh-key`, che è la chiave SSH pubblica dell'istanza, non sarà accessibile perché normalmente la chiave viene fornita dai metadati dell'istanza EC2 e l'accesso avviene tramite gli stessi.
- I dati utente EC2 non saranno disponibili e non verranno eseguiti all'avvio dell'istanza. I dati utente EC2 sono ospitati sull'IMDS. Se disabiliti l'IMDS, disattivi di fatto l'accesso ai dati utente.

Per accedere a questa funzionalità, è possibile riabilitare l'IMDS dopo l'avvio.

Console

Disattivazione dell'accesso ai metadati dell'istanza all'avvio

- Avvia l'istanza nella console di Amazon EC2 con le opzioni specificate di seguito in Advanced details (Dettagli avanzati):
  - Per Metadata accessible (Metadati accessibili), scegli Disabled (Disabilitato).

Per ulteriori informazioni, consulta Dettagli avanzati.

AWS CLI

Disattivazione dell'accesso ai metadati dell'istanza all'avvio

Avvia l'istanza con `--metadata-options` impostato su `HttpEndpoint=disabled`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=disabled"
```

PowerShell

Disattivazione dell'accesso ai metadati dell'istanza all'avvio

Il seguente esempio di New-EC2Instance cmdlet avvia un'istanza con set to. `MetadataOptions_HttpEndpoint` `disabled`

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint disabled
```

CloudFormation

Per specificare le opzioni di metadati per l'utilizzo di un'istanza CloudFormation, consulta la proprietà AWS: :EC2:: nella Guida per l'utente. LaunchTemplate MetadataOptions CloudFormation

Per consentire l'accesso ai tag nei metadati delle istanze

Per impostazione predefinita, non è possibile accedere ai tag dell'istanza nei metadati dell'istanza. Per ogni istanza è necessario consentire l'accesso esplicitamente. Se l'accesso è consentito, le chiavi dei tag dell'istanza devono rispettare specifiche restrizioni relative ai caratteri, altrimenti l'avvio dell'istanza avrà esito negativo. Per ulteriori informazioni, consulta Abilita l'accesso ai tag nei metadati dell'istanza.

Modifica delle opzioni dei metadati dell'istanza per le istanze esistenti

Puoi modificare le opzioni dei metadati dell'istanza per le istanze esistenti.

Puoi inoltre creare una policy IAM che impedisce agli utenti di modificare le opzioni dei metadati dell'istanza in istanze esistenti. Per controllare quali utenti possono modificare le opzioni di metadati dell'istanza, specifica una policy che impedisca a tutti gli utenti diversi dagli utenti con un ruolo specificato di utilizzare l'API. ModifyInstanceMetadataOptions Per un esempio di policy IAM, consulta Utilizzo dei metadati delle istanze.

> **Note**
>
> Se è stata utilizzata una policy dichiarativa per configurare le opzioni dei metadati dell'istanza, non puoi modificarle direttamente all'interno dell'account. Per ulteriori informazioni, consulta Policy dichiarative nella Guida per l'utente di AWS Organizations .

Richiesta dell'uso di IMDSv2

Utilizza uno dei metodi seguenti per modificare le opzioni dei metadati dell'istanza su un'istanza esistente, in modo da utilizzare IMDSv2 quando si richiedono i metadati dell'istanza. Quando è richiesto IMDSv2, non è possibile utilizzare IMDSv1.

> **Note**
>
> Prima di richiedere l'utilizzo di IMDSv2, assicurati che l'istanza non stia effettuando chiamate IMDSv1. La `MetadataNoToken` CloudWatch metrica tiene traccia delle chiamate IMDSv1. Quando `MetadataNoToken` non registra un utilizzo di IMDSv1 per un'istanza, l'istanza è pronta a richiedere IMDSv2.

Console

Per richiedere l'uso di IMDSv2 su un'istanza esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza.
4. Seleziona Operazioni, Impostazioni istanza, Modifica opzioni dei metadati dell'istanza.
5. Nella finestra di dialogo Modifica opzioni dei metadati dell'istanza, esegui una delle operazioni indicate di seguito:
   a. In Servizio di metadati dell'istanza, seleziona Abilita.
   b. Per IMDSv2, scegli Obbligatorio.
   c. Scegli Save (Salva).

AWS CLI

Per richiedere l'uso di IMDSv2 su un'istanza esistente

Utilizza il comando CLI modify-instance-metadata-options e imposta il parametro `http-tokens` su `required`. Quando si specifica un valore per `http-tokens`, è necessario impostare `http-endpoint` anche su `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-tokens required \
    --http-endpoint enabled
```

PowerShell

Per richiedere l'uso di IMDSv2 su un'istanza esistente

Usa il Edit-EC2InstanceMetadataOption cmdlet e imposta il parametro su. `HttpTokens` `required` Quando si specifica un valore per `HttpTokens`, è necessario impostare `HttpEndpoint` anche su `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpTokens required `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Ripristino dell'uso di IMDSv1

Quando IMDSv2 è richiesto su un'istanza, l'utilizzo di una richiesta IMDSv1 avrà esito negativo. Al contrario, quando IMDSv2 è facoltativo, funzioneranno sia IMDSv2 che IMDSv1. Pertanto, per ripristinare IMDSv1, imposta IMDSv2 su optional () utilizzando uno dei seguenti metodi. `httpTokens = optional`

La proprietà `httpTokensEnforced` IMDS impedisce inoltre i tentativi di abilitare IMDSv1 su un'istanza esistente. Se abilitato per un account in una regione, un tentativo di impostazione su `httpTokens optional` genererà un'eccezione. `UnsupportedOperation` Per ulteriori informazioni, consultaRisoluzione dei problemi.

Important

Se l'avvio dell'istanza non riesce a causa dell'applicazione di IMDSv2, sono disponibili due opzioni per consentire il corretto avvio:

- Avvia le istanze come IMDSv2-only: se il software in esecuzione sulle istanze utilizza solo IMDSv2 (nessuna dipendenza da IMDSv1), puoi avviare le istanze solo come IMDSv2. Per fare ciò, configura IMDSv2 solo impostando i parametri di avvio `httpTokens = required` o i valori predefiniti dei metadati per l'account nella Regione.
- Disabilita l'applicazione: se il tuo software dipende ancora da IMDSv1, imposta questa opzione per l'account nella regione. `httpTokensEnforced disabled` Per ulteriori informazioni, consulta Applica IMDSv2 a livello di account.

Console

Per ripristinare l'uso di IMDSv1 su un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza.
4. Seleziona Operazioni, Impostazioni istanza, Modifica opzioni dei metadati dell'istanza.
5. Nella finestra di dialogo Modifica opzioni dei metadati dell'istanza, esegui una delle operazioni indicate di seguito:
   a. In Servizio di metadati dell'istanza, assicurati che l'opzione Abilita sia selezionata.
   b. Per IMDSv2, scegli Facoltativo.
   c. Scegli Save (Salva).

AWS CLI

Per ripristinare l'uso di IMDSv1 su un'istanza

È possibile utilizzare il comando CLI modify-instance-metadata-options con `http-tokens` impostato su `optional` per ripristinare l'utilizzo di IMDSv1 quando si richiedono metadati di istanza.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-tokens optional \
    --http-endpoint enabled
```

PowerShell

Per ripristinare l'uso di IMDSv1 su un'istanza

È possibile utilizzare il Edit-EC2InstanceMetadataOption cmdlet con `HttpTokens` set to per ripristinare l'uso di IMDSv1 quando `optional` si richiedono i metadati dell'istanza.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpTokens optional `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Modifica del limite di hop di risposta PUT

Per istanze esistenti, puoi modificare le impostazioni del limite di hop della risposta PUT.

Attualmente solo gli AWS SDK AWS CLI e supportano la modifica del limite di hop di risposta PUT.

AWS CLI

Per modificare il limite di hop di risposta PUT

Utilizza il comando CLI modify-instance-metadata-options e imposta il parametro `http-put-response-hop-limit` sul numero di hop richiesti. Nell'esempio seguente, il limite di hop è impostato su `3`. Tieni presente che quando si specifica un valore per `http-put-response-hop-limit`, è necessario anche impostare `http-endpoint` su `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-put-response-hop-limit 3 \
    --http-endpoint enabled
```

PowerShell

Per modificare il limite di hop di risposta PUT

Utilizza il Edit-EC2InstanceMetadataOption cmdlet e imposta il `HttpPutResponseHopLimit` parametro sul numero richiesto di hop. Nell'esempio seguente, il limite di hop è impostato su `3`. Tieni presente che quando si specifica un valore per `HttpPutResponseHopLimit`, è necessario anche impostare `HttpEndpoint` su `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpPutResponseHopLimit 3 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Abilitazione degli endpoint IPv4 e IPv6 dell'IMDS

L'IMDS ha due endpoint su un'istanza: IPv4 (`169.254.169.254`) e IPv6 (`[fd00:ec2::254]`). Quando abiliti l'IMDS, l'endpoint IPv4 viene abilitato automaticamente. L'endpoint IPv6 rimane disabilitato anche se si avvia un'istanza in una sottorete. IPv6-only Per abilitare l'endpoint IPv6 è necessario farlo in modo esplicito. Quando abiliti l'endpoint IPv6, l'endpoint IPv4 rimane abilitato.

Puoi abilitare l'endpoint IPv6 all'avvio dell'istanza o dopo.

Requisiti per l'abilitazione dell'endpoint IPv6

- Il tipo di istanza selezionato è un'istanza. Nitro-based
- La sottorete selezionata supporta IPv6, in cui la sottorete è dual-stack o solo IPv6.

Attualmente solo gli AWS SDK AWS CLI e supportano l'abilitazione dell'endpoint IMDS IPv6 dopo l'avvio dell'istanza.

AWS CLI

Per abilitare l'endpoint IPv6 dell'IMDS per l'istanza

Utilizza il comando CLI modify-instance-metadata-options e imposta il parametro `http-protocol-ipv6` su `enabled`. Tieni presente che quando si specifica un valore per `http-protocol-ipv6`, è necessario anche impostare `http-endpoint` su `enabled`.

```
aws ec2 modify-instance-metadata-options \
 --instance-id i-1234567890abcdef0 \
 --http-protocol-ipv6 enabled \
 --http-endpoint enabled
```

PowerShell

Per abilitare l'endpoint IPv6 dell'IMDS per l'istanza

Utilizza il Edit-EC2InstanceMetadataOption cmdlet e imposta il parametro su. `HttpProtocolIpv6` `enabled` Tieni presente che quando si specifica un valore per `HttpProtocolIpv6`, è necessario anche impostare `HttpEndpoint` su `enabled`.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpProtocolIpv6 enabled `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Attivazione dell'accesso ai metadati dell'istanza

Puoi attivare l'accesso ai metadati dell'istanza abilitando l'endpoint HTTP del servizio di metadati dell'istanza (IMDS), indipendentemente dalla versione in uso. Puoi invertire questa modifica in qualsiasi momento disabilitando l'endpoint HTTP.

Per attivare l'accesso ai metadati dell'istanza, utilizza uno dei metodi seguenti.

Console

Per attivare l'accesso ai metadati dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza.
4. Seleziona Operazioni, Impostazioni istanza, Modifica opzioni dei metadati dell'istanza.
5. Nella finestra di dialogo Modifica opzioni dei metadati dell'istanza, esegui una delle operazioni indicate di seguito:

    a. In Servizio di metadati dell'istanza, seleziona Abilita.

    b. Scegli Save (Salva).

AWS CLI

Per attivare l'accesso ai metadati dell'istanza

Utilizza il comando CLI modify-instance-metadata-options e imposta il parametro `http-endpoint` su `enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-endpoint enabled
```

PowerShell

Per attivare l'accesso ai metadati dell'istanza

Utilizzare il Edit-EC2InstanceMetadataOption cmdlet e impostare il parametro su. `HttpEndpoint` `enabled`

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Disattivazione dell'accesso ai metadati dell'istanza

Puoi disattivare l'accesso ai metadati dell'istanza disabilitando l'endpoint HTTP del servizio di metadati dell'istanza (IMDS), indipendentemente dalla versione in uso. Puoi invertire questa modifica in qualsiasi momento abilitando l'endpoint HTTP.

Per disattivare l'accesso ai metadati dell'istanza, utilizza uno dei metodi seguenti.

Console

Come disattivare l'accesso ai metadati dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza.
4. Seleziona Operazioni, Impostazioni istanza, Modifica opzioni dei metadati dell'istanza.
5. Nella finestra di dialogo Modifica opzioni dei metadati dell'istanza, esegui una delle operazioni indicate di seguito:
    a. In Servizio di metadati dell'istanza, deseleziona Abilita.
    b. Scegli Save (Salva).

AWS CLI

Come disattivare l'accesso ai metadati dell'istanza

Utilizza il comando CLI modify-instance-metadata-options e imposta il parametro `http-endpoint` su `disabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-endpoint disabled
```

PowerShell

Come disattivare l'accesso ai metadati dell'istanza

Utilizzare il Edit-EC2InstanceMetadataOption cmdlet e impostare il parametro su. `HttpEndpoint` `disabled`

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpEndpoint disabled).InstanceMetadataOptions
```

Per consentire l'accesso ai tag nei metadati delle istanze

Puoi consentire l'accesso ai tag nei metadati dell'istanza su un'istanza in esecuzione o interrotta. Per ogni istanza è necessario consentire l'accesso esplicitamente. Se l'accesso è consentito, le chiavi dei tag dell'istanza devono rispettare specifiche restrizioni relative ai caratteri, altrimenti si verifica un errore. Per ulteriori informazioni, consulta Abilita l'accesso ai tag nei metadati dell'istanza.

Risoluzione dei problemi

La modifica di un'istanza non riesce IMDSv1-enabled

Description

Viene visualizzato il seguente messaggio di errore:

```
You can't launch instances with IMDSv1 because httpTokensEnforced
is enabled for this account. Either launch the instance with
httpTokens=required or contact your account owner to disable
```

`httpTokensEnforced using the ModifyInstanceMetadataDefaults API or the account settings in the EC2 console.`

Causa

Questo errore viene generato quando si tenta di modificare un'istanza esistente in modo che sia abilitata per IMDSv1 (`httpTokens = optional`) in un account in cui le impostazioni dell'account EC2 o una politica dichiarativa AWS dell'Organizzazione impongono l'uso di IMDSv2 (). `httpTokensEnforced = enabled`

Soluzione

Se hai bisogno del supporto di IMDSv1 su istanze esistenti, dovrai disabilitare l'applicazione di IMDSv2 per l'account nella regione. Per disabilitare l'imposizione di IMDSv2, imposta su. `HttpTokensEnforced disabled` Per ulteriori informazioni, consulta Amazon ModifyInstanceMetadataDefaults EC2 API Reference. Se preferisci configurare questa impostazione utilizzando la console, consultaApplica IMDSv2 a livello di account.

Ti consigliamo di usare solo IMDSv2 (). `httpTokens=required` Per ulteriori informazioni, consulta Passaggio all'utilizzo di Servizio di metadati dell'istanza Versione 2.

Esegui i comandi quando avvii un'istanza EC2 con l'input dei dati utente

Quando avvii un'istanza Amazon EC2, puoi trasferire all'istanza i dati utente utilizzati per eseguire attività di configurazione automatizzate di routine o per l'esecuzione di script all'avvio dell'istanza.

Se sei interessato a scenari di automazione più complessi, potresti prendere in considerazione CloudFormation. Per ulteriori informazioni, consulta Implementazione di applicazioni su Amazon EC2 con CloudFormation nella Guida per l'utente AWS CloudFormation .

Su istanze Linux, puoi trasferire due tipi di dati utente a Amazon EC2, ovvero script della shell e direttive cloud-init. Puoi anche trasferire questi dati alla procedura guidata di avvio dell'istanza come testo normale, come un file (utile per avviare le istanze con gli strumenti a riga di comando) oppure come testo con codifica base64 (per le chiamate API).

Su istanze Windows, gli agenti di avvio gestiscono gli script dei dati utente.

Considerazioni

- I dati utente vengono considerati dati opachi, ovvero i dati forniti saranno i dati visualizzati e disponibili. Il modo in cui viene interpretato dipende dall'istanza.

- I dati utente devono essere codificati con base64. La console Amazon EC2 può eseguire automaticamente la codifica con base64 oppure accettare input codificati con base64. Se recuperi i dati utente usando i metadati dell'istanza o la console, vengono decodificati automaticamente con base64.
- I dati dell'utente sono limitati a 16 KB, in formato raw, prima della codifica base 64. La dimensione di una stringa di lunghezza n dopo la codifica base64 è ceil(n/3)*4.
- I dati utente sono un attributo dell'istanza. Se si crea un'AMI da un'istanza, i dati utente dell'istanza non vengono inclusi nell'AMI.

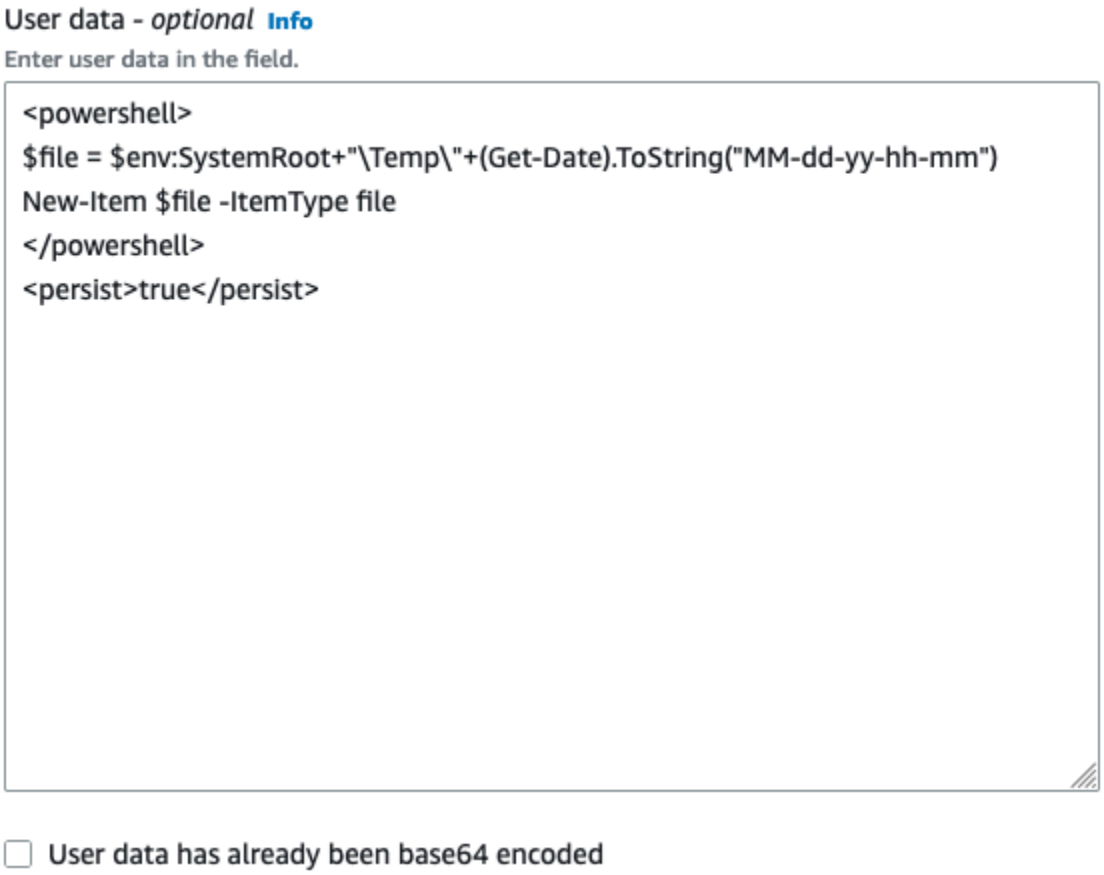
Dati utente in Console di gestione AWS

Puoi specificare i dati utente dell'istanza al momento dell'avvio dell'istanza. Se il volume root dell'istanza è un volume EBS, puoi anche arrestare l'istanza e aggiornare i relativi dati utente.

Specifica i dati utente dell'istanza all'avvio con Launch Wizard

Puoi specificare i dati utente quando si avvia un'istanza con Launch Wizard nella console EC2. Per specificare i dati utente all'avvio, segui la procedura di avvio di un'istanza. Il campo User data (Dati utente) campo si trova nella sezione Dettagli avanzati della procedura guidata di avvio dell'istanza. Inserisci il tuo PowerShell script nel campo Dati utente, quindi completa la procedura di avvio dell'istanza.

Nel seguente screenshot del campo Dati utente, lo script di esempio crea un file nella cartella temporanea di Windows, utilizzando la data e l'orario correnti nel nome del file. Quando includi `<persist>true</persist>`, lo script viene eseguito ogni volta che riavvii o avvii l'istanza. Se lasci vuota la casella di spunta I dati utente sono già stati codificati in base64, la console Amazon EC2 esegue la codifica in base64 per te.



Per ulteriori informazioni, consulta Specifica i dati utente dell'istanza all'avvio con Launch Wizard. Per un esempio di Linux che utilizza il AWS CLI, vedithe section called "I dati dell'utente e AWS CLI". Per un esempio di Windows che utilizza gli Strumenti per Windows PowerShell, vederethe section called "Dati utente e strumenti per Windows PowerShell".

Visualizzazione e aggiornamento dei dati utente dell'istanza

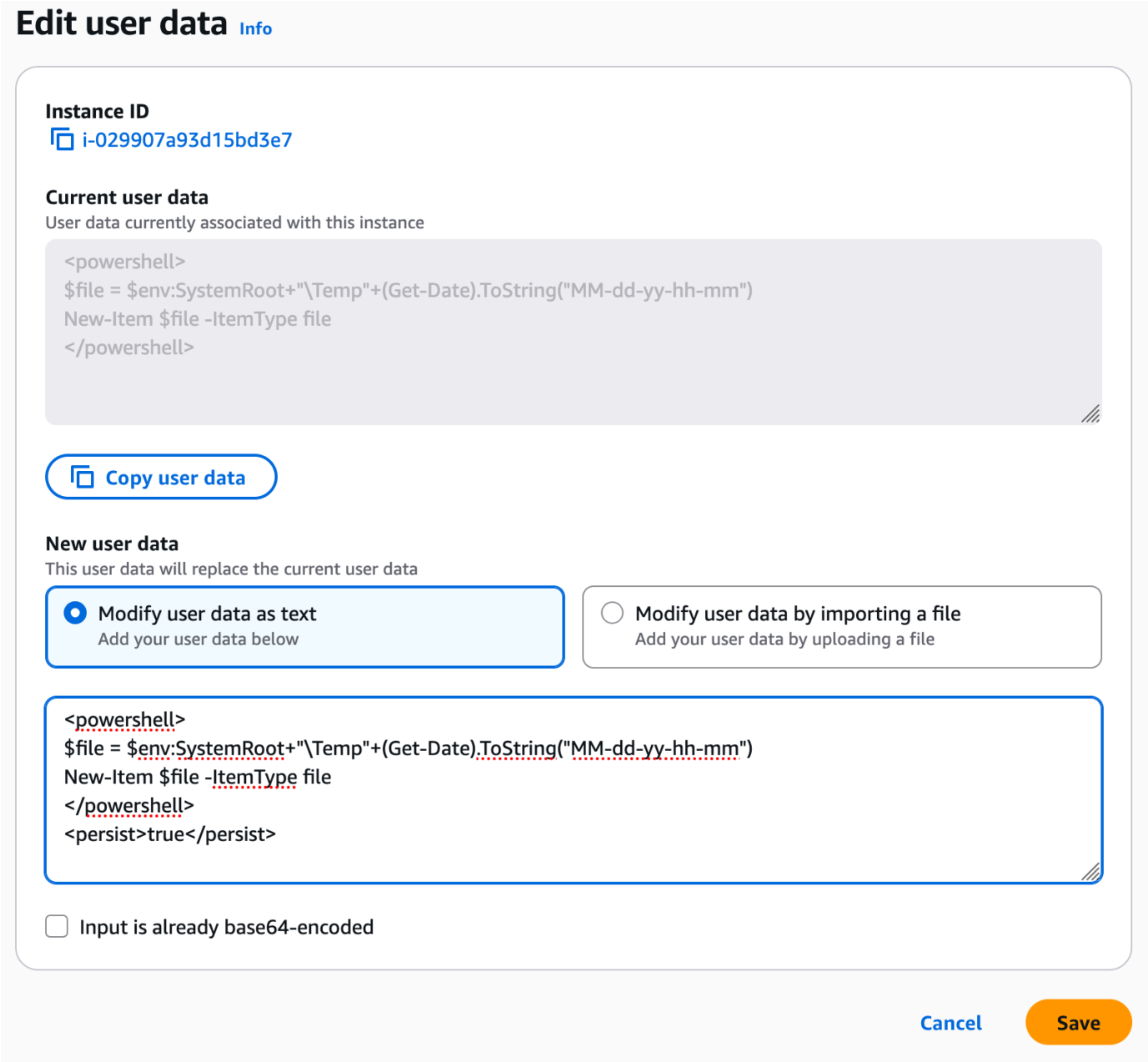
Puoi visualizzare i dati utente dell'istanza per qualsiasi istanza, oltre a poter aggiornare i dati utente dell'istanza per un'istanza arrestata.

Aggiornamento dei dati utente di un'istanza tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza e scegliere Actions (Operazioni), Instance state (Stato istanza), Stop (Arresta).

> **Warning**
>
> Quando si arresta un'istanza, i dati sui volumi dell'archivio di istanze vengono persi. Per preservare questi dati, esegui il backup su uno storage persistente.

4. Quando viene richiesta la conferma, selezionare Stop (Arresta). Possono essere necessari alcuni minuti per arrestare l'istanza.
5. Con l'istanza ancora selezionata, selezionare Actions (Operazioni), Instance Settings (Impostazioni istanza), Edit user data (Modifica i dati utente). Non puoi modificare i dati utente se l'istanza è in esecuzione, ma puoi visualizzarli.
6. Nella finestra di dialogo Edit user data (Modifica i dati utente), aggiorna i dati utente, quindi scegli Save (Salva). Per eseguire gli script dei dati utente ogni volta che riavvii o avvii l'istanza, aggiungi `<persist>true</persist>`, come illustrato nell'esempio seguente:



7. Avviare l'istanza. Se hai abilitato l'esecuzione dei dati utente per i riavvii o gli avvii successivi, gli script dei dati utente aggiornati vengono eseguiti come parte del processo di avvio dell'istanza.

In che modo Amazon EC2 gestisce i dati utente per le istanze Linux

Gli esempi seguenti usano i dati utente per eseguire comandi che configurano un server LAMP all'avvio dell'istanza. In ogni esempio, vengono eseguite le seguenti attività:

- I pacchetti del software di distribuzione vengono aggiornati.

- Il server Web, php, e i pacchetti `mariadb` vengono installati.
- Il servizio `httpd` viene avviato e abilitato.
- L'utente `ec2-user` viene aggiunto al gruppo apache.
- Vengono configurati la proprietà e le autorizzazioni di file appropriati per la directory Web e i file in essa contenuti.
- Viene creata una semplice pagina Web per testare il server Web e il motore PHP.

Indice

- Prerequisiti
- Dati utente e script della shell
- Aggiornamento dei dati utente dell'istanza
- Dati utente e direttive cloud-init
- I dati dell'utente e AWS CLI
- Combinazione di script di shell e direttive cloud-init

Prerequisiti

Per gli esempi in questo argomento si presuppone quanto riportato di seguito:

- L'istanza dispone di un nome DNS pubblico raggiungibile da Internet.
- Il gruppo di sicurezza associato all'istanza è configurato per consentire il traffico SSH (porta 22) in modo da potersi connettere all'istanza per visualizzare i file di log di output.
- L'istanza viene avviata tramite un'AMI Amazon Linux. Per altre distribuzioni Linux, i comandi e le direttive potrebbero non funzionare. Per ulteriori informazioni su altre distribuzioni, ad esempio sul relativo supporto delle direttive cloud-init, consulta la documentazione relativa alla distribuzione specifica.

Dati utente e script della shell

Se hai familiarità con lo scripting della shell, questo è il modo più semplice e completo per inviare le istruzioni a un'istanza all'avvio. L'aggiunta di queste attività in fase di avvio aumenta il tempo necessario per l'avvio dell'istanza. Ti consigliamo di prevedere alcuni minuti aggiuntivi per il completamento delle attività prima di procedere alla verifica del corretto completamento dello script utente.

> **Important**
>
> Per impostazione predefinita, gli script di dati utente e le direttive cloud-init vengono eseguiti solo durante il ciclo di avvio quando si avvia un'istanza per la prima volta. È possibile aggiornare la configurazione per garantire che gli script dei dati utente e le direttive cloud-init vengano eseguiti ogni volta che si riavvia l'istanza. Per ulteriori informazioni, consulta Come posso utilizzare i dati degli utenti per eseguire automaticamente uno script a ogni riavvio della mia istanza Amazon EC2 Linux? nel AWS Knowledge Center.

Gli script della shell relativi ai dati utente devono iniziare con i caratteri `#!` e con il percorso dell'interprete che deve leggere lo script, in genere /bin/bash). Per un'introduzione allo scripting della shell, consulta il Manuale di riferimento di Bash sul sito Web del sistema operativo GNU.

Gli script immessi come dati utente vengono eseguiti come utente root. Non utilizzare pertanto il comando sudo nello script. Ricorda che tutti i file creati saranno di proprietà dell'utente root. Se devi concedere l'accesso ai file a utenti non root, devi modificare di conseguenza le autorizzazioni nello script. Inoltre, dal momento che lo script non viene eseguito in modo interattivo, non puoi includere comandi che richiedono il feedback degli utenti, ad esempio il comando yum update senza il contrassegno `-y`.

Se si utilizza un' AWS API, inclusa la AWS CLI, in uno script di dati utente, è necessario utilizzare un profilo di istanza all'avvio dell'istanza. Un profilo di istanza fornisce le AWS credenziali appropriate richieste dallo script di dati utente per emettere la chiamata API. Per ulteriori informazioni, consulta Use instance profiles nella Guida per l'utente IAM. Le autorizzazioni assegnate al ruolo IAM dipendono dai servizi chiamati con l'API. Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.

Il file di log dell'output della direttiva cloud-init acquisisce l'output della console in modo da semplificare il debug degli script dopo l'avvio se l'istanza ha un comportamento imprevisto. Per visualizzare il file di log, connettiti all'istanza e apri `/var/log/cloud-init-output.log`.

Quando uno script di dati utente viene elaborato, viene copiato ed eseguito da `/var/lib/cloud/instances/`*`instance-id`*`/`. Lo script non viene eliminato dopo l'esecuzione. Assicurati di eliminare gli script di dati utente da `/var/lib/cloud/instances/`*`instance-id`*`/` prima di creare un'AMI dall'istanza. In caso contrario, lo script esisterà in questa directory su qualsiasi istanza avviata dall'AMI.

Aggiornamento dei dati utente dell'istanza

Per aggiornare i dati utente dell'istanza, è necessario prima arrestare l'istanza. Se l'istanza è in esecuzione, è possibile visualizzare i dati utente ma non modificarli.

> **Warning**
>
> Quando si arresta un'istanza, i dati sui volumi dell'archivio delle istanze vengono persi. Per preservare questi dati, esegui il backup su uno storage persistente.

Per modificare i dati utente dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e scegli Instance state (Stato istanza), Stop instance (Arresta istanza). Se questa opzione è disabilitata, l'istanza è già arrestata oppure il suo volume root è un volume di archivio dell'istanza.
4. Quando viene richiesta la conferma, selezionare Stop (Arresta). Possono essere necessari alcuni minuti per arrestare l'istanza.
5. Con l'istanza ancora selezionata, selezionare Actions (Operazioni), Instance Settings (Impostazioni istanza), Edit user data (Modifica i dati utente).
6. Modificare i dati utente in base alle esigenze, quindi scegliere Save (Salva).
7. Avviare l'istanza. I nuovi dati utente sono visibili nell'istanza dopo averla avviata. Tuttavia, gli script dei dati utente non vengono eseguiti.

Dati utente e direttive cloud-init

Il pacchetto cloud-init configura aspetti specifici di una nuova istanza di Amazon Linux quando viene avviata. In particolare, configura il file `.ssh/authorized_keys` per ec2-user in modo da consentirti di eseguire il login utilizzando la tua chiave privata. Per ulteriori informazioni sulle attività di configurazione eseguite dal pacchetto cloud-init per le istanze Linux di Amazon, consulta la seguente documentazione.

- Amazon Linux 2023 – Customized cloud-init
- Amazon Linux 2 – Using cloud-init on Amazon Linux 2

Le direttive utente cloud-init possono essere trasferite a un'istanza all'avvio con le stesse modalità di trasferimento di uno script, anche se la sintassi è diversa. Per ulteriori informazioni su cloud-init, consulta. https://cloudinit.readthedocs.org/en/latest/index.html

> **Important**
>
> Per impostazione predefinita, gli script di dati utente e le direttive cloud-init vengono eseguiti solo durante il ciclo di avvio quando si avvia un'istanza per la prima volta. È possibile aggiornare la configurazione per garantire che gli script dei dati utente e le direttive cloud-init vengano eseguiti ogni volta che si riavvia l'istanza. Per ulteriori informazioni, consulta Come posso utilizzare i dati degli utenti per eseguire automaticamente uno script a ogni riavvio della mia istanza Amazon EC2 Linux? nel AWS Knowledge Center.

L'aggiunta di queste attività in fase di avvio aumenta il tempo necessario per l'avvio di un'istanza. Ti consigliamo di prevedere alcuni minuti aggiuntivi per il completamento delle attività prima di procedere alla verifica del corretto completamento delle direttive relative ai dati utente.

Per trasmettere le direttive cloud-init a un'istanza Amazon Linux

1. Segui la procedura per l'avvio di un'istanza. Il campo User data (Dati utente) campo si trova nella sezione Dettagli avanzati della procedura guidata di avvio dell'istanza. Inserisci il testo della direttiva cloud-init nel campo User data (Dati utente), quindi completa la procedura di avvio dell'istanza.

   Negli esempi riportati di seguito, le direttive creano e configurano un server Web su Amazon Linux. La `#cloud-config` riga in alto è necessaria per identificare i comandi come direttive cloud-init.

   AL2023

   ```
   #cloud-config
   package_update: true
   package_upgrade: all

   packages:
   - httpd
   - mariadb105-server
   - php8.1
   - php8.1-mysqlnd
   ```

```
runcmd:
- systemctl start httpd
- systemctl enable httpd
- [ sh, -c, "usermod -a -G apache ec2-user" ]
- [ sh, -c, "chown -R ec2-user:apache /var/www" ]
- chmod 2775 /var/www
- [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
- [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
- [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
```

AL2

```
#cloud-config
package_update: true
package_upgrade: all

packages:
- httpd
- mariadb-server

runcmd:
- [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
- systemctl start httpd
- systemctl enable httpd
- [ sh, -c, "usermod -a -G apache ec2-user" ]
- [ sh, -c, "chown -R ec2-user:apache /var/www" ]
- chmod 2775 /var/www
- [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
- [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
- [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
```

2. Prevedi tempo aggiuntivo per l'avvio dell'istanza e l'esecuzione delle direttive nei dati utente e quindi verifica se le direttive hanno completato le attività come previsto.

   Nel nostro esempio, in un browser Web, inserisci l'URL del file di test PHP creato dalle direttive. Questo URL è l'indirizzo DNS pubblico dell'istanza, seguito da una barra e dal nome di file.

   ```
   http://my.public.dns.amazonaws.com/phpinfo.php
   ```

   Viene visualizzata la pagina delle informazioni PHP. Se non sei in grado di vedere questa pagina, controlla che il gruppo di sicurezza che stai utilizzando contenga una regola che

consenta il traffico HTTP (porta 80). Per ulteriori informazioni, consulta Configurazione delle regole per i gruppi di sicurezza.

3. (Facoltativo) Se le direttive non hanno completato le attività previste oppure se desideri verificare che siano state completate senza errori, connettiti all'istanza, esamina il file di log dell'output (`/var/log/cloud-init-output.log`) e cerca eventuali messaggi di errore nell'output. Per ulteriori informazioni sul debug, è possibile aggiungere la seguente riga alle direttive:

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

Questa direttiva invia l'output del comando runcmd a `/var/log/cloud-init-output.log`.

I dati dell'utente e AWS CLI

Puoi utilizzare il AWS CLI per specificare, modificare e visualizzare i dati utente per la tua istanza. Per informazioni sulla visualizzazione dei dati utente dall'istanza tramite metadati dell'istanza, consulta Accesso ai metadati dell'istanza per un'istanza EC2.

In Windows, è possibile utilizzare il AWS Tools for Windows PowerShell invece di AWS CLI. Per ulteriori informazioni, consulta Dati utente e strumenti per Windows PowerShell.

Esempio: specifica dei dati utente all'avvio

Per specificare i dati utente all'avvio di un'istanza, utilizza il comando run-instances con il parametro `--user-data`. Conrun-instances, AWS CLI esegue la codifica base64 dei dati utente per te.

L'esempio seguente illustra come specificare uno script come stringa nella riga di comando:

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data echo user data
```

L'esempio seguente illustra come specificare uno script utilizzando un file di testo. Assicurati di utilizzare il prefisso `file://` per specificare il file.

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
```

```
    --user-data file://my_script.txt
```

Di seguito è riportato un esempio di file di testo con uno script della shell.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Esempio: modifica dei dati utente di un'istanza arrestata

Puoi modificare i dati utente di un'istanza arrestata tramite il comando modify-instance-attribute. Conmodify-instance-attribute, AWS CLI non esegue la codifica base64 dei dati utente per te.

- Su un computer Linux utilizzare il comando con codifica Base64 per codificare i dati utente.

  ```
  base64 my_script.txt >my_script_base64.txt
  ```

- Su un computer Windows, utilizza il comando certutil per codificare i dati utente. Prima di poter utilizzare questo file con AWS CLI, è necessario rimuovere la prima riga (BEGIN CERTIFICATE) e l'ultima (END CERTIFICATE).

  ```
  certutil -encode my_script.txt my_script_base64.txt
  notepad my_script_base64.txt
  ```

Utilizza i parametri `--attribute` e `--value` per utilizzare il file di testo codificato per specificare i dati utente. Assicurati di utilizzare il prefisso `file://` per specificare il file.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --value file://my_script_base64.txt
```

Esempio: cancellazione dei dati utente di un'istanza arrestata

Per eliminare i dati utente esistenti, utilizzare il comando modify-instance-attribute come segue:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --user-data Value=
```

Esempio: visualizzazione dei dati utente

Per recuperare i dati utente di un'istanza, utilizza il comando describe-instance-attribute. Condescribe-instance-attribute, AWS CLI non esegue la decodifica in base 64 dei dati utente al posto tuo.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData
```

L'esempio seguente è l'output contenente i dati utente con codifica base64.

```
{
    "UserData": {
        "Value":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQpzZXJ2aWNlIGh0dHBkIHN0YXJ0CmNoa2NvbmZpZyBodHRwZCBvbg=="
    },
    "InstanceId": "i-1234567890abcdef0"
}
```

- Su un computer Linux, utilizza l'opzione `--query` per recuperare i dati utente codificati e il comando con codifica Base64 per decodificarli.

  ```
  aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
   userData --output text --query "UserData.Value" | base64 --decode
  ```

- Su un computer Windows, utilizza l'opzione `--query` per recuperare i dati utente codificati e il comando certutil per decodificarli. Si noti che l'output codificato viene memorizzato in un file, mentre l'output decodificato viene memorizzato in un file diverso.

  ```
  aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
   userData --output text --query "UserData.Value" >my_output.txt
  certutil -decode my_output.txt my_output_decoded.txt
  type my_output_decoded.txt
  ```

Di seguito è riportato un output di esempio.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Combinazione di script di shell e direttive cloud-init

Per impostazione predefinita, nei dati utente puoi includere solo un tipo di contenuto alla volta. Tuttavia, puoi utilizzare tipi di contenuto `text/cloud-config` e `text/x-shellscript` in un file multipart MIME per includere nei dati utente sia uno script di shell che direttive cloud-init.

Di seguito è illustrato il formato multipart MIME.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
cloud-init directives

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
shell script commands
--//--
```

Ad esempio, i seguenti dati utente includono direttive cloud-init e uno script di shell bash. Le direttive cloud-init creano un file (`/test-cloudinit/cloud-init.txt`) e scrivono `Created by cloud-init` in tale file. Lo script della shell bash crea un file (`/test-userscript/userscript.txt`) e scrive `Created by bash shell script` in quel file.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
```

```
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
runcmd:
- [ mkdir, /test-cloudinit ]
write_files:
- path: /test-cloudinit/cloud-init.txt
content: Created by cloud-init

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
mkdir test-userscript
touch /test-userscript/userscript.txt
echo "Created by bash shell script" >> /test-userscript/userscript.txt
--//--
```

In che modo Amazon EC2 gestisce i dati utente per le istanze Windows

Su istanze Windows, l'agente di avvio svolge le attività relative ai dati degli utenti. Per ulteriori informazioni, consulta gli argomenti seguenti:

- EC2Launch v2
- EC2Launch
- EC2Config service

Per esempi di assemblaggio di una `UserData` proprietà in un CloudFormation modello, vedere Proprietà codificata Base64 e UserData Proprietà codificata Base64 con e. UserData AccessKey SecretKey

Per un esempio di esecuzione di comandi su un'istanza all'interno del gruppo Auto Scaling che funzionano con gli hook del ciclo di vita, consulta Tutorial: configurazione dei dati utente per recuperare lo stato del ciclo di vita obiettivo tramite i metadati dell'istanza nella Guida per l'utente di Amazon EC2 Auto Scaling.

Indice

- Script di dati utente
- Dati utente compressi
- Esecuzione dei dati utente
- Dati utente e strumenti per Windows PowerShell

Script di dati utente

Per l'esecuzione di script da `EC2Config` o `EC2Launch`, è necessario racchiudere lo script all'interno di un tag speciale quando viene aggiunto ai dati utente. Il tag da utilizzare dipende dal fatto che i comandi vengano eseguiti in una finestra del prompt dei comandi (comandi batch) o utilizzino Windows. PowerShell

Se si specificano sia uno script batch che uno PowerShell script Windows, lo script batch viene eseguito per primo e lo PowerShell script di Windows viene eseguito successivamente, indipendentemente dall'ordine in cui vengono visualizzati nei dati utente dell'istanza.

Se si utilizza un' AWS API, inclusa la AWS CLI, in uno script di dati utente, è necessario utilizzare un profilo di istanza all'avvio dell'istanza. Un profilo di istanza fornisce le AWS credenziali appropriate richieste dallo script di dati utente per effettuare la chiamata API. Per ulteriori informazioni, consulta Profili delle istanze. Le autorizzazioni assegnate al ruolo IAM dipendono dai servizi chiamati con l'API. Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.

Tipo di script

- Sintassi di script batch
- Sintassi per gli script di Windows PowerShell
- Sintassi per gli script di configurazione YAML
- Codifica Base64

Sintassi di script batch

Specificare uno script batch tramite il tag `script`. Separa i comandi utilizzando le interruzioni di riga, come illustrato nell'esempio seguente.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
```

Per impostazione predefinita, gli script di dati utente vengono eseguiti una volta all'avvio dell'istanza. Per eseguire gli script di dati utente ogni volta che si riavvia o avvia l'istanza, aggiungere `<persist>true</persist>` ai dati utente.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<persist>true</persist>
```

Agente EC2Launch v2

Per eseguire uno script di dati utente XML come processo distaccato con l'operazione executeScript EC2Launch v2 nella fase `UserData`, aggiungi `<detach>true</detach>` ai dati utente.

> **Note**
>
> Il tag detach non è supportato dai precedenti agenti di avvio.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<detach>true</detach>
```

Sintassi per gli script di Windows PowerShell

Le AMI di AWS Windows includono AWS Tools for Windows PowerShell, quindi è possibile specificare questi cmdlet nei dati utente. Se associ un ruolo IAM alla tua istanza, non devi specificare le credenziali per i cmdlet, poiché le applicazioni eseguite sull'istanza utilizzano le credenziali del ruolo per accedere alle AWS risorse (ad esempio, i bucket Amazon S3).

Specifica uno script di Windows utilizzando il tag. PowerShell `<powershell>` Separare i comandi tramite interruzioni di riga. Il tag `<powershell>` rileva la distinzione tra maiuscole e minuscole.

Ad esempio:

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
```

```
    New-Item $file -ItemType file
</powershell>
```

Per impostazione predefinita, gli script di dati utente vengono eseguiti una volta all'avvio dell'istanza. Per eseguire gli script di dati utente ogni volta che si riavvia o avvia l'istanza, aggiungere `<persist>true</persist>` ai dati utente.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

È possibile specificare uno o più PowerShell argomenti con il `<powershellArguments>` tag. Se non viene passato alcun argomento, EC2Launch e EC2Launch v2 aggiungono il seguente argomento per impostazione predefinita: `-ExecutionPolicy Unrestricted`.

Esempio:

```
<powershell>
    $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Agente EC2Launch v2

Per eseguire uno script di dati utente XML come processo distaccato con l'operazione executeScript EC2Launch v2 nella fase `UserData`, aggiungi `<detach>true</detach>` ai dati utente.

> **Note**
>
> Il tag detach non è supportato dai precedenti agenti di avvio.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
```

```
<detach>true</detach>
```

Sintassi per gli script di configurazione YAML

Se si utilizza EC2Launch v2 per eseguire script, è possibile utilizzare il formato YAML. Per visualizzare le attività di configurazione, i dettagli e gli esempi per EC2Launch v2, consulta Configurazione dell'attività di EC2Launch v2.

Specificare uno script YAML con l'attività `executeScript`.

Esempio di sintassi YAML per eseguire uno script PowerShell

```
version: 1.0
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
      New-Item $file -ItemType file
```

Esempio di sintassi YAML per eseguire uno script batch

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: batch
    runAs: localSystem
    content: |-
      echo Current date and time >> %SystemRoot%\Temp\test.log
      echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
```

Codifica Base64

Se utilizzi l'API Amazon EC2 o uno strumento che non esegue la codifica base64 dei dati utente, codificare direttamente i dati utente. In caso contrario, verrà registrato un errore sull'impossibilità di individuare i tag `script` o `powershell` da eseguire. Di seguito è riportato un esempio di codifica utilizzando Windows. PowerShell

```
$UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Di seguito è riportato un esempio che decodifica utilizzando. PowerShell

```
$Script =
 [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData))
```

Per ulteriori informazioni sulla codifica base64, vedere. https://www.ietf.org/rfc/rfc4648.txt

Dati utente compressi

EC2Launch v2 supporta i dati utente compressi come metodo per inviare dati utente che superano il limite di 16 KB imposto da IMDS. Per usare questa funzionalità, comprimi lo script dei dati utente in un archivio `.zip` e passalo all'istanza EC2. Quando EC2Launch v2 rileva dati utente compressi, decomprime automaticamente lo script dei dati utente compressi e lo esegue.

Come per i dati utente standard, se utilizzi l'API Amazon EC2 o uno strumento che non esegue la codifica base64 dei dati utente, codificare direttamente i dati utente compressi. Per ulteriori informazioni sul limite di dimensione dei dati utente e sulla codifica base64, visita consulta Accesso ai metadati dell'istanza per un'istanza EC2.

Esecuzione dei dati utente

Per impostazione predefinita, tutte le AMI di AWS Windows hanno l'esecuzione dei dati utente abilitata per l'avvio iniziale. Puoi specificare che gli script di dati utente vengano eseguiti la prossima volta che l'istanza è riavviata. In alternativa, puoi specificare che gli script di dati utente vengano eseguiti ogni volta che l'istanza è riavviata.

> **Note**
>
> Per impostazione predefinita, l'esecuzione dei dati utente non è abilitata dopo l'avvio iniziale. Per abilitare l'esecuzione dei dati utente al riavvio o all'avvio dell'istanza, consulta Esegui gli script durante i riavvii o gli avvii successivi.

Gli script di dati utente vengono eseguiti dall'account amministratore locale quando viene generata una password casuale. In caso contrario, gli script di dati utente vengono eseguiti dall'account del sistema.

Script di avvio dell'istanza

Gli script nei dati utente dell'istanza vengono eseguiti durante l'avvio iniziale dell'istanza. Se individui il tag `persist`, l'esecuzione dei dati utente è abilitata per i riavvii successivi. I file di log per EC2Launch v2, EC2Launch ed EC2Config contengono i risultati dell'output standard e i flussi di errore standard.

EC2Launch v2

Il file di log per EC2Launch v2 è `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> La cartella `C:\ProgramData` potrebbe essere nascosta. Per visualizzare la cartella, è necessario mostrare i file e le cartelle nascosti.

Le informazioni seguenti vengono registrate durante l'esecuzione dei dati utente:

- `Info: Converting user-data to yaml format` - Se i dati utente sono stati forniti in formato XML
- `Info: Initialize user-data state` - L'inizio dell'esecuzione dei dati utente
- `Info: Frequency is: always` - Se l'attività dei dati utente è in esecuzione a ogni avvio
- `Info: Frequency is: once` - Se l'attività dei dati utente è in esecuzione una sola volta
- `Stage: postReadyUserData execution completed` - La fine dell'esecuzione dei dati dell'utente

EC2Launch

Il file di log per EC2Launch è `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log`.

La cartella `C:\ProgramData` potrebbe essere nascosta. Per visualizzare la cartella, è necessario mostrare i file e le cartelle nascosti.

Le informazioni seguenti vengono registrate durante l'esecuzione dei dati utente:

- `Userdata execution begins` - L'inizio dell'esecuzione dei dati utente

- `<persist> tag was provided: true` - Se viene individuato il tag persist
- `Running userdata on every boot` - Se viene individuato il tag persist
- `<powershell> tag was provided.. running powershell content` - Se viene individuato il tag powershell
- `<script> tag was provided.. running script content` - Se viene individuato il tag script
- `Message: The output from user scripts` - Se vengono eseguiti script di dati utente, il loro output viene registrato

EC2Config

Il file di log per EC2config è `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2Config.log`. Le informazioni seguenti vengono registrate durante l'esecuzione dei dati utente:

- `Ec2HandleUserData: Message: Start running user scripts` - L'inizio dell'esecuzione dei dati utente
- `Ec2HandleUserData: Message: Re-enabled userdata execution` - Se viene individuato il tag persist
- `Ec2HandleUserData: Message: Could not find <persist> and </persist>` - Se non viene individuato il tag persist
- `Ec2HandleUserData: Message: The output from user scripts` - Se vengono eseguiti script di dati utente, il loro output viene registrato

Esegui gli script durante i riavvii o gli avvii successivi

Quando aggiorni i dati utente dell'istanza, il contenuto dei dati utente aggiornati viene riflesso automaticamente nei metadati dell'istanza al successivo riavvio o avvio dell'istanza. Tuttavia, a seconda dell'agente di avvio installato, potrebbe essere necessaria una configurazione aggiuntiva per configurare gli script dei dati utente da eseguire ai successivi riavvii o avvii.

Selezionando l'opzione Arresta con Sysprep, gli script dei dati utente vengono eseguiti al successivo avvio o riavvio dell'istanza, anche se non hai abilitato l'esecuzione dei dati utente per i riavvii o avvii successivi.

Per istruzioni su come abilitare l'esecuzione dei dati utente, seleziona la scheda corrispondente al tuo agente di avvio.

EC2Launch v2

A differenza di EC2Launch v1, EC2Launch v2 valuta l'attività dei dati utente a ogni avvio. Non è necessario pianificare manualmente l'attività relativa ai dati utente. I dati utente vengono eseguiti in base alle opzioni di frequenza o persistenza incluse.

Per gli script dei dati utente in XML

Per eseguire gli script dei dati utente ad ogni avvio, aggiungi il flag `<persist>true</persist>`. Se il flag persist non è compreso, lo script dei dati utente viene eseguito solo all'avvio iniziale.

Per i dati utente YAML

- Per eseguire un'attività nei dati utente all'avvio iniziale, imposta la `frequency` dell'attività su `once`.
- Per eseguire un'attività nei dati utente ad ogni avvio, imposta l'attività `frequency` su `always`.

EC2Launch

1. Connettersi all'istanza Windows.
2. Aprire una finestra di PowerShell comando ed eseguire uno dei seguenti comandi:

   Esegui una volta

   Per eseguire i dati utente una volta all'avvio successivo, utilizza il flag `-Schedule`.

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
   Schedule
   ```

   Esegui su tutti gli avvii successivi

   Per eseguire i dati utente su tutti gli avvii successivi, utilizza il flag `-SchedulePerBoot`.

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
   SchedulePerBoot
   ```

3. Disconnettersi dall'istanza Windows. Per eseguire gli script aggiornati al prossimo avvio dell'istanza, arresta l'istanza e aggiorna i dati utente.

EC2Config

1. Connettersi all'istanza Windows.
2. Aprire `C:\Program Files\Amazon\Ec2ConfigService\Ec2ConfigServiceSetting.exe`.
3. Per Dati utente, seleziona Abilita UserData l'esecuzione per il prossimo avvio del servizio.
4. Disconnettersi dall'istanza Windows. Per eseguire gli script aggiornati al prossimo avvio dell'istanza, arresta l'istanza e aggiorna i dati utente.

Dati utente e strumenti per Windows PowerShell

Puoi utilizzare gli Strumenti per Windows PowerShell per specificare, modificare e visualizzare i dati utente per la tua istanza. Per informazioni sulla visualizzazione dei dati utente dall'istanza tramite metadati dell'istanza, consulta Accesso ai metadati dell'istanza per un'istanza EC2. Per informazioni sui dati utente e su AWS CLI, vedereI dati dell'utente e AWS CLI.

Esempio: Specificare i dati utente dell'istanza all'avvio

Creare un file di testo con i dati utente dell'istanza. Per eseguire gli script dei dati utente ogni volta che si riavvia o avvia l'istanza, aggiungere `<persist>true</persist>`, come illustrato nell'esempio seguente:

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Per specificare i dati utente dell'istanza all'avvio dell'istanza, usa il New-EC2Instance comando. Questo comando non esegue la codifica base64 al tuo posto dei dati utente. Utilizza i seguenti comandi per codificare i dati utente in un file di testo denominato `script.txt`.

```
PS C:\> $Script = Get-Content -Raw script.txt
PS C:\> $UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Utilizzare il parametro `-UserData` per trasferire i dati utente al comando New-EC2Instance.

```
PS C:\> New-EC2Instance -ImageId ami-abcd1234 -MinCount 1 -MaxCount 1 -
InstanceType m3.medium \
    -KeyName my-key-pair -SubnetId subnet-12345678 -SecurityGroupIds sg-1a2b3c4d \
    -UserData $UserData
```

Esempio: Aggiornamento dei dati utente dell'istanza di un'istanza arrestata

È possibile modificare i dati utente di un'istanza interrotta utilizzando il Edit-EC2InstanceAttribute comando.

Creare un file di testo con il nuovo script. Utilizza i seguenti comandi per codificare i dati utente nel file di testo denominato `new-script.txt`.

```
PS C:\> $NewScript = Get-Content -Raw new-script.txt
PS C:\> $NewUserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($NewScript))
```

Utilizzare i parametri `-UserData` e `-Value` per specificare i dati utente.

```
PS C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute userData -
Value $NewUserData
```

Esempio: Visualizzazione dei dati utente dell'istanza

Per recuperare i dati utente per un'istanza, utilizzate il Get-EC2InstanceAttribute comando.

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute
 userData).UserData
```

Di seguito è riportato un output di esempio. Tieni presente che i dati utente sono codificati.

```
PHBvd2Vyc2hlbGw
+DQpSZW5hbWUtQ29tcHV0ZXIgLU5ld05hbWUgdXNlci1kYXRhLXRlc3QNCjwvcG93ZXJzaGVsbD4=
```

Utilizzare i comandi seguenti per archiviare i dati utente codificati in una variabile e poi decodificarli.

```
PS C:\> $UserData_encoded = (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -
Attribute userData).UserData
```

```
PS C:
\> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData_encoded)
```

Di seguito è riportato un output di esempio.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Esempio: rinominare l'istanza per corrispondere al valore di tag

È possibile utilizzare il Get-EC2Tag comando per leggere il valore del tag, rinominare l'istanza al primo avvio in modo che corrisponda al valore del tag e riavviare. Per eseguire efficacemente questo comando, è necessario disporre di un ruolo con autorizzazioni `ec2:DescribeTags` collegate all'istanza, perché le informazioni sul tag sono recuperate da una chiamata all'API. Per ulteriori informazioni sulle autorizzazioni di impostazioni tramite i ruoli IAM, consulta Collegamento di un ruolo IAM all'istanza.

IMDSv2

```
<powershell>
    [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -
UseBasicParsing
    $instanceId = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" =
 $token} -Method GET -Uri 'http://169.254.169.254/latest/meta-data/instance-id' -
UseBasicParsing
 $nameValue = (Get-EC2Tag -Filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
```

```
</powershell>
```

IMDSv1

```
<powershell>
 $instanceId = (Invoke-WebRequest http://169.254.169.254/latest/meta-data/instance-
id -UseBasicParsing).content
 $nameValue = (Get-EC2Tag -Filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

È inoltre possibile rinominare l'istanza utilizzando i tag nei metadati delle istanze, se l'istanza è configurata su access tags from the instance metadata (accedi ai tag dai metadati dell'istanza). Per ulteriori informazioni, consulta Visualizza i tag per le istanze EC2 utilizzando i metadati dell'istanza.

IMDSv2

```
<powershell>
    [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -
UseBasicParsing
 $nameValue = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
 -Method GET -Uri 'http://169.254.169.254/latest/meta-data/tags/instance/Name' -
UseBasicParsing
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
```

```
        Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

IMDSv1

```
<powershell>
 $nameValue = Get-EC2InstanceMetadata -Path /tags/instance/Name
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Identificazione di ciascuna istanza lanciata in una singola richiesta

Questo esempio illustra come puoi utilizzare sia i dati utente che i metadati dell'istanza per configurare le istanze Amazon EC2.

> **Note**
>
> Negli esempi riportati in questa sezione viene utilizzato l'indirizzo IPv4 del servizio di metadati dell'istanza (IMDS): `169.254.169.254`. Se si recuperano i metadati per le istanze EC2 tramite l'indirizzo IPv6, accertarsi invece di abilitare e utilizzare l'indirizzo IPv6: `[fd00:ec2::254]`. L'indirizzo IPv6 del servizio di metadati dell'istanza (IMDS) è compatibile con i comandi IMDSv2. L'indirizzo IPv6 è accessibile solo su Nitro-based istanze in IPv6-supported sottoreti (dual stack o solo IPv6).

Alice vuole avviare quattro istanze dell'AMI del suo database preferito, dove la prima istanza funge da istanza originale e le altre tre fungono da repliche. Al momento dell'avvio vuole aggiungere i dati

utente relativi alla strategia di replica per ciascuna replica. Consapevole del fatto che questi dati saranno disponibili per tutte e quattro le istanze, deve strutturare i dati utente in modo da consentire a ciascuna istanza di riconoscere le parti valide. A tale scopo, utilizza il valore `ami-launch-index` dei metadati dell'istanza, che sarà univoco per ogni istanza. Se hai avviato più di un'istanza contemporaneamente, il `ami-launch-index`indica l'ordine in base al quale sono state avviate le istanze. Il valore della prima istanza avviata è `0`.

Di seguito sono descritti i dati utente strutturati da Alice.

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

I dati `replicate-every=1min` definiscono la configurazione della prima replica, `replicate-every=5min` definisce la configurazione della seconda replica e così via. Alice decide di specificare questi dati come stringa ASCII con una barra verticale (`|`) per delimitare i dati per le singole istanze.

Alice avvia le quattro istanze utilizzando il comando run-instances e specificando i dati utente.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 4 \
    --instance-type t2.micro \
    --user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

Dopo l'avvio, le istanze includono una copia dei dati utente e i metadati comuni riportati di seguito:

- ID AMI: ami-0abcdef1234567890
- ID prenotazione: r-1234567890abcabc0
- Chiavi pubbliche: nessuna
- Nome del gruppo di sicurezza: nome di default
- Tipo di istanza: t2.micro

Tuttavia, ciascuna istanza ha metadati univoci, come mostrato nelle tabelle seguenti.

Metadati	Valore
instance-id	i-1234567890abcdef0
ami-launch-index	0

Metadati	Valore
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.35

Metadati	Valore
instance-id	i-0598c7d356eba48d7
ami-launch-index	1
public-hostname	ec2-67-202-51-224.compute-1.amazonaws.com
public-ipv4	67.202.51.224
local-hostname	ip-10-251-50-36.ec2.internal
local-ipv4	10.251.50.36

Metadati	Valore
instance-id	i-0ee992212549ce0e7
ami-launch-index	2
public-hostname	ec2-67-202-51-225.compute-1.amazonaws.com
public-ipv4	67.202.51.225
local-hostname	ip-10-251-50-37.ec2.internal
local-ipv4	10.251.50.37

Metadati	Valore
instance-id	i-1234567890abcdef0
ami-launch-index	3
public-hostname	ec2-67-202-51-226.compute-1.amazonaws.com
public-ipv4	67.202.51.226
local-hostname	ip-10-251-50-38.ec2.internal
local-ipv4	10.251.50.38

Alice può utilizzare il valore `ami-launch-index` per determinare la parte di dati utente validi per un'istanza specifica.

1. Collega una delle istanze e recupera il valore `ami-launch-index` per tale istanza per assicurarsi che sia una delle repliche:

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/ami-launch-index
   2
   ```

   Per le fasi seguenti, le richieste IMDSv2 utilizzano il token memorizzato dal comando IMDSv2 precedente, presupponendo che non sia scaduto.

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index
   2
   ```

2. Salva il valore `ami-launch-index` come una variabile.

IMDSv2

```
[ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
 http://169.254.169.254/latest/meta-data/ami-launch-index`
```

IMDSv1

```
[ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-
launch-index`
```

3. Salva i dati utente come una variabile.

   IMDSv2

   ```
   [ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/user-data`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ user_data=`curl http://169.254.169.254/latest/user-data`
   ```

4. Alice utilizza infine il comando cut per estrarre la parte di dati utente valida per l'istanza specifica.

   IMDSv2

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

   IMDSv1

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

Individua se un host è un'istanza EC2

Potresti aver bisogno di sapere se la tua applicazione o il tuo sito web è in esecuzione su un'istanza EC2, soprattutto se hai un ambiente di elaborazione misto. Puoi utilizzare una delle seguenti opzioni per stabilire se l'host della tua applicazione o del tuo sito web è un'istanza EC2.

Opzioni

- Ispezionare l'Documenti di identità dell'istanza
- Ispezionare l'UUID del sistema
- Ispezione dell'identificatore di generazione della macchina virtuale del sistema

Ispezionare l'Documenti di identità dell'istanza

Ogni istanza ha un documento di identità dell'istanza firmato che puoi verificare crittograficamente. Puoi trovare questi documenti utilizzando il servizio di metadati di istanza (IMDS).

Per ulteriori informazioni, consulta Documenti di identità dell'istanza.

Ispezionare l'UUID del sistema

Puoi ottenere l'UUID di sistema e verificare la presenza nell'ottetto iniziale dell'UUID per `EC2` (in Linux, potrebbe essere `ec2` in minuscolo). Questo metodo è rapido ma potenzialmente inaccurato perché vi è una piccola probabilità che un sistema che non è un'istanza EC2 possa avere un UUID che inizia con questi caratteri. Inoltre, alcune versioni di SMBIOS usano il formato little-endian, che non include `EC2` all'inizio dell'UUID . Questo potrebbe essere il caso delle istanze EC2 che utilizzano SMBIOS 2.4 per Windows o delle distribuzioni Linux diverse da Amazon Linux che dispongono di una propria implementazione di SMBIOS.

Esempio di Linux: Ottenere l'UUID dalla DMI (solo AMI HVM)

Utilizzare il comando seguente per ottenere l'UUID utilizzando la Desktop Management Interface (DMI):

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

Nell'esempio seguente di output, l'UUID inizia con "EC2", il che indica che il sistema è probabilmente un'istanza EC2.

```
EC2E1916-9099-7CAF-FD21-012345ABCDEF
```

Nell'esempio seguente di output, l'UUID è rappresentato in formato little-endian.

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

In alternativa, per le istanze create sul sistema Nitro, è possibile utilizzare il seguente comando:

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

Se l'output è un ID dell'istanza, come nell'esempio seguente, il sistema è un'istanza EC2:

```
i-0af01c0123456789a
```

Esempio di Linux: Ottenere l'UUID dall'hypervisor (solo AMI PV)

Utilizzare il seguente comando per ottenere l'UUID dall'hypervisor:

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

Nell'esempio seguente di output, l'UUID inizia con "ec2", il che indica che il sistema è probabilmente un'istanza EC2.

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

Esempio Windows: ottenere l'UUID utilizzando WMI o Windows PowerShell

Utilizza la riga di comando Windows Management Instrumentation (WMIC) nel modo seguente:

```
wmic path win32_computersystemproduct get uuid
```

In alternativa, se utilizzi Windows PowerShell, utilizza il Get-WmiObject cmdlet come segue:

```
PS C:\> Get-WmiObject -query "select uuid from Win32_ComputerSystemProduct" | Select
 UUID
```

Nell'esempio seguente di output, l'UUID inizia con "EC2", il che indica che il sistema è probabilmente un'istanza EC2.

```
EC2AE145-D1DC-13B2-94ED-012345ABCDEF
```

Per istanze che utilizzano SMBIOS 2.4, l'UUID potrebbe essere rappresentato in formato little-endian, ad esempio:

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Ispezione dell'identificatore di generazione della macchina virtuale del sistema

Un identificatore di generazione della macchina virtuale è costituito da un buffer univoco di 128 bit interpretato come identificatore intero casuale crittografico. È possibile recuperare l'identificatore di generazione della macchina virtuale per identificare l'istanza di Amazon Elastic Compute Cloud. L'identificatore di generazione viene esposto all'interno del sistema operativo guest dell'istanza tramite una voce della tabella ACPI. Il valore cambierà se il computer viene clonato, copiato o importato in AWS, ad esempio con VM. Import/Export

Esempio: Recupera l'identificatore di generazione della macchina virtuale da Linux

Puoi utilizzare i seguenti comandi per recuperare l'identificatore di generazione della macchina virtuale dalle istanze che eseguono Linux.

Amazon Linux 2

1. Aggiorna i pacchetti software esistenti, se necessario, utilizzando il seguente comando:

   ```
   sudo yum update
   ```

2. Se necessario, utilizza il pacchetto busybox utilizzando il seguente comando:

   ```
   sudo curl https://www.rpmfind.net/linux/epel/next/8/Everything/x86_64/Packages/
   b/busybox-1.35.0-2.el8.next.x86_64.rpm --output busybox.rpm
   ```

3. Se necessario, installa i pacchetti prerequisiti utilizzando il seguente comando:

   ```
   sudo yum install busybox.rpm iasl -y
   ```

4. Esegui il seguente comando `iasl` per produrre output dalla tabella ACPI:

   ```
   sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
   ```

5. Esegui il comando seguente per esaminare l'output del comando `iasl`:

   ```
   cat SSDT2.dsl
   ```

   L'output deve restituire lo spazio degli indirizzi necessario per recuperare l'identificatore di generazione della macchina virtuale:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
```

```
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

6. (Opzionale) Aumenta le autorizzazioni del terminale per i passaggi rimanenti con il seguente comando:

```
sudo -s
```

7. Utilizza il comando seguente per archiviare lo spazio degli indirizzi precedentemente raccolto:

```
VMGN_ADDR=0xFED01000
```

8. Utilizza il comando seguente per scorrere lo spazio degli indirizzi e creare l'identificatore di generazione della macchina virtuale:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

9. Recupera l'identificatore di generazione della macchina virtuale dal file di output con il seguente comando:

```
cat vmgenid ; echo
```

L'output visualizzato dovrebbe essere simile al seguente:

```
EC2F335D979132C4165896753E72BD1C
```

Ubuntu

1. Aggiorna i pacchetti software esistenti, se necessario, utilizzando il seguente comando:

```
sudo apt update
```

2. Se necessario, installa i pacchetti prerequisiti utilizzando il seguente comando:

```
sudo apt install busybox iasl -y
```

3. Esegui il seguente comando `iasl` per produrre output dalla tabella ACPI:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

4. Esegui il comando seguente per esaminare l'output del comando `iasl`:

```
cat SSDT2.dsl
```

L'output deve restituire lo spazio degli indirizzi necessario per recuperare l'identificatore di generazione della macchina virtuale:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
```

```
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

5. (Opzionale) Aumenta le autorizzazioni del terminale per i passaggi rimanenti con il seguente comando:

```
sudo -s
```

6. Utilizza i comandi seguenti per archiviare lo spazio degli indirizzi precedentemente raccolto:

```
VMGN_ADDR=0xFED01000
```

7. Utilizza il comando seguente per scorrere lo spazio degli indirizzi e creare l'identificatore di generazione della macchina virtuale:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

8. Recupera l'identificatore di generazione della macchina virtuale dal file di output con il seguente comando:

```
cat vmgenid ; echo
```

L'output visualizzato dovrebbe essere simile al seguente:

```
EC2F335D979132C4165896753E72BD1C
```

Esempio: recupera l'identificatore di generazione della macchina virtuale da Windows

È possibile creare un'applicazione di esempio per recuperare l'identificatore di generazione della macchina virtuale dalle istanze che eseguono Windows. Per ulteriori informazioni, consulta Obtaining the virtual machine generation identifier (Ottenimento dell'identificatore di generazione della macchina virtuale) nella documentazione Microsoft.

Documenti di identità dell'istanza per le istanze Amazon EC2

Ogni istanza avviata dispone di un Documenti di identità dell'istanza che fornisce informazioni sull'istanza stessa. Puoi utilizzare il Documenti di identità dell'istanza per convalidare gli attributi dell'istanza.

Il documento di identità dell'istanza viene generato quando l'istanza viene arrestata e avviata, riavviata o avviata. Puoi accedere al documento di identità di un'istanza tramite il servizio di metadati di istanza (IMDS). Per le istruzioni, consulta Recupera il documento di identità dell'istanza.

Il documento di identità dell'istanza utilizza il formato JSON in testo semplice. Include le seguenti informazioni.

Dati	Description
`accountId`	L'ID dell' AWS account che ha avviato l'istanza.

Dati	Description
`architecture`	L'architettura dell'AMI utilizzata per avviare l'istanza (i386 | x86_64 | arm64).
`availabilityZone`	Il nome della Zona di disponibilità in cui viene eseguita l'istanza. Ad esempio, `us-east-1` . Tieni presente che i nomi delle zone di disponibilità potrebbero differire tra AWS gli account.
`billingProducts`	I prodotti di fatturazione dell'istanza.
`devpayProductCodes`	Obsoleta.
`imageId`	L'ID dell'AMI utilizzato per avviare l'istanza.
`instanceId`	ID dell'istanza.
`instanceType`	Il tipo di istanza dell'istanza.
`kernelId`	L'ID del kernel associato all'istanza, se applicabile.
`marketplaceProductCodes`	Il codice Marketplace AWS prodotto dell'AMI utilizzato per avviare l'istanza.
`pendingTime`	La data e l'ora in cui l'istanza è stata avviata.
`privateIp`	L'indirizzo IP privato dell'istanza. Per IPv4-only le istanze dual-stack, contiene l'indirizzo IPv4. Ad IPv6-only esempio, contiene l'indirizzo IPv6.
`ramdiskId`	L'ID del disco RAM associato a questa istanza, se applicabile.
`region`	La regione in cui viene eseguita l'istanza.
`version`	Versione del formato del Documenti di identità dell'istanza.

Recupero del documento di identità dell'istanza per un'istanza EC2

Il documento di identità di un'istanza Amazon EC2 utilizza un formato JSON di testo semplice. Per una descrizione del contenuto del documento di identità di un'istanza, consulta. the section called "Documenti di identità dell'istanza"

Il documento di identità dell'istanza è memorizzato nei metadati per l'istanza, nella categoria dei dati dinamici `instance-identity/document`. Puoi accedere al documento di identità dell'istanza connettendoti all'istanza e recuperandolo dai metadati dell'istanza.

Puoi accedere ai metadati dell'istanza utilizzando l'indirizzo IPv4 169.254.169.254 o l'indirizzo IPv6 fd00:ec2::254. Si tratta di Link-local indirizzi, il che significa che puoi accedervi solo dall'istanza. Negli esempi riportati in questa pagina viene utilizzato l'indirizzo IPv4 del servizio di metadati dell'istanza (IMDS): 169.254.169.254. Per recuperare i metadati dell'istanza per le istanze EC2 su IPv6, utilizza fd00:ec2::254.

Per verificare l'autenticità del documento di identità di un'istanza dopo averlo recuperato, consulta Verifica documento di identità dell'istanza.

IMDSv2

Linux

Esegui il comando seguente dall'istanza Linux per recuperare il documento d'identità dell'istanza.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

Esegui il cmdlet seguente dall'istanza Windows per recuperare il documento d'identità dell'istanza.

```
[string]$token = (Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token-ttl-seconds' = '21600'} `
    -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -UseBasicParsing).Content
```

```
(Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $token} `
```

```
    -Uri 'http://169.254.169.254/latest/dynamic/instance-identity/document' -
UseBasicParsing).Content
```

IMDSv1

Linux

Esegui il comando seguente dall'istanza Linux per recuperare il documento d'identità dell'istanza.

```
curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

Esegui il cmdlet seguente dall'istanza Windows per recuperare il documento d'identità dell'istanza.

```
(Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/
document).Content
```

Di seguito è riportato un output di esempio.

```
{
    "devpayProductCodes" : null,
    "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],
    "availabilityZone" : "us-west-2b",
    "privateIp" : "10.158.112.84",
    "version" : "2017-09-30",
    "instanceId" : "i-1234567890abcdef0",
    "billingProducts" : null,
    "instanceType" : "t2.micro",
    "accountId" : "123456789012",
    "imageId" : "ami-5fb8c835",
    "pendingTime" : "2016-11-19T16:32:11Z",
    "architecture" : "x86_64",
    "kernelId" : null,
    "ramdiskId" : null,
    "region" : "us-west-2"
}
```

Verifica il documento di identità dell'istanza per un'istanza Amazon EC2

Se si intende utilizzare i contenuti del Documenti di identità dell'istanza per uno scopo importante, occorre verificarne il contenuto e l'autenticità prima di utilizzarlo.

Il Documenti di identità dell'istanza di testo normale è accompagnato da tre firme con hash e crittografate. Puoi utilizzare queste firme per verificare l'origine e l'autenticità del Documenti di identità dell'istanza e delle informazioni incluse. Vengono fornite le seguenti firme:

- Base64-encoded Firma: si tratta di un hash SHA256 codificato in base64 del documento di identità dell'istanza crittografato utilizzando una coppia di chiavi RSA.
- Firma PKCS7: si tratta di un hash SHA1 del Documenti di identità dell'istanza che è crittografato utilizzando una coppia di chiavi DSA.
- RSA-2048 Firma: si tratta di un hash SHA256 del documento di identità dell'istanza crittografato utilizzando una coppia di chiavi. RSA-2048

Ogni firma è disponibile in un endpoint diverso nei metadati dell'istanza. Puoi utilizzare una di queste firme qualsiasi a seconda dei requisiti di hashing e di crittografia. Per verificare le firme, è necessario utilizzare il certificato pubblico corrispondente. AWS

Opzioni

- Opzione 1: Verifica il documento di identità dell'istanza usando la firma PKCS7
- Opzione 2: Verifica il documento di identità dell'istanza usando la firma con codifica base64
- Opzione 3: verifica il documento di identità dell'istanza utilizzando la firma RSA-2048

Opzione 1: Verifica il documento di identità dell'istanza usando la firma PKCS7

Questo argomento spiega come verificare il documento di identità dell'istanza utilizzando la firma PKCS7 e il certificato pubblico AWS DSA.

Istanze Linux

Per verificare il documento di identità dell'istanza utilizzando la firma PKCS7 e il AWS Certificato pubblico DSA

1. Collegati all'istanza.

2. Recuperare la firma PKCS7 dai metadati dell'istanza e aggiungerla a un file denominato `pkcs7` insieme all'intestazione e al piè di pagina richiesti. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
    && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/pkcs7 >> pkcs7 \
    && echo "" >> pkcs7 \
    && echo "-----END PKCS7-----" >> pkcs7
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
    && curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7
    >> pkcs7 \
    && echo "" >> pkcs7 \
    && echo "-----END PKCS7-----" >> pkcs7
   ```

3. Trovare il certificato pubblico DSA per la propria regione in AWS certificati pubblici, ad esempio, firme di documenti di identità e aggiungere i contenuti in un nuovo file denominato `certificate`.

4. Utilizzare il comando OpenSSL smime per verificare la firma. Includere l'opzione `-verify` per indicare che la firma deve essere verificata e l'opzione `-noverify` per indicare che il certificato non deve essere verificato.

   ```
   $ openssl smime -verify -in pkcs7 -inform PEM -certfile certificate -noverify | tee
    document
   ```

   Se la firma è valida, viene visualizzato il messaggio `Verification successful`.

   Il comando, inoltre, scrive i contenuti del documento di identità dell'istanza in un nuovo file denominato `document`. Puoi confrontare i contenuti del documento di identità dell'istanza dai metadati dell'istanza con i contenuti di questo file utilizzando i comandi seguenti.

   ```
   $ openssl dgst -sha256 < document
   ```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Se non è possibile verificare la firma, contattare Supporto.

Istanze Windows

Prerequisiti

Questa procedura richiede la classe `System.Security` Microsoft .NET Core. Per aggiungere la classe alla PowerShell sessione, esegui il comando seguente.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> Il comando aggiunge la classe solo alla PowerShell sessione corrente. Se avvii una nuova sessione, devi eseguire nuovamente il comando.

Per verificare il documento di identità dell'istanza utilizzando la firma PKCS7 e il AWS Certificato pubblico DSA

1. Collegati all'istanza.
2. Recuperare la firma PKCS7 dai metadati dell'istanza, convertirla in un array di byte e aggiungerla a una variabile denominata `$Signature`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-ec2-
   metadata-token-ttl-seconds' = '21600'} -Uri http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} -Uri http://169.254.169.254/latest/
   dynamic/instance-identity/pkcs7).Content)
   ```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Uri
 http://169.254.169.254/latest/dynamic/instance-identity/pkcs7).Content)
```

3. Recuperare il documento di identità dell'istanza in testo normale dai metadati dell'istanza, convertirlo in un array di byte e aggiungerlo a una variabile denominata `$Document`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} -Uri http://169.254.169.254/latest/
   dynamic/instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Trovare il certificato pubblico DSA per la propria regione in AWS certificati pubblici, ad esempio, firme di documenti di identità e aggiungere i contenuti in un nuovo file denominato `certificate.pem`.

5. Estrarre il certificato dal file del certificato e archiviarlo in una variabile denominata `$Store`.

   ```
   PS C:\> $Store =
    [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
   Path certificate.pem)))
   ```

6. Verifica la firma.

   ```
   PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
   ```

   ```
   PS C:\> $SignatureDocument.Decode($Signature)
   ```

   ```
   PS C:\> $SignatureDocument.CheckSignature($Store, $true)
   ```

Se la firma è valida, il comando non restituisce alcun output. Se non è possibile verificare la firma, il comando restituisce `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Se non è possibile verificare la firma, contattare Supporto AWS.

7. Convalidare il contenuto del documento di identità dell'istanza.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Se il contenuto del documento di identità dell'istanza è valido, il comando restituisce `True`. Se il documento di identità dell'istanza non può essere convalidato, contatta Supporto AWS.

Opzione 2: Verifica il documento di identità dell'istanza usando la firma con codifica base64

Questo argomento spiega come verificare il documento di identità dell'istanza utilizzando la firma con codifica base64 e il certificato pubblico RSA. AWS

Istanze Linux

Per convalidare il documento di identità dell'istanza utilizzando la firma con codifica base64 e il AWS Certificato pubblico RSA

1. Collegati all'istanza.
2. Recuperare la firma con codifica base64 dai metadati dell'istanza, convertirla in un formato binario e aggiungerla a un file denominato `signature`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
 && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/signature | base64 -d >> signature
```

IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/signature |
 base64 -d >> signature
```

3. Recuperare il Documenti di identità dell'istanza in testo normale dai metadati dell'istanza e aggiungerlo a un file denominato `document`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/document >> document
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
    >> document
   ```

4. Trovare il certificato pubblico RSA per la propria regione in AWS certificati pubblici, ad esempio, firme di documenti di identità e aggiungere i contenuti in un nuovo file denominato `certificate`.
5. Estrai la chiave pubblica dal certificato pubblico AWS RSA e salvala in un file denominato. `key`

   ```
   $ openssl x509 -pubkey -noout -in certificate >> key
   ```

6. Utilizzare il comando OpenSSL dgst per verificare il Documenti di identità dell'istanza.

   ```
   $ openssl dgst -sha256 -verify key -signature signature document
   ```

   Se la firma è valida, viene visualizzato il messaggio `Verification successful`.

   Il comando, inoltre, scrive i contenuti del documento di identità dell'istanza in un nuovo file denominato `document`. Puoi confrontare i contenuti del documento di identità dell'istanza dai metadati dell'istanza con i contenuti di questo file utilizzando i comandi seguenti.

   ```
   $ openssl dgst -sha256 < document
   ```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Se non è possibile verificare la firma, contattare Supporto.

Istanze Windows

Per convalidare il documento di identità dell'istanza utilizzando la firma codificata in base64 e il AWS Certificato pubblico RSA

1. Collegati all'istanza.
2. Recuperare la firma con codifica base64 dai metadati dell'istanza, convertirla in un array di byte e aggiungerla alla variabile denominata `$Signature`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/signature).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
   ```

3. Recuperare il documento di identità dell'istanza in testo normale dai metadati dell'istanza, convertirlo in un array di byte e aggiungerlo a una variabile denominata `$Document`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

IMDSv2

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
 @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
instance-identity/document).Content)
```

IMDSv1

```
PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Trovare il certificato pubblico RSA per la propria regione in AWS certificati pubblici, ad esempio, firme di documenti di identità e aggiungere i contenuti in un nuovo file denominato `certificate.pem`.
5. Verificare il documento di identità dell'istanza.

```
PS C:\> [Security.Cryptography.X509Certificates.X509Certificate2]::new((Resolve-
Path certificate.pem)).PublicKey.Key.VerifyData($Document, 'SHA256', $Signature)
```

Se la firma è valida, il comando restituisce `True`. Se non è possibile verificare la firma, contattare Supporto.

Opzione 3: verifica il documento di identità dell'istanza utilizzando la firma RSA-2048

Questo argomento spiega come verificare il documento di identità dell'istanza utilizzando la RSA-2048 firma e il certificato AWS RSA-2048 pubblico.

Istanze Linux

Per verificare il documento di identità dell'istanza utilizzando la RSA-2048 firma e il AWS RSA-2048 certificato pubblico

1. Collegati all'istanza.
2. Recupera la RSA-2048 firma dai metadati dell'istanza e aggiungila a un file denominato nell'intestazione e nel `rsa2048` piè di pagina richiesti. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

IMDSv2

```
$ echo "-----BEGIN PKCS7-----" >> rsa2048 \
 && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
 && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/rsa2048 >> rsa2048 \
 && echo "" >> rsa2048 \
 && echo "-----END PKCS7-----" >> rsa2048
```

IMDSv1

```
$ echo "-----BEGIN PKCS7-----" >> rsa2048 \
 && curl -s http://169.254.169.254/latest/dynamic/instance-identity/rsa2048
 >> rsa2048 \
 && echo "" >> rsa2048 \
 && echo "-----END PKCS7-----" >> rsa2048
```

3. Trova il certificato RSA-2048 pubblico per la tua regione in AWS certificati pubblici, ad esempio, firme di documenti di identità e aggiungi il contenuto a un nuovo file denominato. `certificate`
4. Utilizzare il comando OpenSSL smime per verificare la firma. Includere l'opzione `-verify` per indicare che la firma deve essere verificata e l'opzione `-noverify` per indicare che il certificato non deve essere verificato.

   ```
   $ openssl smime -verify -in rsa2048 -inform PEM -certfile certificate -noverify |
    tee document
   ```

   Se la firma è valida, viene visualizzato il messaggio `Verification successful`. Se non è possibile verificare la firma, contattare Supporto.

Istanze Windows

Prerequisiti

Questa procedura richiede la classe `System.Security` Microsoft .NET Core. Per aggiungere la classe alla PowerShell sessione, esegui il comando seguente.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> Il comando aggiunge la classe solo alla PowerShell sessione corrente. Se avvii una nuova sessione, devi eseguire nuovamente il comando.

Per verificare il documento di identità dell'istanza utilizzando la RSA-2048 firma e il AWS RSA-2048 certificato pubblico

1. Collegati all'istanza.
2. Recupera la RSA-2048 firma dai metadati dell'istanza, la converti in un array di byte e aggiungila a una variabile denominata. `$Signature` Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/rsa2048).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
   ```

3. Recuperare il documento di identità dell'istanza in testo normale dai metadati dell'istanza, convertirlo in un array di byte e aggiungerlo a una variabile denominata `$Document`. Utilizzare uno dei comandi seguenti a seconda della versione IMDS utilizzata dall'istanza.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

IMDSv1

```
PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Trova il certificato RSA-2048 pubblico per la tua regione in AWS certificati pubblici, ad esempio, firme di documenti di identità e aggiungi il contenuto a un nuovo file denominato `certificate.pem`

5. Estrarre il certificato dal file del certificato e archiviarlo in una variabile denominata `$Store`.

```
PS C:\> $Store =
 [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
Path certificate.pem)))
```

6. Verifica la firma.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

   Se la firma è valida, il comando non restituisce alcun output. Se non è possibile verificare la firma, il comando restituisce `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Se non è possibile verificare la firma, contattare Supporto AWS.

7. Convalidare il contenuto del documento di identità dell'istanza.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

   Se il contenuto del documento di identità dell'istanza è valido, il comando restituisce `True`. Se il documento di identità dell'istanza non può essere convalidato, contatta Supporto AWS.

AWS certificati pubblici, ad esempio, firme di documenti di identità

I seguenti certificati AWS pubblici possono essere utilizzati per verificare il contenuto del documento di identità dell'istanza di un'istanza, come descritto inVerifica documento di identità dell'istanza.

Assicurarsi di utilizzare il certificato corretto per la propria regione e per la procedura di verifica utilizzata. Se si verifica la firma PKCS7, utilizzare il certificato DSA. Se si verifica la firma con codifica base64, utilizzare il certificato RSA. Se stai verificando la RSA-2048 firma, usa il RSA-2048 certificato.

Espandi ciascuna regione qui sotto per visualizzare i Region-specific certificati.

Stati Uniti orientali (Virginia settentrionale) – us-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUE1y2NIKCU+Rg4uu4u32koG9QEYIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MzQwMVoXDTI5MDQyODE3MzQwMVowXDELMAkGA1UEBhMCVVMx
```

```
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUE1y2NIKC
U+Rg4uu4u32koG9QEYIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAlxSmwcWnhT4uAeSinJuz+1BTcKhVSWb5jT8pYjQb8ZoZkXXRGb09mvYeU
NeqOBr27rvRAnaQ/9LUQf72+SahDFuS4CMI8nwowytqbmwquqFr4dxA/SDADyRiF
ea1UoMuNHTY49J/1vPomqsVn7mugTp+TbjqCfOJTpu0temHcFA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALFpzEAVWaQZMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU5MTJaGA8yMTk1MDExNzA4NTkxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjS2vqZu9mEOhOq+0bRpAbCUiapbZMFNQqRg7kTlr7Cf+gDqXKpHPjsng
SfNz+JHQd8WPI+pmNs+q0Z2aTe23klmf2U52KH9/j1k8RlIbap/yFibFTSedmegX
E5r447GbJRsHUmuIIfZTZ/oRlpuIIO5/Vz7SOj22tdkdY2ADp7caZkNxhSP915fk
2jJMTBUOzyXUS2rBU/ulNHbTTeePjcEkvzVYPahD30TeQ+/A+uWUu89bHSQOJR8h
Um4cFApzZgN3aD5j2LrSMu2pctkQwf9CaWyVznqrsGYjYOY66LuFzSCXwqSnFBfv
fFBAFsjCgY24G2DoMyYkF3MyZlu+rwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUrynSPp4uqSECwy+PiO4qyJ8TWSkwgY4GA1UdIwSBhjCBg4AUrynS
Pp4uqSECwy+PiO4qyJ8TWSmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALFpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADW/s8lXijwdP6NkEoH1m9XLrvK4YTqkNfR6
er/uRRgTx2QjFcMNrx+g87gAml11z+D0crAZ5LbEhDMs+JtZYR3ty0HkDk6SJM85
haoJNAFF7EQ/zCp1EJRIkLLsC7bcDL/Eriv1swt78/BB4RnC9W9kSp/sxd5svJMg
N9a6FAplpNRsWAnbP8JBlAP93oJzblX2LQXgykTghMkQO7NaY5hg/H5o4dMPclTK
lYGqlFUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZWtxwZ0osljV4rDjm9Q3VpA
NWIsDEcp3GUB4proOR+C7PNkY+VGODitBOw09qBGosCBstwyEqY=
-----END CERTIFICATE-----
```

Stati Uniti orientali (Ohio) - us-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUVJTc+hOU+8Gk3JlqsX438Dk5c58wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MTE0OVoXDTI5MDQyODE3MTE0OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUVJTc+hOU
+8Gk3JlqsX438Dk5c58wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAywJQaVNWJqW0R0T0xVOSoN1GLk9x9kKEuN67RN9CLin4dA97qa7Mr5W4P
FZ6vnh5CjOhQBRXV9xJUeYSdqVItNAUFK/fEzDdjf1nUfPlQ3OJ49u6CV01NoJ9m
usvY9kWcV46dqn2bk2MyfTTgvmeqP8fiMRPxxnVRkSzlldP5Fg==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM07oeX4xevdMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA2MTAx
MjU4MThaGA8yMTk1MTExNDEyNTgxOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6v6kGMnRmFDLxBEqXzP4npnL65OO0kmQ7w8YXQygSdmNIoScGSU5wfh9
mZdcvCxCdxgALFsFqPvH8fqiE9ttI0fEfuZvHOs8wUsIdKr0Zz0MjSx3cik4tKET
ch0EKfMnzKOgDBavraCDeX1rUDU0Rg7HFqNAOry3uqDmnqtk00XC9GenS3z/7ebJ
fIBEPAam5oYMVFpX6M6St77WdNE8wEU8SuerQughiMVx9kMB07imeVHBiELbMQ0N
lwSWRL/61fA02keGSTfSp/0m3u+lesf2VwVFhqIJs+JbsEscPxOkIRlzy8mGd/JV
ONb/DQpTedzUKLgXbw7KtO3HTG9iXQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU2CTGYE5fTjx7gQXzdZSGPEWAJY4wgY4GA1UdIwSBhjCBg4AU2CTG
YE5fTjx7gQXzdZSGPEWAJY6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM07oeX4xevdMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANdqkIpVypr2PveqUsAKke1wKCOSuw1UmH9k
xX1/VRoHbrI/UznrXtPQOPMmHA2LKSTedwsJuorUn3cFH6qNs8ixBDrl8pZwfKOY
IBJcTFBbI1xBEFkZoO3wczzo5+8vPQ60RVqAaYb+iCa1HFJpccC3Ovajfa4GRdNb
n6FYnluIcDbmpcQePoVQwX7W3oOYLB1QLN7fE6H1j4TBIsFdO3OuKzmaifQlwLYt
DVxVCNDabpOr6Uozd5ASm4ihPPoEoKo7Ilp0fOT6fZ41U2xWA4+HF/89UoygZSo7
K+cQ90xGxJ+gmlYbLFR5rbJOLfjrgDAb2ogbFy8LzHo2ZtSe60M=
-----END CERTIFICATE-----
```

Stati Uniti occidentali (California settentrionale) - us-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUK2zmY9PUSTR7rc1k2OwPYu4+g7wwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MDI0M1oXDTI5MDQyODE3MDI0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUK2zmY9PU
STR7rc1k2OwPYu4+g7wwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQA1Ng4QmN4n7iPh5CnadSOc0ZfM7by0dBePwZJyGvOHdaw6P6E/vEk76KsC
Q8p+akuzVzVPkU4kBK/TRqLp19wEWoVwhhTaxHjQ1tTRHqXIVlrkw4JrtFbeNM21
GlkSLonuzmNZdivn9WuQYeGe7nUD4w3q9GgiF3CPorJe+UxtbA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJANNPkIpcyEtIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAzMDdaGA8yMTk1MDQwMzA5MDMwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApHQGvHvq3SVCzDrC7575BW7GWLzcj8CLqYcL3YY7JffupZ7OjcftO57Z
4fo5Pj0CaS8DtPzh8+8vdwUSMbiJ6cDd3ooio3MnCq6DwzmsY+pY7CiI3UVG7KcH
```

```
4TriDqr1Iii7nB5MiPJ8wTeAqX89T3SYaf6Vo+4GCb3LCDGvnkZ9TrGcz2CHkJsj
AIGwgopFpwhIjVYm7obmuIxSIUv+oNH0wXgDL029Zd98SnIYQd/njiqkzE+lvXgk
4h4Tu17xZIKBgFcTtWPky+POGu81DYFqiWVEyR2JKKm2/iR1dL1YsT39kbNg47xY
aR129sS4nB5Vw3TRQA2jL0ToTIxzhQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUgepyiONs8j+q67dmcWu+mKKDa+gwgY4GA1UdIwSBhjCBg4AUgepy
iONs8j+q67dmcWu+mKKDa+ihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJANNPkIpcyEtIMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGLFWyutf1u0xcAc+kmnMPqtc/Q6b79VIX0E
tNoKMI2KR8lcV8ZElXDb0NC6v8UeLpe1WBKjaWQtEjL1ifKg9hdY9RJj4RXIDSK7
33qCQ8juF4vep2U5TTBd6hfWxt1Izi88xudjixmbpUU4YKr8UPbmixldYR+BEx0u
B1KJi9l1lxvuc/Igy/xeHOAZEjAXzVvHp8Bne33VVwMiMxWECZCiJxE4I7+Y6fqJ
pLLSFFJKbNaFyXlDiJ3kXyePEZSc1xiWeyRB2ZbTi5eu7vMG4i3AYWuFVLthaBgu
lPfHafJpj/JDcqt2vKUKfur5edQ6j1CGdxqqjawhOTEqcN8m7us=
-----END CERTIFICATE-----
```

Stati Uniti occidentali (Oregon) - us-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDITCCAoqgAwIBAgIUFx8PxCkbHwpD31bOyCtyz3GclbgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MjM1OVoXDTI5MDQyODE3MjM1OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFx8PxCkb
HwpD31bOyCtyz3GclbgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBzOl+9Xy1+UsbUBI95HO9mbbdnuX+aMJXgG9uFZNjgNEbMcvx+h8P9IMko
z7PzFdheQQ1NLjsHH9mSR1SyC4m9ja6BsejH5nLBWyCdjfdP3muZM4O5+r7vUa1O
dWU+hP/T7DUrPAIVMOE7mpYa+WPWJrN6BlRwQkKQ7twm9kDalA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALZL3lrQCSTMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAxMzJaGA8yMTk1MDExNzA5MDEzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA02Y59qtAA0a6uzo7nEQcnJ26OKF+LRPwZfixBH+EbEN/Fx0gYy1jpjCP
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMY9ALA/Ipz0n00Huxj38EBZmX/NdNqKm7C
qWu1q5kmIvYjKGiadfboU8wLwLcHo8ywvfgI6FiGGsEO9VMC56E/hL6Cohko11LW
dizyvRcvg/IidazVkJQCN/4zC9PUOVyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y
tIYxDhR6TIZsSnRjz3bOcEHxt1nsidc65mY0ejQty4hy7ioSiapw316mdbtE+RTN
fcH9FPIFKQNBpiqfAW5Ebp3Lal3/+wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
x8Qnd75qA9XotSWT3IhvJmqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALZL3lrQCSTMMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFZ1e2MnzRaXCaLwEC1pW/f0oRG8nHrlPZ9W
OYZEWbh+QanRgaikBNDtVTwARQcZm3z+HWSkaIx3cyb6vM0DSkZuiwzm1LJ9rDPc
aBm03SEt5v8mcc7sXWvgFjCnUpzosmky6JheCD4O1Cf8k0olZ93FQnTrbg62OK0h
83mGCDeVKU3hLH97FYoUq+3N/IliWFDhvibAYYKFJydZLhIdlCiiB99AM6Sg53rm
oukS3csyUxZyTU2hQfdjyo1nqW9yhvFAKjnnggiwxNKTTPZzstKW8+cnYwiiTwJN
```

```
QpVoZdt0SfbuNnmwRUMi+QbuccXweav29QeQ3ADqjgB0CZdSRKk=
-----END CERTIFICATE-----
```

Africa (Città del Capo) - af-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7DCCAqwCCQCncbCtQbjuyzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA2MDQxMjQ4MDVaFw00
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQC12Nr1gMrHcFSZ7S/A
pQBSCMHWmn2qeoQTMVWqe50fnTd0zGFxDdIjKxUK58/8zjWG5uR4TXRzmZpGpmXB
bSufAR6BGqud2LnT/HIWGJAsnX2uOtSyNfCoJigqwhea5w+CqZ6I7iBDdnB4TtTw
qO6TlnExHFVj8LMkylZgiaE1CQIVAIhdobse4K0QnbAhCL6R2euQzloXAoGAV/21
WUuMz/79Ga0JvQcz1FNy1sT0pU9rU4TenqLQIt5iccn/7EIfNtvVO5TZKulIKq7J
gXZr0x/KIT8zsNweetLOaGehPIYRMPX0vunMMR7hN7qA7W17WZv/76adywIsnDKq
ekfe15jinaX8MsKUdyDK7Y+ifCG4PVhoM4+W2XwDgYQAAoGAIxOKbVgwLxbn6Pi2
6hBOihFv16jKxAQI0hHzXJLV0Vyv9QwnqjJJRfOCy3dB0zicLXiIxeIdYfvqJr+u
hlN8rGxEZYYJjEUKMGvsc0DW85jonXz0bNfcP0aaKH0lKKVjL+OZi5n2kn9wgdo5
F3CVnMl8BUra8A1Tr2yrrE6TVZ4wCQYHKoZIzjgEAwMvADAsAhQfa7MCJZ+/TEY5
AUr0J4wm8VzjoAIUSYZVu2NdRJ/ERPmDfhW5EsjHlCA=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAKumfZiRrNvHMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTExMjcw
NzE0MDVaGA8yMTk5MDUwMjA3MTQwNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFd571nUzVtke3rPyRkYfvs3jh0C0EMzzG72boyUNjnfw1+m0TeFraTLKb9T6F
7TuB/ZEN+vmlYqr2+5Va8U8qLbPF0bRH+FdaKjhgWZdYXxGzQzU3ioy5W5ZM1VyB
7iUsxEAlxsybC3ziPYaHI42UiTkQNahmoroNeqVyHNnBpQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAAJLylWyElEgOpW4B1XPyRVD4pAds8Guw2+krgqkY0HxLCdjosuH
RytGDGN+q75aAoXzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK
s5gbPOnokhKTMPXbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAIFI+O5A6/ZIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy7/WHBBHOrk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
oeVmR9nqnhfij2wOcQdbLandh0EGtbxerete3IoXzd1KXJb11PVmzrzyu5SPBPuP
iCeV4qdjjkXo2YWM6t9YQ911hcG96YSp89TBXFYUh3KLxfqAdTVhuC0NRGhXpyii
j/czo9njofHhqhTr7UEyPun8NVS2QWctLQ86N5zWR3Q0GRoVqqMrJs0cowHTrVw2
9Qr7QBjjBOVbyYmtYxm/DtiKprYV/e6bCAVok015X1sZDd3oCOQNoGlv5XbHJe2o
JFD8GRRy2rkWO/lNwVFDcwec6zC3QwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNImUjrSBOfBJsfFulyg1Zgn2nDCK7kQhx
jMJmNIvXbps3yMqQ2cHUkKcKf5t+WldfeT4Vk1Rz6HSA8sd0kgVcIesIaoy2aaXU
VEB/oQziRGyKdN1d4TGYVZXG44CkrzSDvlbmfiTq5tL+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEe6YyE1Rakl62VncYSXiGe/i2XvsiNH3Qlmnx5XS7W0SCN0oAxW
EH9twibauv82DVg1WOkQu8EwFw8hFde9X0Rkiu0qVcuU8lJgFEvPWMDFU5sGB6ZM
gkEKTzMvlZpPbBhg99Jl
-----END CERTIFICATE-----
```

Asia Pacifico (Hong Kong) - ap-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQCO7MJe5Y3VLjAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDMwMjIxMjFaFw00
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDvQ9RzVvf4MAwGbqfX
blCvCoVb9957OkLGn/04CowHXJ+vTBR7eyIa6AoXltsQXBOmrJswToFKKxT4gbuw
jK7s9QQX4CmTRWcEgO2RXtZSVjOhsUQMh+yf7Ht4OVL97LWnNfGsX2cwjcRWHYgI
7lvnuBNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOCG
eSNmxpW4QFu4pIlAykm6EnTZKKHT87gdXkAkfoC5fAfOxxhnE2HezZHp9Ap2tMV5
8bWNvoPHvoKCQqwfm+OUBlAxC/3vqoVkKL2mG1KgUH9+hrtpMTkwO3RREnKe7I5O
x9qDimJpOihrL4I0dYvy9xUOoz+DzFAW8+ylWVYpA4GFAAKBgQDbnBAKSxWr9QHY
6Dt+EFdGz6lAZLedeBKpaP53Z1DTO34J0C55YbJTwBTFGqPtOLxnUVDlGiD6GbmC
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvkhWVnLJkFJ
```

```
9pdOu/ibRPH1lE2nz6pK7GbOQtLyHTAJBgcqhkjOOAQDAzAAMC0CFQCoJlwGtJQC
cLoM4p/jtVFOj26xbgIUUS4pDKyHaG/eaygLTtFpFJqzWHc=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICSzCCAbQCCQDtQvkVxRvK9TANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1hem9uYXdzLmNvbTAe
Fw0xOTAyMDMwMzAwMDZaFw0yOTAyMDIwMzAwMDZaMGoxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgwFgYDVQQKEw9B
bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1kkHXYTfc7gY5Q55JJhjTieHAgacaQkiR
Pity9QPDE3b+NXDh4UdP1xdIw73JcIIG3sG9RhWiXVCHh6KkuCTqJfPUknIKk8vs
M3RXflUpBe8Pf+P92pxqPMCz1Fr2NehS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY
Rh84dK98VwIDAQABMA0GCSqGSIb3DQEBCwUAA4GBAA6xV9f0HMqXjPHuGILDyaNN
dKcvplNFwDTydVg32MNubAGnecoEBtUPtxBsLoVYXCOb+b5/ZMDubPF9tU/vSXuo
TpYM5Bq57gJzDRaBOntQbX9bgHiUxw6XZWaTS/6xjRJDT5p3S1E0mPI3lP/eJv4o
Ezk5zb3eIf10/sqt4756
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA3MjAw
ODQ0NDRaGA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA4T1PNsOg0FDrGlWePoHeOSmOJTA3HCRy5LSbYD33GFU2eBrOIxoU/+SM
rInKu3GghAMfH7WxPW3etIAZiyTDDU5RLcUq2Qwdr/ZpXAWpYocNc/CEmBFtfbxF
z4uwBIN3/drM0RSbe/wP9EcgmNUGQMMZWeAji8sMtwpOblNWAP9BniUG0Flcz6Dp
uPovwDTLdAYT3TyhzlohKL3f6O48TR5yTaV+3Ran2SGRhyJjfh3FRpP4VC+z5LnT
WPQHN74Kdq35UgrUxNhJraMGCzznolUuoR/tFMwR93401GsM9fVA7SW3jjCGF81z
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDK
2/+C3nPMgtyOFX/I3Cyk+Pui44IgOwCsIdNGwuJysdqp5VIfnjegEu2zIMWJSKGO
lMZoQXjffkVZZ97J7RNDW06oB7kj3WVE8a7U4WEOfnO/CbMUf/x99CckNDwpjgW+
K8V8SzAsQDvYZs2KaE+18GFfLVF1TGUYK2rPSZMHyX+v/TIlc/qUceBycrIQ/kke
jDFsihUMLqgmOV2hXKUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLf1t5SbsGdUA3AUY1
3If8s81uTheiQjwY5t9nM0SY/1Th/tL3+RaEI79VNEVfG1FQ8mgqCK0ar4m0oZJl
tmmEJM7xeURdpBBx36Di
```

```
-----END CERTIFICATE-----
```

Asia Pacifico (Hyderabad) - ap-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXjrQ4+XMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAJCKGBBoxIUxqBk94JHhwZZbgvbP0DAOoHENQWxp/98lI7/
YOfYJOVMJS22aCnHDurofmo5rvNIkgXi7Rztbhu
+lko9rK6DgpmpUwBU0WZtf34aZ2IWNBwHaVhHvWAQf9/46u18dMa2YucK1Wi+Vc+M
+KldrvgXmhym6ErNlzhJyMAkGByqGSM44BAMDLwAwLAIUaaPKxaOHoYvwz709xXpsQueIq+UCFFa/
GpzoDOSokl1057NU/2hnsiW4
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJAPw1mjt5QguhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yNjA1Mjgx
MDQzMjlaFw0zMTA1MjcxMDQzMjlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
08B7tDQ/rBXKG6473AGJtDzUQ/H+EdYwM76C7dvqhnjkwMjtR7bY+nJrGDdwD9YT
eYmLqaRYmLJdnjT2vwg9FYNAQHwxZVea846QNI+0yWm1YeJI+yb7Q/sWDIusBEAO
MekjzjWODnmdvvKPx0vJ7nKVg1XT0TunIllJTIY5g5sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFM4QY6Q5jpIb3pUP7EBEDUVlvGgsMIGOBgNVHSME
gYYwgYOAFM4QY6Q5jpIb3pUP7EBEDUVlvGgsoWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQD8NZo7eUILoTASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAGPVdLHdjH2PVcfoK41bRQCp
vzwwOB0XpQ1AqQBYZXmm6+Ggc3nQLoOKLG1oRlc38psWtxBjGRL+ktvyAjgwk+BL
xM7Yx+wDf8m2nfrvIdaMHk0i+U7bWaiFod3cD6XICfwg/tFz50auWTtlIPcNOXAU
qPuHbYlFgMUlNuNp78nB
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAIVWfPw/X82fMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MDQx
NDMwMjhaGA8yMjAxMTIwODE0MzAyOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAg29QEFriG+qFEjYW/v62nN70lMJY/Hevx5TtmU/VIYBPQa3HUGTBAbbI
2Tmy8UMpa8kZeaYeI3RAfiQWt0Ws7wUrBuO2Pdp518WDPaJUH7RWEuu1BDDkyZRW
NAMNPCn3ph7Od243IFcLGku7HVekel5poqRpSfojrMasjlf+CvixUeAJbmFoxUHK
kh5unzG2sZyO4wHXcJPQkRf5a8zSTPe9YZP1kXPPEv4p/jTSggaYPxXyS6QVaTlV
zLeLFZ0fesLPMeil3KYQtV7IKLQiEA2F6dxWnxNWQlyMHtdq6PucfEmVx17i/Xza
yNBRo0azY8WUNVkEXrRhp/pU8Nh3GQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU9AO1aZk9RLXk2ZvRVoUxYvQy9uwwgY4GA1UdIwSBhjCBg4AU9AO1
aZk9RLXk2ZvRVoUxYvQy9uyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAIVWfPw/X82fMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADexluMRQRftqViahCnauEWGdMvLCBr8A+Yr
6hJq0guoxEk/lahxR137DnfMPuSbi1Rx5QKo7oBrWfG/zsgQUnF2IwHTzwD+i/2m
XCane6FiS5RpK3lGdILq8ZmlhQk+6iI8yoZLr0LCfTh+CLgIKHOknfR5lFzgzAiF
SI8/Q9mm+uvYtSTZECI6Zh57QZPoETAG/yl+9jiOy2lAelqa/k1i+Qo8gMfOc+Pm
dwY7o6fV+oucgRlsdey6VM45LeyILQqv0RXtVzjuowanzmCCFMjgqiO9oZAWu4Oh
+F3unijELo01vZJs8s2N3KGlo3/jtUFTX6RTKShZlAPLwBi5GMI=
-----END CERTIFICATE-----
```

Asia Pacifico (Giacarta) - ap-southeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXbVDEikMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAPjuiEx05N3JQ6cVwntJie67D8OuNo4jGRn
+crEtL7YO0jSVB9zGE1ga
+UgRPIaYETL293S8rTJTVgXAqdpBwfaHC6NUzre8U8iJ8FMNnlP9Gw1oUIlgQBjORyynVJexoB31TDZM
```

```
+/52g9O/bpq1QqNyKbeIgyBBlc1dAtr1QLnsMAkGByqGSM44BAMDLwAwLAIUK8E6RDIRtwK+9qnaTOBhvO/
njuQCFFocyT1OxK+UDR888oNsdgtif2Sf
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUMDbUg+reaqO28n34vFUuk6gFWbgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI2MDQyMjEyMDY0MFoXDTMxMDQyMTEyMDY0MFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCnCS/Vbt0gQ1ebWcur2hSO7PnJifE4OPxQ7RgSAlc4/spJp1sD
P+ZrS0LO1ZJfKhXf1R9S3AUwLnsc7b+IuVXdY5LK9RKqu64nyXP5dx170zoL8loE
yCSuRR2fs+04i2QsWBVP+KFNAn7P5L1EHRjkgTO8kjNKviwRV+OkP9ab5wIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUsnsEPOUYPQO0Gv9t4arIC2NN
kHQwgZkGA1UdIwSBkTCBjoAUsnsEPOUYPQO0Gv9t4arIC2NNkHShYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUMDbUg+re
aqO28n34vFUuk6gFWbgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCFibNMMdZF13osIpWxjb7uXrqpDYFat+196JVSdq+WMYLfcQtudZOcTclo
Zh+OXR49nRv9x/Q4XRfMWGCdptp4q/6NCScEUPBbY2+7CJyH0gyC6vYcGmLfJbUi
kMB27EWJ4tm18a/qZockIeGgJgqt5/KSZb5iN5CuxRHRDGZI+Q==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMtdyRcH51j9MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MDgx
MjM5MTZaGA8yMjAxMDkxMjEyMzkxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvUsKCxoH6KXRYJLeYTWAQfaBQeCwhJaR56mfUeFHJE4g8aFjWkiN4uc1
TvOyYNnIZKTHWmzmulmdinWNbwP0GiROHb/i7ro0Hhvnptyycgt8ag8affiIbx5X
7ohdwSN2KJ6G0IKflIx7f2NEI0oAMM/9k+T1eVF+MVWzpZoiDp8frLNkqp8+RAgz
ScZsbRfwv3u/if5xJAvdg2nCkIWDMSHEVPoz0lJo7v0ZuDtWWsL1LHnL5ozvsKEk
+ZJyEi23r+U1hIT1NTBdp4yoigNQexedtwCSr7q36oOdDwvZpqYlkLi3uxZ4ta+a
01pzOSTwMLgQZSbKWQrpMvsIAPrxoQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU1GgnGdNpbnL3lLF30Jomg7Ji9hYwgY4GA1UdIwSBhjCBg4AU1Ggn
GdNpbnL3lLF30Jomg7Ji9hahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
```

```
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMtdyRcH51j9MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACVl00qQlatBKVeiWMrhpczsJroxDxlZTOba
6wTMZk7c3akb6XMOSZFbGaifkebPZqTHEhDlrClM2j9AIlYcCx6YCrTf4cuhn2mD
gcJN33143eOWSaeRY3ee4j+V9ne98y3kO2wLz95VrRgclPFR8po2iWGzGhwUi+FG
q8dXeCH3N0DZgQsSgQWwmdNQXZZej6RHLU/8In5trHKLY0ppnLBjn/UZQbeTyW5q
RJB3GaveXjfgFUWj2qOcDuRGaikdS+dYaLsi5z9cA3FolHzWxx9MOs8io8vKqQzV
XUrLTNWwuhZy88cOlqGPxnoRbw7TmifwPw/cunNrsjUUOgs6ZTk=
-----END CERTIFICATE-----
```

Asia Pacifico (Malesia) – ap-southeast-5

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQC5X6U+vgoLEDAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMxMjU3NTRaGA8y
MDUwMDEwMzEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBAIzEMPCIPFfOYCg4
BCjKGyl60wOfmwHPzSOXZ3Z2wS/LYNHUtHGwtVNePSTyCu/CuZF6gC9n/wBORtQp
+SSkn+weGc/BmUA1mp/vrN7v+aSCgKJoO+sgpa1PPOgNvUaMw6O5odsZWQCMSjkU
6RTo/PL2v/tMfiCocF4ghvyRC6hvAhUA0VoObKC2IXzXgVvRRupo4qHbcm8CgYAe
bbNuawh3rAxkFvUs9FPzW5E+xllG16Z//61PENKqonmk+zBiBdiIlS1F6ZqmTqkI
z5+qfSt1m3pb3j2W0NT7lEDFvy8Gr6Y2vohCHmL+T1u1Yy4PeqbgrFwcen7y7WoO
/KCV7Y9/ODQMMyuAzT3h5wJNweT7L5MUN8JYpZSi3QOBhAACgYBqaDuG2u6V91Qj
K2wEAElxaaRaNo/ewg/wWDmHYqoeHOR0HfuFCYgASE9f7ULqYtX1VURcgcjw9XN4
BDmPilXvfi04INPTnw4IxFJKDzzC0kVH7esVas982Po8v3megH32H9Rl87r7UG1c
ZEbkSkKVX6YKYg1PR3rfjXgdwVZv/zAJBgcqhkjOOAQDAzAAMC0CFFWeRe2fYW2i
6mMd26Wzbx87Y0DXAhUAoPCnF+5hGJw0jT9aL7QsgcfLi9Y=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAMuBl6rhZCJKMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMx
MjU3NTRaGA8yMjAzMDYwOTEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
```

```
gQDFuKydxZsordNH7bLwIluEGOkX7/CdLdpeqkDKEhQkFwzpRxaX4EAlkGh2/o7D
8qneC9cGQhqSG5WVVBrmZG7sfkFOM4m1AtY++kfv+MYto1VFgLk1xJbkpq1r4YeQ
Ul+ZsJYsZpyX/t+g8s7rW0OVcBsYx4L75bf34z38mwK8PQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBADD9C4pWL8RUvF1CJW8kExj35xmozlFlmrKs8Zpi8+Eg6q+W9dgd
xMdH95tgZtmVMDqlvVR+DK0iO1BNpqPjrqWkk2tTLivpS+sGzCE/jCl18Q28Rk71
/A3gLD7Rtbq5TKNvuFCHwYMjrTDHI6aBjIaAlDm4e2/j/OxVtHyZGTre
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANC3xtbPhQ2GMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMx
MjU3NTRaGA8yMjAzMDYwOTEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAt3aMy7Hsp4ySG3mlfi+pdTcZw6H6XNU1Y36fNdi4c+MzinQQbnqMPyt7
QLgU+XCWmcWsVo7GQF6n9N01Rh+UXXUZU4jcXlFocQPCWf9O+IIIPXkd67kFMUV
HAxCELjfxHbC+I8e7dwOJhmdF4Bfi52Ty8zz0HdE8JDypPkTDlXuGvTgDyW7NP56
I/vlQaXLoYSbcQe5pv2a9gyBaaCM1QoeqwAHAeCNXb9Nuj9ZX3GHGJb3TuqAeKCD
5i9TscCB9XjY6Fx+zfSAobjBZwgLEtLOwJhbZnKmx4gJMaaNFipAjVT2FSS3+yev
eTYBoa1dvhk0ivQyQIPpHmihrmkWuwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBC
fdgyI8GjmCqiHAlh+L1bj0LdNql9zl7RXmOEzsuRdtdMumkxYXX88UtROy3fdi1i
VaEwHdAK8ThzRkesgHza/cXzqCMewaYxujSI6p6G7x99FFeGif1x0FJdj8AoeTL7
4h9bmS/6l4/NL7DJI9G7ovES/hoUA9v9TDhv+vauxXlgfrp0MPecprxBYlrc+DH2
adGCdKCp2lQ2YDKOD9TCEjYIli8XSoyevoWHUjfDYrCrCp8l4s/p7HOgYr8fJBAs
EuVy8211LVz1/X4EMBRNtNjXK9sklsxAOX14NDfBFSS0toxl3K6Tf9t/PviBl95d
hncyDAcFgDCK4w8LLlVW
-----END CERTIFICATE-----
```

Asia Pacifico (Melbourne) - ap-southeast-4

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjWF7P2MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
```

```
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAPRXSsQP9E3dw8QXKlrgBgEVCprLHdK/bbrMas0XMu1EhOD
+q
+0PcTr8+iwbtoXlY5MCeatWIp1GrXQjVqsF8vQqxlEuRuYKbR3nq4mWwaeGlx9AG5EjQHRa3GQ44wWHOdof0M3NRI1MP
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUUOsUa3Aj7pphfmDjsZAFNWODCUowDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI2MDYwMzEwNDM1M1oXDTMxMDYwMjEwNDM1M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDHezwQr2VQpQSTW5TXNefiQrP+qWTGAbGsPeMX4hBMjAJUKys2
NIRcRZaLM/BCew2FIPVjNtlaj6Gwn9ipU4Mlz3zIwAMWi1AvGMSreppt+wV6MRtf
Ojh0Dvj/veJe88aEZJMozNgkJFRS+WFWsckQeL56tf6kY6QTlNo8V/0CsQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUVCy+PqHsYEzvAHcGK+lrlknS
UvowgZkGA1UdIwSBkTCBjoAUVCy+PqHsYEzvAHcGK+lrlknSUvqhYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUUOsUa3Aj
7pphfmDjsZAFNWODCUowEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBRI72kM+Q6PCU584L6UZ8rk6uERCeq5g8dDzlLZMaMpV4n/s2MJbFP2hO+
ovahJnxLTrs7jP3VXZeVj5Eb0dfYneg0+zNtycnHe+9jH+GTKS8+QkwGj3zmwxqG
mZ9V6XoGwtO/aEz24Yp7CRf8etCYEnVI2ChD7xClRV3DJwliEA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAN4GTQ64zVs8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTMx
MzMzMDBaGA8yMjAxMTIxNzEzMzMwMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA2BYgeCr+Rk/jIAEDOHS7wJql62vc83QEwjuzk0qOFEReIZzlN1fBRNXK
g0T178Kd3gLYcE59wEFbTe/X5yOA1Lo95x1anSAo7R+Cisf9C2HQuJp+gVb+zx71
lniPF7gHziGpm0M8DdAU/IW+wkZwGbP4z7Hq9+bJ0P2ltvPJ5yxSgkFuDsI9VBHa
CLoprHsCHh2VdP8KcMgQQMmHe1NmBpyTk0ul/aLmQkCQEX6ZIRGOeq228fwlh/t+
Ho+jv87duihVKic6MrL32SlD+maX0LSDUydWdaOLLTGkh7oV7+bFuH6msrXUu+Ur
```

```
ZEP1r/MidCWMhfgrFzeTBzOHA97qxQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUcHMd1cHqzmsQ5hpUK3EMLhHdsi4wgY4GA1UdIwSBhjCBg4AUcHMd
1cHqzmsQ5hpUK3EMLhHdsi6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAN4GTQ64zVs8MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAI4PFyVN+7EGSObioiPnv0LL0f70SSzUZJ8p
XO90d4rWea7jIbgZ2AKb+ErynkU9xVg7XQQ5k6KDWgp/4jYFL2dqnt/YAY4PS0un
RSrYElawxLT0BcLn4rcSDC79vQe1xGC5//wDdV6b399COAHRAK6axWYy5w32u9PL
uw0cIp3Ch8JoNwcgTHKRRGzePmBeR4PNqhHTArG4/dJk6/aUO4OpX0WzI6L67CGY
6Nex3dau+gkLCK93dTEkrXtyXHu4wB0J9zd1w+iQ0SEa9eKc78/NjEsF/FZdGrWC
t57lIMOOXJhQ1kRgSwNeZdQWV1dRakvO6sfcvVYkfj1wAvZvvAw=
-----END CERTIFICATE-----
```

Asia Pacifico (Mumbai) - ap-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUDLA+x6tTAP3LRTr0z6nOxfsozdMwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
```

```
MB4XDTI0MDQyOTE0MTMwMVoXDTI5MDQyODE0MTMwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUDLA+x6tT
AP3LRTr0z6nOxfsozdMwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAZ7rYKoAwwiiH1M5GJbrT/BEk3OO2VrEPw8ZxgpqQ/EKlzMlOs/0Cyrmp7
UYyUgYFQe5nq37Z94rOUSeMgv/WRxaMwrLlLqD78cuF9DSkXaZIX/kECtVaUnjk8
BZx0QhoIHOpQocJUSlm/dLeMuE0+0A3HNR6JVktGsUdv9ulmKw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPRYyD8TtmC0MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjAzMDcx
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA0LSS5I/eCT2PM0+qusorBx67QL26BIWQHd/yF6ARtHBb/1DdFLRqE5Dj
07Xw7eENC+T79mOxOAbeWg91KaODOzw6i9I/2/HpK0+NDEdD6sPKDA1d45jRra+v
CqAjI+nV9Vw91wv7HjMk3RcjWGziM8/hw+3YNIutt7aQzZRwIWlBpcqx3/AFd8Eu
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+Z
w9RVHm24BGhlLxLHLmsOIxvbrF277uX9Dxu1HfKfu5D2kimTY7xSZDNLR2dt+kNY
/+iWdIeEFpPT0PLSILt52wP6stF+3QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBI
E6w+WWC2gCfoJO6c9HMyGLMFEpqZmz1n5IcQt1h9iyO7Vkm1wkJiZsMhXpk73zXf
TPxuXEacTX3SOEa07OIMCFwkusO5f6leOyFTynHCzBgZ3U0UkRVZA3WcpbNB6Dwy
h7ysVlqyT9WZd7EOYm5j5oue2G2xdei+6etgn5UjyWm6liZGrcOF6WPTdmzqa6WG
ApEqanpkQd/HM+hUYex/ZS6zEhd4CCDLgYkIjlrFbFb3pJ1OVLztIfSN5J4Oolpu
JVCfIq5u1NkpzL7ys/Ub8eYipbzI6P+yxXiUSuF0v9b98ymczMYjrSQXIf1e8In3
OP2CclCHoZ8XDQcvvKAh
-----END CERTIFICATE-----
```

Asia Pacifico (Nuova Zelanda): ap-southeast-6

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQCcP+D4eLFOajAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEyMDMxMjEzMDZaGA8y
MDUwMTIwNDEyMTMwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBANBMmM/LbAX13IeB
3yr2pMMpiTW1b1go/axNLfcxEmj0fThKk8y0FAT1frN/UPdI9qRInsyBdEZQLiIH
4WHCXk8IidQLh4DED3G9DvSFFC4Gb8ax+UIQY11wfHPWO4+wA9q8liYTg/FxdJMM
tZS9tZAZxjH6+8yfV8Bt0wUd2Y+lAhUAwg0CxCmZPinHtKbFnpMQfKnzjCMCgYAf
i+D7nGVFOWJ8EYOpRYbG0pHkrpwNy+h01csn6IAwQbIfeOG+SF4N3LeuOAC9vXGY
VGh9XNxuasvqkRAzgRmJ/EYM5Xa/YN62EhddRuN8wCOg66MeczUDh3RTb+Tu6HK0
UR6oTSOQ6rxA5aA1qTc7TqI0+pRZv+QYIZK/ozsZzgOBhAACgYAbVm+rOX8J38cG
LxKjUXVM0KB69SksGLEqjO4ps80EcZ/0W3g1hGLnSX/RjYfAS60hbKK1GX9PpcaO
4mDzCTm3dZ6shbae5t8bBU+mUi8BmaK+Pdu3z5J77y4zv22/yXte8ulZ5J0zKP9K
QP3p3pa7XI9NaXpKGT3yZsJ0BWY2xTAJBgcqhkjOOAQDAzAAMC0CFBs4KQmrxHjQ
OHh0r8JqB8UiwlutAhUAwgxid7wT6FNm8Zwq9hioQ2v2K0A=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAMwLuv2/tk9eMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEyMDMx
MjEzMDZaGA8yMjA0MDUwOTEyMTMwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQC9AsBNOUfT8QpguHqMa9KIXP/YgZOmfRAgEmnLawXTC+40bXUq/fwkx+cebv3x
CvUx6d07/iDlD0dm2Hf2HhPFi3OaCI7vc8c3lqVBvcn6yzmwv35aSEvtVm2NHC3j
4/q6vN2tR2d4a1Mf1QhmOVOJ7XiTEbCy2Yv+pmDbk29V6QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAHatyQIy612kio8neI4r5VBg8pgKwW+mFGpAzOQ2NOyLCNoOeD1D
lPRaSipBN7WW6jpIozbz7JG7Kqc3N+piPGGzfjH9gZjqUqfOGrNHB5nsxvMHI2iL
e+DwsOcV7qnEVRgYbmLYOVKJv25wCsM/Tcn/6f6scEX2x+H0hAh7rwiP
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
```

```
MIIDOzCCAiOgAwIBAgIJAI/xUfWwSQOtMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEyMDMx
MjEzMDZaGA8yMjA0MDUwOTEyMTMwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArbid9Tnunu0pWCQUqZCkGeiF8hWixi+LBS1AOew2UsT9keAt2rXXGlU/
wSMriKHsvcrfKtuVKj5chArsOyFvagszH5lIKhI+GfWVQEd2aZiOvAJ+iRUQq1+R
gOr2gyjWlf3znZXTcyhHcJoXDhbn5e+kEa3pwS4yKNRpM3P61V4M2702xis08hjP
qMDxwXMa1Fiy4b7nAyNQifgrwb3bCA5k5prmkl/iajaWa1zMMFgLI9vA6UwUSbTK
H9iOuL/xNfMX+Xzq4CCaQYiJ8zdi56kqnB/lrA05NSjOPLskg6sUGkyiDxGK4gzC
DFrO6oygcdlBaxnyAECGdJcOM6TOmwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBg
8yVPNpctrvSvTazf/Ij8qC6+q6df1SptdYKQkOYWeUVZR7+3uTZ9Yiyq+Bh8Hbyf
NcR0eR6UqhgiB3p5slYNhTvLkpuMuqTpVJFvQtzZycnmKXAQ35G5zCYV0+pkF59L
ch26SukWk0+VP3kIM9VmaIZQKJEBlBLcnbDZyXlHUDnZAYPcxxKQ8uFPkW0GOFMr
ekFCGOUmFSItFXOHy5hD2xmctKNk3l12m6cKydYvONtk/3DovKNnw3c5k40WHQW/
Zdh/LWd4/Jrkan+kQnqm4rkrXF+x3aF0qrKTtHMICvpkZ8g7/588hBs4mZnCmFLa
q/g9WqIcd9SMmBkT6KZ8
-----END CERTIFICATE-----
```

Asia Pacifico (Osaka-Locale) - ap-northeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUHTRhxHhBZFOGvTFKxHoy9+f5Hl8wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NTQwN1oXDTI5MDQyODE2NTQwN1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUHTRhxHhB
ZFOGvTFKxHoy9+f5Hl8wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAUZx7DcYbhWNTD4BNGhr5beruT2OUoGHH9J73UKxwdqeb9bH1LIWhIZO0X
/1mjn3bWBgCwfoS8gjZwsVB6fZbNBRy8urdBZJ87xF/4JPBjt7S9oGx/zthDUYrC
yK0Y0v4G0PgiS81CvYLg09LpmYhLSJbXENlkC04v5yxdKxZxyg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMn1yPk22ditMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA3MTkx
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArznEYef8IjhrJoazI0QGZkmlmHm/4rEbyQbMNifxjsDE8YWtHNwaM91z
zmyK6Sk/tKlWxcnl3g31iq305ziyFPEewe5Qbwf1iz2cMsvfNBcTh/E6u+mBPH3J
gvGanqUJt6c4IbipdEouIjjnynyVWd4D6erLl/ENijeR1OxVpaqSW5SBK7jms49E
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmklcqTfMfPCkzmJCRgp
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijeDn7kTsQzgO07Z2SAE63PIO48JK8HcObH
tXORUQ/XF1jzi/SIaUJZT7kq3kWl8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBj
ThtO9dLvU2QmKuXAhxXjsIdlQgGG3ZGh/Vke4If1ymgLx95v2Vj9Moxk+gJuUSRL
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gI8kqkG7V8iRyPIFekv+M
pcai1+cIv5IV5qAz8QOMGYfGdYkcoBjsgiyvMJu/2N2UbZJNGWvcEGkdjGJUYYOO
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiIUgEaW3UFEbThJT+z8UfHG9fQjzzfN/J
nT6vuY/0RRu1xAZPyh2gr5okN/s6rnmh2zmBHU1n8cbCc64MVfXe2g3EZ9Glq/9n
izPrI09hMypJDP04ugQc
```

```
-----END CERTIFICATE-----
```

Asia Pacifico (Seoul) - ap-northeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUbBSn2UIO6vYk4iNWV0RPxJJtHlgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEzMzg0NloXDTI5MDQyODEzMzg0NlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUbBSn2UIO
6vYk4iNWV0RPxJJtHlgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
```

```
AAOBgQAmjTjalG8MGLqWTC2uYqEM8nzI3px1eo0ArvFRsyqQ3fgmWcQpxExqUqRy
l3+2134Kv8dFab04Gut5wlfRtc2OwPKKicmv/IXGN+9bKFnQFjTqif08NIzrDZch
aFT/uvxrIiM+oN2YsHq66GUhO2+xVRXDXVxM/VObFgPERbJpyA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANuCgCcHtOJhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTQx
NTU3NDRaGA8yMTk1MDIxNzE1NTc0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA66iNv6pJPmGM20W8HbVYJSlKcAg2vUGx8xeAbzZIQdpGfkabVcUHGB6m
Gy59VXDMDlrJckDDk6dxUOhmcX9z785TtVZURq1fua9QosdbTzX4kAgHGdp4xQEs
mO6QZqg5qKjBP6xr3+PshfQ1rB8Bmwg0gXEm22CC7o77+7N7Mu2sWzWbiUR7vil4
9FjWS8XmMNwFTlShp4l1TDTevDWW/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa
LHaVCH/Yy52rsz0hM/FlghnSnK105ZKj+b+KIp3adBL8OMCjgc/Pxi0+j3HQLdYE
32+FaXWU84D2iP2gDT28evnstzuYTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC1
mA4q+12pxy7By6g3nBk1s34PmWikNRJBwOqhF8ucGRv8aiNhRRye9lokcXomwo8r
KHbbqvtK85l0xUZp/Cx4sm4aTgcMvfJP29jGLclDzeqADIvkWEJ4+xncxSYVlS9x
+78TvF/+8h9U2LnSl64PXaKdxHy2IsHIVRN4GtoaP2Xhpa1S0M328Jykq/571nfN
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy8lkiOsvU9XzUaZ0fZSfXX
wXxZamQbONvFcxVHY/0PSiM8nQoUmkkBQuKleDwRWvkoJKYKyr3jvXK7HIWtMrO4
jmXe0aMy3thyK6g5sJVg
-----END CERTIFICATE-----
```

Asia Pacifico (Singapore) - ap-southeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
```

```
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUSqP6ih+++5KF07NXngrWf26mhSUwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MzAxNFoXDTI5MDQyODE0MzAxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUSqP6ih++
+5KF07NXngrWf26mhSUwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAw13BxW11U/JL58j//Fmk7qqtrZTqXmaz1qm2WlIpJpW750MOcP4ux1uPy
eM0RdVZ4jHSMv5gtLAv/PjExBfw9n6vNCk+5GZG4Xec5DoapBZHXmfMo93sjxBFP
4x9rWn0GuwAVO9ukjYPevq2RerilrqSVvppHtbATVNY2qecXDA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAJVMGw5SHkcvMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
ODU3MTlaGA8yMTk1MDQwMzA4NTcxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAlaSSLfBl7OgmikjLReHuNhVuvM20dCsVzptUyRbut+KmIEEc24wd/xVy
2RMIrydGedkW4tUjkUyOyfET5OAyT43jTzDPHZTkRSVkYjBdcYbe9o/0Q4P7IVS3
XlvwrUu0qo9nSID0mxMnOoF1l8KAqnn10tQ0W+lNSTkasW7QVzcb+3okPEVhPAOq
```

```
MnlY3vkMQGI8zX4iOKbEcSVIzf6wuIffXMGHVC/JjwihJ2USQ8fq6oy686g54P4w
ROg415kLYcodjqThmGJPNUpAZ7MOc5Z4pymFuCHgNAZNvjhZDA842Ojecqm62zcm
Tzh/pNMNeGCRYq2EQX0aQtYOIj7bOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAJVMGw5SHkcvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAF/0dWqkIEZKg5rca8o0P0VS+tolJJE/FRZO
atHOeaQbWzyac6NEwjYeeV2kY63skJ+QPuYbSuIBLM8p/uTRIvYM4LZYImLGUvoO
IdtJ8mAzq8CZ3ipdMs1hRqF5GRp8lg4w2QpX+PfhnW47iIOBiqSAUkIr3Y3BDaDn
EjeXF6qS4iPIvBaQQ0cvdddNh/pE33/ceghbkZNTYkrwMyBkQlRTTVKXFN7pCRUV
+L9FuQ9y8mP0BYZa5e1sdkwebydU+eqVzsil98ntkhpjvRkaJ5+Drs8TjGaJWlRw
5WuOr8unKj7YxdL1bv7//RtVYVVi296ldoRUYv4SCvJF11z0OdQ=
-----END CERTIFICATE-----
```

Asia Pacifico (Sydney) - ap-southeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFxWyAdk4oiXIOC9PxcgjYYh71mwwDQYJKoZIhvcNAQEL
```

```
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MjE0M1oXDTI5MDQyODE1MjE0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFxWyAdk4
oiXIOC9PxcgjYYh71mwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQByjeQe6lr7fiIhoGdjBXYzDfkX0lGGvMIhRh57G1bbceQfaYdZd7Ptc0jl
bpycKGaTvhUdkpMOiV2Hi9dOOYawkdhyJDstmDNKu6P9+b6Kak8He5z3NU1tUR2Y
uTwcz7Ye8Nldx//ws3raErfTI7D6s9m63OX8cAJ/f8bNgikwpw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL2bOgb+dq9rMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAwNTdaGA8yMTk1MDQwMzA5MDA1N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAmRcyLWraysQS8yDC1b5Abs3TUaJabjqWu7d5gHik5Icd6dKl8EYpQSeS
vz6pLhkgO4xBbCRGlgE8LS/OijcZ5HwdrxBiKbicR1YvIPaIyEQQvF5sX6UWkGYw
Ma5IRGj4YbRmJkBybw+AAV9Icb5LJNOMWPi34OWM+2tMh+8L234v/JA6ogpdPuDr
sM6YFHMZ0NWo58MQ0FnEj2D7H58Ti//vFPl0TaaPWaAIRF85zBiJtKcFJ6vPidqK
f2/SDuAvZmyHC8ZBHg1moX9bR5FsU3QazfbW+c+JzAQWHj2AaQrGSCITxCMlS9sJ
l51DeoZBjnx8cnRe+HCaC4YoRBiqIQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU/wHIo+r5U31VIsPoWoRVsNXGxowwgY4GA1UdIwSBhjCBg4AU/wHI
o+r5U31VIsPoWoRVsNXGxoyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL2bOgb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACobLvj8IxlQyORTz/9q7/VJL509/p4HAeve
92riHp6+Moi0/dSEYPeFTgdWB9W3YCNc34Ss9TJq2D7t/zLGGlbI4wYXU6VJjL0S
hCjWeIyBXUZOZKFCb0DSJeUElsTRSXSFuVrZ9EAwjLvHni3BaC9Ve34iP71ifr75
8Tpk6PEj0+JwiijFH8E4GhcV5chB0/iooU6ioQqJrMwFYnwo1cVZJD5v6D0mu9bS
TMIJLJKv4QQQqPsNdjiB7G9bfkB6trP8fUVYLHLsVlIy5lGx+tgwFEYkG1N8IOO/
2LCawwaWm8FYAFd3IZl04RImNs/IMG7VmH1bf4swHOBHgCN1uYo=
```

```
-----END CERTIFICATE-----
```

Asia Pacifico (Taipei): ap-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQDrb+HArMxssTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA1MjQxNDU2MDZaGA8y
MDUwMDUyNTE0NTYwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBAPFb5R5TBUs2N0YW
aJcOjxr4UCDrpVT3x6EeqoGFNAc1yiZw9iv++ff6wsXm0VG5XV1QkWMQcjPfK/2I
TvXh9XEOhsG7vaBHoWkb2gmIxE6C2u8TfoZu0ZmiMceFK7aYz5w/q2J9CmRs38dT
I9qgTq0LYX+VkiNYOQnn7sQXQ8CjAhUAp2Lue9SfYTmubbpH+3j91Sivc+cCgYAi
DiyGU5R5VgiNV3mhuAyiHCft3LEmTIxos/hx/rHzgm+vCMH55tYejIrv9n7YGrIZ
MejOt8bGYxqSf0Ir/aoj3ZfHihxUzwyfyzwH7D8kAodXJNsPUTKi0O0pGl/e+nVD
JhTIFV3AwC8Tt0r2hljbjhOiyhdYy5hxWHa/WokLAQOBhAACgYAkGGHXbFr/JXol
itpS1qfiETWSRkXGHrdSmUkRumgti2y7c57TgXPwCyNlP1sTr1duy/kYDpwSwyqi
qEYfko0b/xWpDEQQPsWBgolpEYP7RIT85IxrTCrC9ohz85n7v6m9oF6BiBQGtZdk
GBN7iqemg85UaF6mXfHvl3tUYjsB2jAJBgcqhkjOOAQDAy8AMCwCFED9Ybn6fEVF
wLNjDvULmki5bPBWAhR64pxsHFRHz0ZQi+SYMWdIpEs5RQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAJp99iy2CTXhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA1MjQx
NDU2MDZaGA8yMjAzMTAyOTE0NTYwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDVdclgpcIIsyGG51ag8srK1UMfZ+Ioh9E4PLP+cIWQcdh31fv2kV/whKaqfmif
NefBIuHrTPl6L+mJQbsfeA+TiEx1Jamg4lwQfhgQKQCmjZVMaHtK+AY57TVN6FBf
HXxT2MXzktsKxAQRGeSTFQYrHRzSYvu+GkA+37lqyWRfcwIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBABM+WL9MSb7z3bNOTMkM7ufPucvj+LQ+zEAJiuG0rcB8GI2DhGB5
8ohDPUGlq1cP7vYmDkWG/FrLqx7qgIzkbE3zfb62JpdOuX73oHgCmikMfq8ifoS1
CUxMQ36PDZBFNPzGZxv5kEORqhmGBkYCoIUCQ43jh3aALR/A/rfzfij8
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJt5hgMuWbpMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA1MjQx
NDU2MDZaGA8yMjAzMTAyOTE0NTYwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA91FXs9Wk9kMI3lkNhjC69C6RTBpSvdLWSohPDlJKXFoaGYIDtyW1ViwO
FORAKz0koarVBx1D4fNKCxf+mhYAf//4Pxt31GzjehHNs2YVGimwhq/SNr+3AuIO
PibA+qScXamaiknE1Pxb4jisbBu2PMAG9OxU2dESNwiqBMvdJvg30YNTUITZ6r0e
MPjR1Y/EFVx/SLHW6wdvwqhNi9hz8HHdThzjCbCQPvmoLBJIKXIfosKqvauSezt1
KJSoS2jMx1OjJB2bBlQTZC8vF0WFNPoiH4jXyJ6+wMUMNSSd5b3uL5stVTMzuIz4
39Hd5YW41rmAy+6jmpGp2eXn6Td0rQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAs
gcgv+Xr67Cj08jKdAUT4GuCoGxveOFAjSDjs5y0cD+kXIT/Yj/+HKFOx5cwThT8F
TxNQ/oVuo3bGeuFEX799H0rT9Jupy0WiE1Vx81mk2M/1EDtns437edM4ofiWR8tR
Q1VNiRgz6Crr0nFgNoQa9HmR6/M+bImxevHJkWB3skvnxtA+lpKGwJs8jo6fA7AW
jr00opK0r731iBd1z/5hjIjkHn5NizAdiJEh3lVY/A3WS82aygW8LvYnKZeaBfZJ
J4NgxeflxocLFKBJD+hyf5u1hhvl7Mn/aGr5VI8/0F2oUqYo+xsHLT3keNghywO4
NNcyLcD9u16HVXhRhGvo
-----END CERTIFICATE-----
```

Asia Pacifico (Thailandia): ap-southeast-7

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8TCCAq8CCQCOEEMWiJIJpTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA0MTIxNTI4NTZaGA8y
MDUwMDQxMzE1Mjg1NlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtzCCASsGByqGSM44BAEwggEeAoGBAJWKfrIlz9+/U4wm
NDJPX00avUTdksBKX5RwHkY4o0///2G2HWwiBbxw8F1U+RzCXr80gSoe4+/SCSg3
uDuhJyzN5r4jr7c590CAgsiGdWERs7l4gLQCP504feU4TEjJoq9A8MfRZeqMj7Ug
fT5InTUW7S1/r98ddG/rBHMsJwEbAhUAneIckZ1YeyGcCeL32lujMhj+g68CgYA+
RsyTXCy3Tug5aHun51IfcG2d+pn5K/tv/N3WUR18RplVctrLhwIOUoAsDWPWtxNV
sODetezAyo759CK43JAmYGzXKbRFUHm3n46jP88tSdhuSeJhc/D4l5/0+2L7ndXp
L3+W4N05NdiKSGI8e8t452wTZv/RODivPZ3RtuCDywOBhQACgYEAjVS1Huwzdn1J
+kpd2Rcbe1BAGkmvk5sUu0KhyttqIB1kxTxeWZgsdO8REZSC5gJOwkcGFvXnb3DY
+Ms45r0e0s0rx2FFYjqMLwyRpK9wUjJfSXeJMa9iLQEXuyzBz6zPgfemXbS3zNq/
```

```
eoJ9ztIwjB9DMoKL+E1vSLsTGhehqRowCQYHKoZIzjgEAwMxADAuAhUAmljDM3c9
hf0j4XbMjjpnzrx1xhkCFQCASR9pgFNgLK8y6Kojj+P1KJkrSQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAIuIHAhL0xWcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA0MTIx
NTI4NTZaGA8yMjAzMDkxNzE1Mjg1NlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCajgAeOauwvqGDLrHvxujnZ1BnkMzwjrycMUTkj8jqNtWoDQWUJVNPZJILosEU
VwK2I3oNkEsx/ryl9XfXcNNceoYfVEPzkTzozrZyuOG66FWtUU1LKeJ7h9/rX0Zd
9lZEokrdr6dLPt9FsHWaK5ExlUnWBjNltcQLkkKqoeYaFwIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAE4G5G+FvKTsX3T7BEcId7f5LSCc2J9gZRDiWn2oTr40CrBMOzJT
KsWr9W89YXW3gaGWltzc0WCwYQbJZgAkuEAZItJjbhdnns87ZbsFO+NZhc6gDtjA
WC3dPlSB9b6rfVoVW9O6Xwa7iNXZo8ddYVJ/ZOIv/totUz9qJt4DmmKk
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANaQIrYcijxaMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA0MTIx
NTI4NTZaGA8yMjAzMDkxNzE1Mjg1NlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAxtMGK4r6WerVtMfpRRCY3DMP9Q/s4jnRIqolPaxeT99BAFp03HXyOrTz
WjggEHArRGGeDowFkL7Vj+QNY7ran2lnYVlAQ7Ow6OLl6WttT6lMsgsLUIcsED6G
eJ1Ko+ovT1qvmuush1U5R2pHkcCJ1IT2s6uQff85l066K7dCFpaoA1QHUk9zACHj
i0DtWuTAWBXirAZSGlmtP6uj1Aw6y5kACDTjIvZJeW/kmswfApTKaJ56eNkJsUBU
NpKwt3um1BMZduy0cjUv0Sc3dIbLNyfOdyPn8tX5u5ck0EPdtBB5WjEh71IXdZJD
oaBREV7AHg5ERPQsm0BqSvMQt09KiwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
qJyZbv/GUQnm8dEyVYgilQr3Yu35n8sfTwwZ1OJzIVce7NBPWePMfYii/tvGoKNp
KwFa/Vugbn1EwqpTEKqkPE1dOZvnUa97XxhYkoW5U7sgdKCANi1KWjywn7MiJ3Eg
j4gdqYK8wxvHi21ppqr572UO77uA8YMBoBT/CyQzWYUSmbqwKnnzaQBAZeO2iAk
VHuNU+9UsntNB676gRl9ag3Wfxq3yx5Ee1CeQf+US3HJn/pKk1H8dExXmBHvHwO6
GKUVNPN1rxfjTiaSt8wuO80uElAnyHIM3VOR8rJO7PKsobyEeJV0WI1hURO+wxpL
h3IsW7iBrFVvhX5xx7ZU
-----END CERTIFICATE-----
```

Asia Pacifico (Tokyo) - ap-northeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULgwDh7TiDrPPBJwscqDwiBHkEFQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEyMjMxMFoXDTI5MDQyODEyMjMxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIEExMQ4IULgwDh7Ti
DrPPBJwscqDwiBHkEFQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBtjAglBde1t4F9EHCZOj4qnY6Gigy07Ou54i+lR77MhbpzE8V28Li9l+YT
QMIn6SzJqU3/fIycIro1OVY1lHmaKYgPGSEZxBenSBHfzwDLRmC9oRp4QMe0BjOC
gepj1lUoiN7OA6PtA+ycNlsP0oJvdBjhvayLiuM3tUfLTrgHbw==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL9KIB7Fgvg/MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAwMjVaGA8yMTk1MDExNzA5MDAyNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAz0djWUcmRW85C5CiCKPFiTIvj6y2OuopFxNE5d3Wtab10bm06vnXVKXu
tz3AndG+Dg0zIL0gMlU+QmrSR0PH2PfV9iejfLak9iwdm1WbwRrCEAj5VxPe0Q+I
KeznOtxzqQ5Wo5NLE9bA61sziUAFNVsTFUzphEwRohcekYyd3bBC4v/RuAjCXHVx
40z6AIksnAOGN2VABMlTeMNvPItKOCIeRLlllSqXX1gbtL1gxSW40JWdF3WPB68E
e+/1U3F7OEr7XqmNODOL6yh92QqZ8fHjG+afOL9Y2Hc4g+P1nk4w4iohQOPABqzb
MPjK7B2Rze0f9OEc51GBQu13kxkWWQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU5DS5IFdU/QwYbikgtWvkU3fDwRgwgY4GA1UdIwSBhjCBg4AU5DS5
IFdU/QwYbikgtWvkU3fDwRihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL9KIB7Fgvg/MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAG/N7ua8IE9IMyno0n5T57erBvLTOQ79fIJN
Mf+mKRM7qRRsdg/eumFft0rLOKo54pJ+Kim2cngCWNhkzctRHBV567AJNt4+ZDG5
hDgV0IxWO1+eaLE4qzqWP/9VrO+p3reuumgFZLVpvVpwXBBeBFUf2drUR14aWfI2
L/6VGINXYs7uP8v/2VBS7r6XZRnPBUy/R4hv5efYXnjwA9gq8+a3stC2ur8m5ySl
faKSwE4H320yAyaZWH4gpwUdbUlYgPHtm/ohRtiWPrN7KEG5Wq/REzMIjZCnxOfS
6KR6PNjlhxBsImQhmBvz6j5PLQxOxBZIpDoiK278e/1Wqm9LrBc=
-----END CERTIFICATE-----
```

Canada (Centrale) - ca-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUIrLgixJJB5C4G8z6pZ5rB0JU2aQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MzU0M1oXDTI5MDQyODE1MzU0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUIrLgixJJ
B5C4G8z6pZ5rB0JU2aQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBHiQJmzyFAaSYs8SpiRijIDZW2RIo7qBKb/pI3rqK6yOWDlPuMr6yNI81D
IrKGGftg4Z+2KETYU4x76HSf0s//vfH3QA57qFaAwddhKYy4BhteFQl/Wex3xTlX
LiwI07kwJvJy3mS6UfQ4HcvZy219tY+0iyOWrz/jVxwq7TOkCw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJNKhJhaJOuMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA3Mjkx
MTM3MTdaGA8yMTk2MDEwMjExMzcxN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAhDUh6j1ACSt057nSxAcwMaGr8Ez87VA2RW2HyY8l9XoHndnxmP50Cqld
+26AJtltlqHpI1YdtnZ6OrVgVhXcVtbvte0lZ3ldEzC3PMvmISBhHs6A3SWHA9ln
```

```
InHbToLX/SWqBHLOX78HkPRaG2k0COHpRy+fG9gvz8HCiQaXCbWNFDHZev9OToNI
xhXBVzIa3AgUnGMalCYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGUcMO0
LBvmTGGeWhi04MUZWfOkwn9JjQZuyLg6B1OD4Y6s0LB2P1MovmSJKGY4JcF8Qu3z
xxUbl7Bh9pvzFR5gJN1pjM2n3gJEPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ
UNKM+gIIHNk0G0tzv6vZBT+o/vt+tIp8lEoZwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTamOsguuPrhVpl12OgRWLcT
rjg/K60UMXRsmg2w/cxV45pUBcyVb5h6Op5uEVAVq+CVns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre2IHLsJH5D4SdWcYqBsfTpf3FQThH0l0KoacGrXtsedsxs
9aRd7OzuSEJ+mBxmzxSjSwM84Ooh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+ttEHwRRngX7
-----END CERTIFICATE-----
```

Canada occidentale (Calgary) - ca-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAYPouptUMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAMITzTJUa6cBsIfdHN69zW/
aHjUB4r1ZfKb1FMhIp9EZtEf5n+06oXjUG2+dKRSlFQeEK333ehNZsPd6uqey6TYKtHpFb5XRLS8BpqB
+7gnbAd0CBZM5o4NWesSQ1GLnTdQcGZkYG/
QESkbadoCXQTifCujJE682hTDLIVt1d4ewwCQYHKoZIzjgEAwMvADAsAhRJc4gRS/HWTkCR2MESaQEe/
jOMNQIUNoTwLvuPrmGPupPlGiHe0veZiO8=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUCVFIhsz9lHA88TjOEChaY+KhHjkwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI2MDYxNzA5MjE0M1oXDTMxMDYxNjA5MjE0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDK1kIcG5Q6adBXQM75GldfTSiXl7tn54p10TnspI0ErDdb2B6q
2Ji/v4XBVH13ZCMgqlRHMqV8AWI5iO6gFn2A9sN3AZXTMqwtZeiDdebq3k6Wt7ie
```

```
YvpXTg0qvgsjQIovRZWaBDBJy9x8C2hW+w9lMQjFHkJ7Jy/PHCJ69EzebQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUwCJ9341XAe3MNiXb/yszt4om
ccIwgZkGA1UdIwSBkTCBjoAUwCJ9341XAe3MNiXb/yszt4omccKhYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUCVFIhsz9
lHA88TjOEChaY+KhHjkwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCuorFtp2WcEreUMNlL44zF8JDSkju0ik27J4OdKRow6tPvqYDmyGTvybWh
N4GtOuNEhWzmj4E7eMHzRslxaHXNhxIa8l+M/GRaq9jJwAb6aU9YWcVH9FT/6Jr0
q6myzukFBNLZ9zCrrclp8dOFdGf0310RDpmGmF3qzU0MlHh+Iw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALyTn5IHrIZjMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMzEyMDcx
NTM3MDFaGA8yMjAzMDUxMzE1MzcwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA1GP5os424BJmGPCKOSgOclP7lzUiB85du03M4hfjzSOszsBpmBGFDLz1
owYHtIxlq3+Vi1Lt5Qlx3id/ov1QyaBPFWXVeklHVXy9vieCcI3TdjGjTl1W/8MM
m3X26QPcsnHM/Kk2wJ7s186MrqmdSsp3SCPpxv4vEG2Q9yR2bXY41hpc2rWlW8qU
D0JGXluvmmAdFnto20l1XWZ6xFen1h60DRugek/ufCbN+ljKy0xLqPoavH0Ybjsb
UpsAsBs7phaoN+X/5hIERfbp5LfVnqq54pNG5KNu4KynfW9+kA/WS4cJ6FTTN5t+
y0P1HvcL+BL2RuDy6T2bB21xw5WqtQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQURTvu/Dd4zDnmS5G5CfVLnmUBNOswgY4GA1UdIwSBhjCBg4AURTvu
/Dd4zDnmS5G5CfVLnmUBNOuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALyTn5IHrIZjMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFt523A3Aug6/F8xxyITgA8gkU0btFhlXNSP
U4U2OQ9n0tWI9WqnKNWH3KBxwY5EPitU6b3LM4xc9lDWpz7h2Pto+WhxP9LVKe6f
r8r7teTLCVZ7cfYZHzHg+flZjVpAgzE5BVfrRlj3QKpv0hYT3J1wMtI++Vorq5Nf
aPjzedehJLhmZVALwnfqfLrgv6/gmraP9Vmoa8U4D6AljNiQGYaLwyoPoRm3bUs2
v1Mh9GkEQ1b9+1pFXcqgzJJTGRuiPCyPbECI79FAnx5JM/CkGJV8HlOmjIW1qkK1
Y2qT7wzErrKLJyB53Pw15BdIM1onbDAQreZb0yZQLdoEl/tx7Uk=
-----END CERTIFICATE-----
```

Cina (Pechino) - cn-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
```

```
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAOtrM5XLDSjCMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQx
MDAxNDJaGA8yMTk1MDExNzEwMDE0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvVBz+WQNdPiM9S+aUULOQEriTmNDUrjLWLr7SfaOJScBzis5D5ju0jh1
+qJdkbuGKtFX5OTWTm8pWhInX+hIOoS3exC4BaANoa1A3o6quoG+Rsv72qQf8LLH
sgEi6+LMlCN9TwnRKOToEabmDKorss4zFl7VSsbQJwcBSfOcIwbdRRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9KxsOrcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh4ObXlFN92VtvzD6QBs3CcoFWgyWGvzg+dNG5VCbsiiuRdmii3kcijZ3H
Nv1wCcZoEAqH72etVhsuvNRC/xAP8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA8
ezx5LRjzUU9EYWYhyYIEShFlP1qDHs7F4L46/5lc4pL8FPoQm5CZuAF31DJhYi/b
fcV7i3n++/ymQbCLC6kAg8DUB7NrcROll5ag8d/JXGzcTCnlDXLXx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokEIOtbH1P+g5yll3bI2leYE6Tm8
LKbyfK/532xJPqO9abx4Ddn89ZEC6vvWVNDgTsxERg992Wi+/xoSw3XxkgAryIv1
zQ4dQ6irFmXwCWJqc6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGVgjM6wivVA
-----END CERTIFICATE-----
```

Cina (Ningxia) - cn-nordovest-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
```

```
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPu4ssY3BlzcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEyMDMy
MTI5MzJaGA8yMTk1MDUwODIxMjkzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAsOiGi4A6+YTLzCdIyP8b8SCT2M/6PGKwzKJ5XbSBoL3gsnSWiFYqPg9c
uJPNbiy9wSA9vlyfWMd90qvTfiNrT6vewP813QdJ3EENZOx4ERcf/Wd22tV72kxD
```

```
yw1Q3I1OMH4bOItGQAxU5OtXCjBZEEUZooOkU8RoUQOU2Pql4NTiUpzWacNutAn5
HHS7MDc4lUlsJqbN+5QW6fFrcNG/0Mrib3JbwdFUNhrQ5j+Yq5h78HarnUivnX/3
Ap+oPbentv1qd7wvPJu556LZuhfqI0TohiIT1Ah+yUdN5osoaMxTHKKtf/CsSJ1F
w3qXqFJQA0VWsqjFyHXFI32I/GOupwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCn
Um00QHvUsJSN6KATbghowLynHn3wZSQsuS8E0COpcFJFxP2SV0NYkERbXu0n/Vhi
yq5F8v4/bRA2/xpedLWmvFs7QWlomuXhSnYFkd33Z5gnXPb9vRkLwiMSw4uXls35
qQraczUJ9EXDhrv7VmngIk9H3YsxYrlDGEqh/oz4Ze4ULOgnfkauanHikk+BUEsg
/jsTD+7e+niEzJPihHdsvKFDlud5pakEzyxovHwNJ1GS2I//yxrJFIL91mehjqEk
RLPdNse7N6UvSnuXcOokwu6l6kfzigGkJBxkcq4gre3szZFdCQcUioj7Z4xtuTL8
YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----
```

Europa (Francoforte) - eu-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFD5GsmkxRuecttwsCG763m3u63UwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1NTUyOVoXDTI5MDQyODE1NTUyOVowXDELMAkGA1UEBhMCVVMx
```

```
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFD5Gsmkx
RuecttwsCG763m3u63UwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBBh0WaXlBsW56Hqk588MmJxsOrvcKfDjF57RgEDgnGnQaJcStCVWDO9UYO
JX2tdsPw+E7AjDqjsuxYaotLn3Mr3mK0sNOXq9BljBnWD4pARg89KZnZI8FN35HQ
O/LYOVHCknuPL123VmVRNs51qQA9hkPjvw21UzpDLxaUxt9Z/w==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDExNzA5MDgxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAka8FLhxs1cSJGK+Q+q/vTf8zVnDAPZ3U6oqppOW/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6xPn/3o//wti0cNt6MLsiUeHqNl5H/4U/Q/fR+GA8pJ+L
npqZDG2tFi1WMvvGhGgIbScrjR4VO3TuKy+rZXMYvMRk1RXZ9gPhk6evFnviwHsE
jV5AEjxLz3duD+u/SjPp1vloxe2KuWnyC+EKInnka909sl4ZAUh+qIYfZK85DAjm
GJP4W036E9wTJQF2hZJrzsiB1MGyC1WI9veRISd30izZZL6VVXLXUtHwVHnVASrS
zZDVpzj+3yD5hRXsvFigGhY0FCVFnwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUxC2l6pvJaRflgu3MUdN6zTuP6YcwgY4GA1UdIwSBhjCBg4AUxC2l
6pvJaRflgu3MUdN6zTuP6YehYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAKD+v6LeR/WrMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAIK+DtbUPppJXFqQMv1f2Gky5/82ZwgbbfXa
HBeGSii55b3tsyC3ZW5ZlMJ7Dtnr3vUkiWbV1EUaZGOUlndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AFO/6pQDdPxXn3xBhF0mTKPrOGdvYmjZUtQMSVb9lbMWCFfs
w+SwDLnm5NF4yZchIcTs2fdpoyZpOHDXy0xgxO1gWhKTnYbaZOxkJvEvcckxVAwJ
obF8NyJla0/pWdjhlHafEXEN8lyxyTTyOa0BGTuYOBD2cTYYynauVKY4fqHUkr3v
Z6fboaHEd4RFamShM8uvSu6eEFD+qRmvqlcodbpsSOhuGNLzhOQ=
-----END CERTIFICATE-----
```

Europa (Irlanda) - eu-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUakDaQ1Zqy87Hy9ESXA1pFC116HkwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MTgxMFoXDTI5MDQyODE2MTgxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUakDaQ1Zq
y87Hy9ESXA1pFC116HkwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQADIkn/MqaLGPuK5+prZZ5Ox4bBZLPtreO2C7r0pqU2kPM2lVPyYYydkvP0
lgSmmsErGu/oL9JNztDe2oCA+kNy17ehcsf8cw0uP861czNFKCeU8b7FgBbL+sIm
qi33rAq6owWGi/5uEcfCR+JP7W+oSYVir5r/yDmWzx+BVH5S/g==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOrmqHuaUt0vMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTA2MTlaGA8yMTk1MDQwMzA5MDYxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjE7nVu+aHLtzp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECCtc4ssnf
zQHq2JRVr0GRchvDrbm1HaP/avtFQR/Thvfltwu9AROVT22dUOTvERdkNzveoFCy
hf52Rqf0DMrLXG8ZmQPPXPDFAv+sVMWCDftcChxRYZ6mP9O+TpgYNT1krD5PdvJU
7HcXrkNHDYqbsg8A+Mu2hzl0QkvUET83Csg1ibeK54HP9w+FsD6F5W+6ZSHGJ88l
FI+qYKs7xsjJQYgXWfEt6bbckWs1kZIaIOyMzYdPF6ClYzEec/UhIe/uJyUUNfpT
VIsI5OltBbcPF4c7Y20jOIwwI2SgOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUF2DgPUZivKQR/Zl8mB/MxIkjZDUwgY4GA1UdIwSBhjCBg4AUF2Dg
PUZivKQR/Zl8mB/MxIkjZDWhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOrmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1RlXTMYgXXxl0YggX88XPmPtok17
l4hib/D9/lu4IaFIyLzYNSzsETYWKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nROon79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPZiKzqWa87xh2DbAyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KWkdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----
```

Europa (Londra) - eu-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUCgCV/DPxYNND/swDgEKGiC5I+EwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MjkxNFoXDTI5MDQyODE2MjkxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUCgCV/DPx
YNND/swDgEKGiC5I+EwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQATPu/sOE2esNa4+XPEGKlEJSgqzyBSQLQc+VWo6FAJhGG9fp7D97jhHeLC
5vwfmtTAfnGBxadfAOT3ASkxnOZhXtnRna460LtnNHm7ArCVgXKJo7uBn6ViXtFh
uEEw4y6p9YaLQna+VC8Xtgw6WKq2JXuKzuhuNKSFaGGw9vRcHg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANBx0E2bOCEPMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA4MTEx
NDU2NDJaGA8yMTk2MDExNTE0NTY0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArYS3mJLGaMrh2DmiPLbqr4Z+xWXTzBWCjOwpsuHE9H6dWUUyl2Bgnu+Z
d8QvW306Yleec45M4F2RA3J4hWHtShzsMlOJVRt+YulGeTf9OCPr26QmIFfs5nD4
```

```
fgsJQEry2MBSGA9Fxq3Cw6qkWcrOPsCR+bHOU0XykdKl0MnIbpBf0kTfciAupQEA
dEHnM2J1L2iI0NTLBgKxy5PXLH9weX20BFauNmHH9/J07OpwL20SN5f8TxcM9+pj
Lbk8h1V4KdIwVQpdWkbDL9BCGlYjyadQJxSxz1J343NzrnDM0M4h4HtVaKOS7bQo
Bqt2ruopLRCYgcuFHck/1348iAmbRQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBG
wujwU1Otpi3iBgmhjMClgZyMMn0aQIxMigoFNqXMUNx1Mq/e/Tx+SNaOEAu0n2FF
aiYjvY0/hXOx75ewzZvM7/zJWIdLdsgewpUqOBH4DXFhbSk2TxggSPb0WRqTBxq5
Ed7F7+7GRIeBbRzdLqmISDnfqey8ufW0ks51XcQNomDIRG5s9XZ5KHviDCar8FgL
HngBCdFI04CMagM+pwTO9XN1Ivt+NzUj208ca3oP1IwEAd5KhIhPLcihBQA5/Lpi
h1s3170z1JQ1HZbDrH1pgp+8hSI0DwwDVb3IIH8kPR/J0Qn+hvOl2HOpaUg2Ly0E
pt1RCZe+W7/dF4zsbqwK
-----END CERTIFICATE-----
```

Europa (Milano) - eu-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAqwCCQCMElHPdwG37jAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA0MjkyMDM1MjJaFw00
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQDAkoL4YfdMI/MrQ0oL
NPfeEk94eiCQA5xNOnU7+2eVQtEqjFbDADFENh1p3sh9Q9OoheLFH8qpSfNDWn/0
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJJmT
HJSKSsVUgpdDIRvJXuyB0zdB+wIVALQ3OLaVGdlPMNfS1nD/Yyn+32wnAoGAPBQ3
7XHg5NLOS4326eFRUT+4ornQFjJjP6dp3pOBEzpImNmZTtkCNNUKE4Go9hv5T4lh
R0pODvWv0CBupMAZVBP9ObplXPCyEIZtuDqVa7ukPOUpQNgQhLLAqkigTyXVOSmt
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwJpKADgYQAAoGAV1OEQPYQUg5/M3xf
6vE7jKTxxyFWEyjKfJK7PZCzOIGrE/swgACy4PYQW+AwcUweSlK/Hx2OaZVUKzWo
wDUbeu65DcRdw2rSwCbBTU342sitFo/iGCV/Gjf+BaiAJtxniZze7J1ob8vOBeLv
uaMQmgOYeZ5e0fl04GtqPl+lhcQwCQYHKoZIzjgEAwMwADAtAhQdoeWLrkm0K49+
AeBK+j6m2h9SKQIVAIBNhS2a8cQVABDCQXVXrc0tOmO8
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAOZ3GEIaDcugMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTEwMjQx
NTE5MDlaGA8yMTk5MDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCjiPgW3vsXRj4JoA16WQDyoPc/eh3QBARaApJEc4nPIGoUolpAXcjFhWplo2O+
ivgfCsc4AU9OpYdAPha3spLey/bhHPRi1JZHRNqScKP0hzsCNmKhfnZTIEQCFvsp
DRp4zr91/WS06/flJFBYJ6JHhp0KwM81XQG59lV6kkoW7QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkuGZGT2+rMkk2n81/abzTJvsqRqGRrWv
XRKRXlKdM/dfiuYGokDGxiC0Mg6TYy6wvsR2qRhtXW1OtZkiHWcQCnOttz+8vpew
wx8JGMvowtuKB1iMsbwyRqZkFYLcvH+Opfb/Aayi20/ChQLdI6M2R5VU
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAO/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA0Mjky
MDM1MjJaGA8yMTk4MTAwMjIwMzUyMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAv1ZLV+Z/P6INq+R1qLkzETBg7sFGKPiwHekbpuB6lrRxKHhj8V9vaReM
lnv1Ur5LAPpMPYDsuJ4WoUbPYAqVqyMAo7ikJHCCM1cXgZJefgN6z9bpS+uA3YVh
V/0ipHh/X2hc2S9wvxKWiSHu6Aq9GVpqL035tJQD+NJuqFd+nXrtcw4yGtmvA6wl
5Bjn8WdsP3xOTKjrByYY1BhXpP/f1ohU9jE9dstsRXLa+XTgTPWcWdCS2oRTWPGR
c5Aeh47nnDsyQfP9gLxHeYeQItV/BD9kU/2Hn6mnRg/B9/TYH8qzlRTzLapXp4/5
iNwusrTNexGl8BgvAPrfhjDpdgYuTwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB7
5ya11K/hKgvaRTvZwVV8GlVZt0CGPtNvOi4AR/UN6TMm51BzUB5nurB4z0R2MoYO
Uts9sLGvSFALJ4otoB77hyNpH3drttU1CVVwal/yK/RQLSon/IoUkaGEbqalu+mH
nYad5IG4tEbmepX456XXcO58MKmnczNbPyw3FRzUZQtI/sf94qBwJ1Xo6XbzPKMy
xjL57LHIZCssD+XPifXay69OFlsCIgLim11HgPkRIHEOXLSf3dsW9r+4CjoZqB/Z
jj/P4TLCxbYCLkvglwaMjgEWF40Img0fhx7yT2X92MiSrs3oncv/IqfdVTiN8OXq
jgnq1bf+EZEZKvb6UCQV
-----END CERTIFICATE-----
```

Europa (Parigi) - eu-west-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
```

```
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUaC9fX57UDr6u1vBvsCsECKBZQyIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MzczOFoXDTI5MDQyODE2MzczOFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUaC9fX57U
Dr6u1vBvsCsECKBZQyIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCARv1bQEDaMEzYI0nPlu8GHcMXgmgA94HyrXhMMcaIlQwocGBs6VILGVhM
TXP2r3JFaPEpmXSQNQHvGA13clKwAZbni8wtzv6qXb4L4muF34iQRHF0nYrEDoK7
mMPR8+oXKKuPO/mv/XKo6XAV5DDERdSYHX5kkA2R9wtvyZjPnQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALWSfgHuT/ARMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA1MzEx
MTE4MTZaGA8yMTk2MTEwMzExMTgxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy5V7KDqnEvF3DrSProFcgu/oL+QYD62b1U+Naq8aPuljJe127Sm9WnWA
EBdOSASkOaQ9fzjCPoG5SGgWKxYoZjsevHpmzjVv9+Ci+F57bSuMbjgUbvbRIFUB
bxQojVoXQPHgK5v433ODxkQ4sjRyUbf4YV1AFdfU7zabC698YgPVOExGhXPlTvco
8mlc631ubw2g52j0lzaozUkHPSbknTomhQIvO6kUfX0e0TDMH4jLDG2ZIrUB1L4r
OWKG4KetduFrRZyDHF6ILZu+s6ywiMicUd+2UllDFC6oas+a8D11hmO/rpWU/ieV
jj4rWAFrsebpn+Nhgy96iiVUGS2LuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDE
iYv6FQ6knXCg+svlcaQG9q59xUC5z8HvJZ1+SxzPKKC4PKQdKvIIfE8GxVXqlZG1
cl5WKTFDMapnzb9RV/DTaVzWx3cMYT77vm1Hl1XGjhx611CGcENH1egI3lOTILsa
+KfopuJEQQ9TDMAIkGjhA+KieU/U5Ctv9fdej6d0GC6OEuwKkTNzPWue6UMq8d4H
2xqJboWsE1t4nybEosvZfQJcZ8jyIYcYBnsG13vCLM+ixjuU5MVVQNMY/gBJzqJB
V+U0QiGiuT5cYgY/QihxdHt99zwGaE0ZBC7213NKrlNuLSrqhDI2NLu8NsExqOFy
OmY0v/xVmQUQl26jJXaM
-----END CERTIFICATE-----
```

Europa (Spagna) - eu-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAq
+gAwIBAgIGAXjwLk46MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAGG2m8EKmaf5qQqj3Z
+rzSaTaXE3B/R/4A2VuGqRYR7MljPtwdmU6/3CPjCACcZmTIcOAKbFiDHqadQgBZXfzGpzw8Zo
+eYmmk5fXycgnj57PYH1dIWU6I7mCbAah5MZMcmHaTmIsomGrhcnWB8d8qOU7oZ0UWK4lbiAQs1MihoUwCQYHKoZIzjg
WmbaU7YM5GwCFCvIJOesO5hZ8PHC52dAR8WWC6oe
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUbtiu7xW+c3P65VHqW/gxSFWHT8kwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI2MDYwOTA4NDMzMVoXDTMxMDYwODA4NDMzMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
```

```
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDB/VvR1+45Aey5zn3vPk6xBm5o9grSDL6D2iAuprQnfVXn8CIb
SDbWFhA3fi5ippjKkh3sl8VyCvCOUXKdOaNrYBrPRkrdHdBuL2Tc84RO+3m/rxIU
Z2IK1fDlC6sWAjddf6sBrV2w2a78H0H8EwuwiSgttURBjwJ7KPPJCqaqrQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUcZuHrkKFfuCOW/tfRxCPB7Ro
XQQwgZkGA1UdIwSBkTCBjoAUcZuHrkKFfuCOW/tfRxCPB7RoXQShYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUbtiu7xW+
c3P65VHqW/gxSFWHT8kwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQANhLKjQrxeWPzqlTkLK8b44iyITsV0E+o8+gJN6tKmC0Cgapp1+rCcYDzt
4R3uglYdoRDRrEPJVLjS8XcX5cefteIJRKJGm06d+fTvgzVY11IXo77tnzJF356m
Nwunpudg2r1diQCWQKKftqbdTsQxPGPVTVOFv+tXyW1s1TYj9Q==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALWSmO6DvSpQMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
MzU4NDNaGA8yMjAxMTIyMjEzNTg0M1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuAAhuSpsHC00/fD2zNlBDpNLRndi9qbHsNeuz3WqN7Samj2aSrM2hS+i
hUxx0BspZj0tZCOsbpPZ+i74NOEQtFeqQoEGvKhB1nJiF4y5I81HDhs5qHvoIivm
7rbbik3zgm1PqS/DmDjVQaXPcD31Rd9ILwBmWEwJqHigyNVlxYtCzTQcrlBrvNZM
dnNgCDAdX/HBEFxx9O12xeu0bSt0s+PJWZ1RTbYrNe7LIH6ntUqHxP/ziQ5trXEZ
uqy7aWk1L8uK4jmyNph0lbaqBa3Y6pYmU1nC27UE4i3fnPB0LSiAr+SrwVvX1g4z
ilo8kr+tbIF+JmcgYLBvO8Jwp+EUqQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUwvGzKJL9A5LReJ4Fxo5K6I20xcowgY4GA1UdIwSBhjCBg4AUwvGz
KJL9A5LReJ4Fxo5K6I20xcqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALWSmO6DvSpQMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAJAZd31jyoTGLawAD2+v/vQsaB9vZIx5EImi
G8YGkd61uFWeNhAmtrwyE/i6FDSIphDrMHBkvw/D3BsqK+Ev/JOK/VYuaYDx/8fp
H4cwp9jC57CXzdIDREWNf6M9PsHFg2WA9XNNtClOZL5WJiJwel8eDSg+sqJUxE0l
MW+QChq/20F6niyaRK4bXrZq14as7h+F9u3A9xHEOVP7Zk9C2ehrBXzCMLSDt3GV
fEuMea2RxMhozwz34Hkdb6j18qoCfygubulovRNQjKw/cEmgPR16KfZPP5caILVt
9qkYPvePmbiVswZDee73cDymJYxLqILpOZwyXvUH8StiH42FHZQ=
-----END CERTIFICATE-----
```

Europa (Stoccolma) - eu-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUN1c9U6U/xiVDFgJcYKZB4NkH1QEwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MDYwM1oXDTI5MDQyODE2MDYwM1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUN1c9U6U/
xiVDFgJcYKZB4NkH1QEwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBTIQdoFSDRHkpqNPUbZ9WXR2O5v/9bpmHojMYZb3Hw46wsaRso7STiGGX/
tRqjIkPUIXsdhZ3+7S/RmhFznmZc8e0bjU4n5vi9CJtQSt+1u4E17+V2bF+D3h/7
wcfE0l3414Q8JaTDtfEf/aF3F0uyBvr4MDMd7mFvAMmDmBPSlA==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALc/uRxg++EnMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
NDAwMTFaGA8yMTk3MDkxMzE0MDAxMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzwCGJEJIxqtr2PD2a1mA6LhRzKhTBa1AZsg3eYfpETXIVlrpojMfvVoN
qHvGshWLgrGTT6os/3gsaADheSaJKavxwX3X6tJA8fvEGqr3a1C1MffH9hBWbQqC
LbfUTAbkwis4GdTUwOwPjT1Cm3u9R/VzilCNwkj7iQ65AFAI8Enmsw3UGldEsop4
yChKB3KW3WI0FTh0+gD0YtjrqqYJxpGOYBpJp5vwdd3fZ4t1vidmDMs7liv4f9Bx
p0oSmUobU4GUlFhBchK1DukICVQdnOVzdMonYm7s+HtpFbVHR8yf6QoixBKGdSal
mBf7+y0ixjCn0pnC0VLVooGo4mi17QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
4ONZiixgk2sjJctwbyD5WKLTH6+mxYcDw+3y/F0fWz561YORhP2FNnPOmEkf0Sl/
Jqk4svzJbCbQeMzRoyaya/46d7UioXMHRZam5IaGBhOdQbi97R4VsQjwQj0RmQsq
yDueDyuKTwWLK9KnvI+ZA6e6bRkdNGflK4N8GGKQ+fBhPwVELkbT9f16OJkezeeN
S+F/gDADGJgmPXfjogICb4Kvshq0H5Lm/xZlDULF2g/cYhyNY6EOI/eS5m1I7R8p
D/m6WoyZdpInxJfxW616OMkxQMRVsruLTNGtby3u1g6ScjmpFtvAMhYejBSdzKG4
FEyxIdEjoeO1jhTsck3R
-----END CERTIFICATE-----
```

Europa (Zurigo) - eu-central-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXiKJnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAYNjaCNg/
cfgQOOl1BUj5ClUulqwZ9Q+SfDzPZh9D2C0VbiRANiZoxrV8RdgmzzC5T7VcriVwjwvta2Ch//
b+sZ86E5h0XWWr+BeEjD9cu3eDj12XB5sWEbNHNx49p5Tmtu5r2LDtlL8X/
Rpfalu2Z2OJgjFJWGf7hRwxe456n
+lowCQYHKoZIzjgEAwMvADAsAhRChsLcj4U5CVb2cp5M0RE1XbXmhAIUeGSnH+aiUQIWmPEFja+itWDufIk=
```

```
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJAK+7ZflHYRFQMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yNjA1MjYx
MDU0MDBaFw0zMTA1MjUxMDU0MDBaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
tpnRnabOUc9o82HBjbIBE0xlLYSUa1akp1FiV05VWiG5BjyyjujqwH1ihadrIES
fLy7I6AVUeXBElSu3LitcCLY7ycov6KSmQFLrCcdoaYFN6VB4ZafQE4f1XlQ+fNo
03fSGPvLeTA2umd3xpYgchIl89CxB3YvDAWnC0RLtU8CAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFDFYNKA6vm8m8PtCqgIoU4I3+EpSMIGOBgNVHSME
gYYwgYOAFDFYNKA6vm8m8PtCqgIoU4I3+EpSoWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQCvu2X5R2ERUDASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBADsVuZ+wv4qEfSnGx+MH8s7p
oBWc/w6DTMCltWl7+q6a7C7uTIymgfsbug31ClwB7O3dhy26Ae9gNzXfpRnWN7iK
chhz057HHESzeogH1rTHD2RkJE5z6KCC0F8JgEg+JQSSCuTFKzUuBkW4S8WMQ3Tj
kCniK/KM2bEKllCqvINx
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALvT012pxTxNMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
NTEyMDdaGA8yMjAxMTIyMjE1MTIwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAyn+Lsnq1ykrfYlZkk6aAAYNReNd9Iw8AUwCBkgOr2eBiBBepYxHwU85N
++moQ+j0EV2VaahBeTLShGZZS1HsyK8+cYT2QzpghIoamcYhrPXyIxlWiRQlaqSg
OFiE9bsqL3rCF5Vz+tOiTe5W/7ojfOFls6++g7ZpobwJlpMbuJepqyeHMPyjvO5A
age81lJewc4bxo2ntaW0HCqNksqfYB78j6X6kn3PFpX7FaYAwZA+Xx6C7UCY7rNi
UdQzfAo8htfJi4chz7frpUdQ9kl3IOQrsLshBB5fFUjl09NiFipCGBwi+8ZMeSn1
5qwBI01BWXPfG7WX6OwyjhmH6JtE1wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU8HN4vvJrsZgPQeksMBgJb9xR1yYwgY4GA1UdIwSBhjCBg4AU8HN4
vvJrsZgPQeksMBgJb9xR1yahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALvT012pxTxNMBIGA1UdEwEB/wQIMAYBAf8C
```

```
AQAwDQYJKoZIhvcNAQELBQADggEBAGlHYDtcHpfBvdHx9HeQE8HgNugJUPdEqxun
t9U33p8VFrs+uLPtrOd9HDJEGvvs5h84EUie/oGJxRt7V1Vlid1PvHf6cRmpjgqY
YdggAVkZtY/PnFVmzf2bMVlSQPrqCl7U0zaw2Kvnj4zgX0rZyCetgrRZSUSxotyp
978Wy9ccXwVSeYG/YAr5rJpS6ZH7eRQvUY0IzwFNeaOPgOTEVpcjWlV6+MQEvsEx
W85q+s6AVr49eppEx8SLJsl0C23yB+L+t32tAveQImRWtJMpzZ5cxh/sYgDVeoC0
85H1NK/7H9fAzT1cPu1oHSnB0xYzzHGOAmXmusMfwUk8fL1RQkE=
-----END CERTIFICATE-----
```

Israele (Tel Aviv) - il-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq+gAwIBAgIGAX0QPi
+9MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYX
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAbazCL5XXyPmcw3+oMYQUF5/9YogW6D0FZbYuyPgjOoUwWdl6fjlzWca
pq+l1ezuK2DFOzNTEyPEwwCQYHKoZIzjgEAwMvADAsAhRt1jkpXsvrS
+xTo2M9h2s2uLAhEQIUOZ2FcnTSrshF2EIdixZZwtNv66Q=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUPgjnsnqT7OaGnZgGF7/43ihPh+0wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI2MDYxMjA5MjQyOVoXDTMxMDYxMTA5MjQyOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDrc24u3AgFxnoPgzxR6yFXOamcPuxYXhYKWmapb+S8vOy5hpLo
Re4RkOrY0cM3bN07GdEMlin5mU0y1t8y3ct4YewvmkgT42kTyMM+t1K4S0xsqjXx
xS716uGYh7eWtkxrCihj8AbXN/6pa095h+7TZyl2n83keiNUzM2KoqQVMwIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU+dSlCYS89nZaff8nPOdiQJje
2PkwgZkGA1UdIwSBkTCBjoAU+dSlCYS89nZaff8nPOdiQJje2PmhYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUPgjnsnqT
```

```
7OaGnZgGF7/43ihPh+0wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQDOq6yTQkIXzAZffpLDBss1R8VZzRoLvRzsFa1xpOcRnPqIm0untEHsOGX/
q34FiGQBOVY6btNaZb7aQXDlZGX+sGvst6BYC2u6H6Zpyo0qy0mz6AGA3eVEonJ2
lKpvAwBkrGajRC8JW0Gx31UZDmAcn3gjQi5zMWFead9mJJJA3g==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOVp1h2I9wW7MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTUx
MjQ0MTJaGA8yMjAxMTIxOTEyNDQxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13PkyWvl61iV/SYfO1UFO76UpDfPm2SF/Rz/o33cm699X++EYPxTnoEc
vmWeS0I7eDXc4OCUiToG0sEx0klE0CX1Z1tK6qJ+zgWQLZ9SZEC9H0NsSA6LhrHu
Nq0dzeK3LjhdfcX46/4GqdiptpdTuM4m/hOQ5yx4JMQ/n1sdpv4M5VLRWwWW9Lem
ufb79Id7O9SispxgRsz1KXIjp7N9S4BY7itSXz97uSyzTqEjWZ6mDUhTu3t21GKC
6flALGTTrG2yghEhz53rkvLsvwzjPSSlT6LIf0mrRPzHaf+EdaKoasElE1SHh+ZH
9mI81HywpE+HZ+W+5hBCvjYp90Y1fwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU58tN2JO+yEGq5JbIXxGi4vRVPyIwgY4GA1UdIwSBhjCBg4AU58tN
2JO+yEGq5JbIXxGi4vRVPyKhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOVp1h2I9wW7MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANBN0e1EqNy4+IU2yQzMJ+Wy5ZIOtTP6GSBR
7muVY1bDeAwtNTEOpwgrZVlC7/xq5Q0LC1y0Z70hHXEf8au7qStaAoUtxzvhTAZI
NC0lwoFU56UFw4N0vZII17iqEfoqRC4PpI3OxqEJHFy0VLlvAzJoKB4QLLqDAYVA
LXCiOLoVT+y9tRYsxw5MyO0Bi6fxQIIADl2bE9xkunTN1Jkkwqo3LxNy/ryz4QWR
8K7jHUItifv4h/hxBKpHEquN8CkdvM9oeGl7I8PFrSFEpGr1euDXY0euZzzYiDBV
m6GpTJgzpVsEuIX52dPcPemwQncoIfZyhWDW85MJUnby2WTEcFo=
-----END CERTIFICATE-----
```

Messico (centrale): mx-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq8CCQD4QwfTExrgxTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDExMTQwOTQ4MjRaGA8y
MDUwMTExNTA5NDgyNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
```

```
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtzCCASwGByqGSM44BAEwggEfAoGBAK+pJEOtD2RFlCbf
oAzONffZa42FB8G6OA/30DT81xWvB2Hnmgw7LfiELYqgfuck3YSDffNDcmiFTJuX
AU9u0NtbbxcOytcdUq4HInpHiB85I6WWWKYB66aGbvYowUPpqBZkASb1i/pYAh5W
nNYvx408008tTzqpMfZDchJHzWqBAhUA0ogoJzTw2/4pKhz9aqTsRCzRVPsCgYEA
qklRUcuU0du/bT/M6kWxYvrTGhO9KXQe+7RtbaIq4dWRsCBnO4smDY/GmI9H8ew1
LRJ9AcLGmxDm795CvVZkHNcht7PDAREagWmz2YvhLA+ev6U0RpfdlBXCck2p1CxQ
LMtoFO7DThksHIQBtnlQdHDvguKEZQz/Iobhne6Kb3wDgYQAAoGAQSTlOqFq6RtR
Jvp406XhGl+eO9SQUpevpzG3Dzbdy6EQ8PBJDOHHJvxbebvpnQssh0CnQfTkSw26
jwPy9V5zRC0ZezwnRTyGSJwiErUKDGeVekEAoNJL1USy8jKkgBajlskZrR+0JHDN
Jv3UwYIPplc4ZS2f2E7btrtlaWt/P70wCQYHKoZIzjgEAwMvADAsAhRXljPWKWYf
61DkDVdgPPHsS2/LuwIUejcGV9WuS3uPvJ6lmn4opxUGBZw=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICPzCCAaigAwIBAgIUCmzpTTMBQYItpMC2VDYsZfIAS7IwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcMB1NlYXR0bGUxIDAeBgNVBAoMF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQwMjEyNTAzNloXDTI5MDQwMTEyNTAzNlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYXR0bGUxIDAe
BgNVBAoMF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDfvOnCzm1iN58Nm7k6ehoy6v0lnnFI617D6CY3bfuq01RCdEQL
96+pYawJieTH8JAQKj02CAa3AeaqdXTE/pDhI/YKLreeMb4K68WMn24Wjjs6oxjB
bAmsKXtt9ihKHGBFNUhgFrNFYyA2i7ieJviwpHjQ/XgXiG2u1/t/4VydUwIDAQAB
MA0GCSqGSIb3DQEBCwUAA4GBAL5+vvj4lhaE+J5tuCqV3XJzDd97lsD4le2O2uGw
P0sGdUcRAdxzU3Bwq/hhtzNWnfwo0aCEQKmLM7xyd3nUa0VvKXLq+DDuayipWINr
OATnNxFRe99d38qHTR1dgkjZdKbbtnl6O4fgM57tVEuQJd/N4ILl9jaRcJ5Ip+9t
3y5t
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALxuE00HoJomMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEwMzEx
MTE0MzNaGA8yMjA0MDQwNjExMTQzM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13xWucALo8M/TXbZJgHrqFqFON91dSLPE/eLbmeIJbP1pb9ICd33qKAx
HlKSrXI9b9YS3U1Pl0bF3ZgfeE/x4Y0KDDZwzpf07H8IgRittULJoNLYVKCJXWPq
```

```
Ky1qvDJX3653dUbUu9eAdVCTRgk7eKpPBLAmW27+pgAGzEYrVV3u2AvqNTonvfTU
sPgEVnAL1J490pNM85KtFynxFTWGigHkd3BHidxmLrTH4I4eRxNZ9q/3gsDW+zKt
jQlpM7JzZa2OqxsF5YQDh1fF52Emqsr+ufLeGqDLOgT1QWcqpz57AX8GqZpgZULo
itCRNXbQDzZY9FxIgpiFJv3y/qYYDQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCt
MTeH4EgqjJEjb1qm5tzXYurLprVrEVQ+PhGXJFJd3xAZyeaDVYy7kio08E2xhmHd
HtkBDty2KnOHsTQmeAJCci7d4tYXZ/1qe341wwm9OoFcO8jhIndx6FXJCgQUY4dL
AAr9HQJFWG5dMZgbi1Zuhxdio3sSoOBjL2p7QIsGNkITvCDIs/H0/szpJnyyyIqu
wmUhSel5hdy5MwOsyUKVGnAdaS5Vd9oL4kLszS9nBZ7ny6BC9odIkFAdGqQ5vM4z
vcbfOq14hjatQmJgJhksN/0Dpl78Gheq0pIhP8LTkAOEG2832nQLzCa3oxSk8otG
GJXkzzyQjse+13r8+yNJ
-----END CERTIFICATE-----
```

Medio Oriente (Bahrein) - me-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQCVWIgSmP8RhTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDUxMzA2MjFaFw00
NTAyMDUxMzA2MjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDcwojQfgWdV1QliO0B
8n6cLZ38VE7ZmrjZ9OQV//Gst6S1h7euhC23YppKXi1zovefSDwFU54zi3/oJ++q
PHlP1WGL8IZ34BUgRTtG4TVolvp0smjkMvyRu5hIdKtzjV93Ccx15gVgyk+o1IEG
fZ2Kbw/Dd8JfoPS7KaSCmJKxXQIVAIZbIaDFRGa2qcMkW2HWASyNDl7bAoGBANtz
IdhfMq+l2I5iofY2oj3HI21Kj3LtZrWEg3W+/4rVhL3lTm0Nne1rl9yGujrjQwy5
Zp9V4A/w9w2O10Lx4K6hj34Eefy/aQnZwNdNhv/FQP7Az0fju+Yl6L13OOHQrL0z
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAAKBgQCVS7m77nuNAlZ8
wvUqcooxXMPkxJFl54NxAsAul9KP9KN4svm0O3Zrb7t2FOtXRM8zU3TqMpryq1o5
mpMPsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGWm5EDl
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXHjuQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAqWgAwIBAgIJAMl6uIV/zqJFMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0dGxlMSAw
HgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwRZWMyLmFt
YXpvbmF3cy5jb20wIBcNMTkwNDI2MTQzMjQ3WhgPMjE5ODA5MjkxNDMyNDdaMHIx
```

```
CzAJBgNVBAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0
dGxlMSAwHgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwR
ZWMyLmFtYXpvbmF3cy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALVN
CDTZEnIeoX1SEYqq6k1BV0ZlpY5y3KnoOreCAE589TwS4MX5+8Fzd6AmACmugeBP
Qk7Hm6b2+g/d4tWycyxLaQlcq81DB1GmXehRkZRgGeRge1ePWd1TUA0I8P/QBT7S
gUePm/kANSFU+P7s7u1NNl+vynyi0wUUrw7/wIZTAgMBAAGjgdcwgdQwHQYDVR0O
BBYEFILtMd+T4YgH1cgc+hVsVOV+480FMIGkBgNVHSMEgZwwgZmAFILtMd+T4YgH
1cgc+hVsVOV+480FoXakdDByMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGlu
Z3RvbjEQMA4GA1UEBwwHU2VhdHRsZTEgMB4GA1UECgwXQW1hem9uIFdlYiBTZXJ2
aWNlcyBMTEMxGjAYBgNVBAMMEWVjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOBgQBhkNTBIFgWFd+ZhC/LhRUY
4OjEiykmbEp6hlzQ79T0Tfbn5A4NYDI2icBP0+hmf6qSnIhwJF6typyd1yPK5Fqt
NTpxxcXmUKquX+pHmIkK1LKDO8rNE84jqxrxRsfDi6by82fjVYf2pgjJW8R1FAw+
mL5WQRFexbfB5aXhcMo0AA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANZkFlQR2rKqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTAyMDUx
MzA2MjBaGA8yMTk4MDcxMTEzMDYyMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy4Vnit2eBpEjKgOKBmyupJzJAiT4fr74tuGJNwwa+Is2vH12jMZn9Il1
UpvvEUYTIboIgISpf6SJ5LmV5rCv4jT4a1Wm0kjfNbiIlkUi8SxZrPypcw24m6ke
BVuxQZrZDs+xDUYIZifTmdgD50u5YE+TLg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIpf635JLU3KIBLNEmrkXCVSnDFlsK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU1l9daQeG9roHR+4rIWSPa0opmMxv5nctgypOrE6zKXx2dNXQldd
VULv+WH7s6Vm4+yBeG8ctPYH5GOo+QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBs
ZcViiZdFdpcXESZP/KmZNDxB/kktlIEIhsQ+MNn29jayE5oLmtGjHj5dtA3XNKlr
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTUwI+Fc01JkYZxRFlVBuFA
WGZO+98kxCS4n6tTwVt+nSuJr9BJRVC17apfHBgSS8c5OWna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q34lXZ629IyFirSJ5TTOIc0osNL7vwMQYj8HOn4OBYqxKy8
ZJyvfXsIPh0Na76PaBIs6ZlqAOflLrjGzxBPiwRM/XrGmF8ze4KzoUqJEnK13O6A
KHKgfiigQZ1+gv5FlyXH
-----END CERTIFICATE-----
```

Regione Medio Oriente (EAU) - me-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXhqnnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAW+csuHsWp/7/
pv8CTKFwxsYudxuR6rbWaHCykIeAydXL9AWnphK6yp1ODEMBFl68Xq8Hp23sOWyf8moOhqCom9+0+ovuUFdpvCie86bp
TOZU568Ty1ff3dDWbdRzeNQRHodRG+XEQSizMkAreeWt4kBa+PUwCQYHKoZIzjgEAwMvADAsAhQD3Z
+XGmzKmgaLgGcVX/Qf1+Tn4QIUH1cgksBSVKbWj81tovBMJeKgdYo=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjRrnDjMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
KyA6zyruJQrYy00a6wqLA7eeUzk3bMiTkLsTeDQfrkaZMfBAjGaaOymRo1C3qzE4rIenmahvUplu9ZmLwL1idWXMRX2R
+d2SeoKOKQWoc2UOFZMHYxDue7zkyk1CIRaBukTeY13/
RIrlc6X61zJ5BBtZXlHwayjQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBABTqTy3R6RXKPW45FA+cgo7YZEj/
Cnz5YaoUivRRdX2A83BHuBTvJE2+WX00FTEj4hRVjameE1nENoO8Z7fUVloAFDlDo69fhkJeSvn51D1WRrPnoWGgEfr1
B+Wqm3kVEz/QNcz6npmA6
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM4h7b1CVhqqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MTEx
MDE1MDNaGA8yMjAxMDkxNTEwMTUwM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApybTWfMOhSoMpqPo72eqAmnn1dXGZM+G8EoZXzwHwT/+IHEXNB4q5N6k
tudYLre1bJxuzEw+iProSHjmb9bB9YscRTofjVhBlt35Fc+i8BaMeH94SR/eE8QO
mll8gnLNW3d62lyuhzuyv1e5wVlRqzYw+X2zRH4/wRDOCOpzjKoHIgyPKsMgwsw5
aTZhNMsGxZN9dbkf0iCGeQLDytwU/JTh/HqvSr3VfUOapTJJiyAxoCtZWgp1/7wC
RvOCSMRJobpUqxZgl/VsttwNkikSFz1wGkcYeSQvk+odbnYQckA8tdddoVI56eD4
```

```
qtREQvfpMAX5v7fcqLexl5d5vH8uZQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUOadrbTs+OhzwoAgUJ7RqQNdwufkwgY4GA1UdIwSBhjCBg4AUOadr
bTs+OhzwoAgUJ7RqQNdwufmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM4h7b1CVhqqMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAICTdAOGEOnII8HaGCpCB8us/hGFaLptJaAf
D5SJAyVy66/mdfjGzE1BKkKxnbxemEVUIzbRidOnyilB+pKwN3edAjTZtWdpVA0V
R/G/qQPmcVljtycBz4VC6SuOUYflGzLH1GZ6GJWbuDtFzw8r7HGdRN1wrEPe3UF2
sMpuVezqnRUdvVRoVQP4jFgNsE7kNvtn2NiPhb/CtrxpcwIQ7r6YeoHcBSheuV1Z
xZDHynC3KUprQGx1+Z9QqPrDf180MaoqAlTl4+W6Pr2NJYrVUFGS/ivYshMg574l
CPU6r4wWZSKwEUXq4BInYX6z6iclp/p/J5QnJp2mAwyi6M+I13Y=
-----END CERTIFICATE-----
```

America del Sud (San Paolo) — sa-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUX4Bh4MQ86Roh37VDRRX1MNOB3TcwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
```

```
MB4XDTI0MDQyOTE2NDYwOVoXDTI5MDQyODE2NDYwOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUX4Bh4MQ8
6Roh37VDRRX1MNOB3TcwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBnhocfH6ZIX6F5K9+Y9V4HFk8vSaaKL5ytw/P5td1h9ej94KF3xkZ5fyjN
URvGQv3kNmNJBoNarcP9I7JIMjsNPmVzqWawyCEGCZImoARxSS3Fc5EAs2PyBfcD
9nCtzMTaKO09Xyq0wqXVYn1xJsE5d5yBDsGrzaTHKjxo61+ezQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMcyoxx4U0xxMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU4MDJaGA8yMTk1MDExNzA4NTgwMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAw45IhGZVbQcy1fHBqzROhO8CsrDzxj/WP4cRbJo/2DAnimVrCCDs5O86
FA39Zo1xsDuJHDlwMKqeXYXkJXHYbcPWc6EYYAnR+PlLG+aNSOGUzsy202S03hT0
B20hWPCqpPp39itIRhG4id6nbNRJOzLm6evHuepMAHR4/OV7hyGOiGaV/v9zqiNA
pMCLhbh2xk0PO35HCVBuWt3HUjsgeks2eEsu9Ws6H3JXTCfiqp0TjyRWapM29OhA
cRJfJ/d/+wBTz1fkWOZ7TF+EWRIN5ITEadlDTPnF1r8kBRuDcS/lIGFwrOOHLo4C
cKoNgXkhTqDDBDu6oNBb2rS0K+sz3QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGTwwgY4GA1UdIwSBhjCBg4AUqBy7
D847Ya/w321Dfr+rBJGsGTyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMcyoxx4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACOoWSBf7b9AlcNrl4lr3QWWSc7k90/tUZal
PlT0G3Obl2x9T/ZiBsQpbUvs0lfotG0XqGVVHcIxF38EbVwbw9KJGXbGSCJSEJkW
vGCtc/jYMHXfhx67Szmftm/MTYNvnzsyQQ3v8y3Rdah+xe1NPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIzZhQyyjtsrgGfTLvXeXRokktvsLDS/
YgKedQ+jFjzVJqgr4NjfY/Wt7/8kbbdhzaqlB5pCPjLLzv0zp/XmO6k+JvOePOGh
JzGk5t1QrSju+MqNPFk3+1O7o910Vrhqw1QRB0gr1ExrviLbyfU=
-----END CERTIFICATE-----
```

AWS GovCloud () — us-gov-east-1 US-East

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULVyrqjjwZ461qelPCiShB1KCCj4wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE1MjIzNloXDTI5MDUwNjE1MjIzNlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULVyrqjjw
Z461qelPCiShB1KCCj4wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBfAL/YZv0y3zmVbXjyxQCsDloeDCJjFKIu3ameEckeIWJbST9LMto0zViZ
puIAf05x6GQiEqfBMk+YMxJfcTmJB4Ebaj4egFlslJPSHyC2xuydHlr3B04INOH5
Z2oCM68u6GGbj0jZjg7GJonkReG9N72kDva/ukwZKgq8zErQVQ==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALPB6hxFhay8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
MjMyNDlaGA8yMTk3MDkxMzEyMzI0OVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAva9xsI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWAPkZVxEdl2Gdhwr3SULoKcKmkqE6ltVFrVuPT33La1UufguT9k8ZDDuO9C
hQNHUdSVEuVrK3bLjaSsMOS7Uxmnn7lYT990IReowvnBNBsBlcabfQTBV04xfUG0
/m0XUiUFjOxDBqbNzkEIblW7vK7ydSJtFMSljga54UAVXibQt9EAIF7B8k9l2iLa
mu9yEjyQy+ZQICTuAvPUEWe6va2CHVY9gYQLA31/zU0VBKZPTNExjaqK4j8bKs1/
7dOV1so39sIGBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBt
hO2W/Lm+Nk0qsXW6mqQFsAou0cASc/vtGNCyBfoFNX6aKXsVCHxq2aq2TUKWENs+
mKmYu1lZVhBOmLshyllh3RRoL3Ohp3jCwXytkWQ7ElcGjDzNGc0FArzB8xFyQNdK
MNvXDi/ErzgrHGSpcvmGHiOhMf3UzChMWbIr6udoDlMbSIO7+8F+jUJkh4Xl1lKb
YeN5fsLZp7T/6YvbFSPpmbn1YoE2vKtuGKxObRrhU3h4JHdp1Zel1pZ6lh5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrfOds4VrVVSj+x0ZdY19Plv2
9shw5ez6Cn7E3IfzqNHO
-----END CERTIFICATE-----
```

AWS GovCloud (US-West) — usa-gov-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
```

```
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUe5wGF3jfb7lUHzvDxmM/ktGCLwwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE3MzAzMloXDTI5MDUwNjE3MzAzMlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUe5wGF3jf
b7lUHzvDxmM/ktGCLwwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCbTdpx1Iob9SwUReY4exMnlwQlmkTLyA8tYGWzchCJOJJEPfsW0ryy1A0H
YIuvyUty3rJdp9ib8h3GZR71BkZnNddHhy06kPs4p8ewF8+d8OWtOJQcI+ZnFfG4
KyM4rUsBrljpG2aOCm12iACEyrvgJJrS8VZwUDZS6mZEnn/lhA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANCOF0Q6ohnuMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTAx
OTQyNDdaGA8yMTk1MDIxMzE5NDI0N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzIcGTzNqie3f1olrrqcfzGfbymSM2QfbTzDIOG6xXXeFrCDAmOq0wUhi
3fRCuoeHlKOWAPu76B9os71+zgF22dIDEVkpqHCjBrGzDQZXXUwOzhm+PmBUI8Z1
qvbVD4ZYhjCujWWzrsX6Z4yEK7PEFjtf4M4W8euw0RmiNwjy+knIFa+VxK6aQv94
lW98URFP2fD84xedHp6ozZlr3+RZSIFZsOiyxYsgiwTbesRMI0Y7LnkKGCIHQ/XJ
OwSISWaCddbu59BZeADnyhl4f+pWaSQpQQ1DpXvZAVBYvCH97J1oAxLfH8xcwgSQ
/se3wtn095VBt5b7qTVjOvy6vKZazwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA/
```

```
S8+a9csfASkdtQUOLsBynAbsBCH9Gykq2m8JS7YE4TGvqlpnWehz78rFTzQwmz4D
fwq8byPkl6DjdF9utqZ0JUo/Fxelxom0h6oievtBlSkmZJNbgc2WYm1zi6ptViup
Y+4S2+vWZyg/X1PXD7wyRWuETmykk73uEyeWFBYKCHWsO9sI+62O4Vf8Jkuj/cie
1NSJX8fkervfLrZSHBYhxLbL+actVEo00tiyZz8GnhgWx5faCY38D/k4Y/j5Vz99
7lUX/+fWHT3+lTL8ZZK7fOQWh6NQpI0wTP9KtWqfOUwMIbgFQPoxkP00TWRmdmPz
WOwTObEf9ouTnjG9OZ20
-----END CERTIFICATE-----
```

AWS Cloud sovrano europeo — eusc-de-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAq8CCQDyckpYH0omIDAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEwMTgwOTM5MzdaGA8y
MDUwMTAxOTA5MzkzN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtzCCASsGByqGSM44BAEwggEeAoGBAJR1zx7FzSGhXd3m
U1PfwH33QEK4CHnFSnp/DUse0SdLwsvLkHw7Tq3M7IX4E+TZ6OzYZZeoVZttqbyq
OZ8ROUS7CzDWcQ0503de/ya51cTs4BiO4nv2awm1WEoV9XtQyA2JLn0Jv7g2uja0
317krS+Dk3kjs9RpWvkmiyTMu1YhAhUA69U+A26BWLVpNIZZ0uWMZJSNlIkCgYBw
w1cgrHFGEqJNhqN7Sjs2YwTP+jpp1GvhxKyce5aOh5ErVvufb5gVVoKahrrHEBms
TrBXxnfcPaTupwdmEZ9eM8a+9RS2vye//KU1kGIOMgafPEzBEXs9m7okmAQpYXnG
cVOTtx2gd/E/VfKRiMSAmam178qwvcbcijNqRdLjRQOBhQACgYEAiEFVGYVCntmy
va8c2oU5/owdMws+NZ6u9blat0ymPr/8Q+DR77CgUPJW+K0k41GdgWpVlrsjiiPw
iygzw4DW7Vsl018KcIFUTiSwpzv2in+tKNUkO5Ly0q6arbSxrXZffYe7aOZKtCCH
XWDMKOH2iCvZptMpG7fDDSc7Be8v4AgwCQYHKoZIzjgEAwMwADAtAhQyvCF3q437
RvdPXMFcMc6qrD0svAIVAMvsN3NwOY4KRYlFv9Dnok8D/ixI
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAPybReXZqUSNMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEwMTgw
OTM5MzdaGA8yMjA0MDMyNDA5MzkzN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDShbskmohorgcjN7gfApw89CEsg7praCDggaUVXF6gy9JdJ5INcv7+DkwKaAxd
NQWDsWZnxIOqPuPfyAYVP3D2/exP3Rfxj31UomLduu7S83zgiJ8VVL/GzlDELv5/
```

```
K2rTcd+580NjLSa6FYDcXDip2ir6TXxRYBYHP65dwniE+wIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAKu9t3CAtZt7c+k4bCZlmxrwgps1668p24x7QRmLxgXnwj5A2MOM
qEtxA9Q3q3WxUc0nWKaCTvRrTfWW917xsLcvVL8rI6xCjg2bb5FJ73xzcfSxHr9I
Q1mThJgLaWVIblllGJK7+EogR7gfqlPhc0Ql5bYuaozdt+r69xNuJlyR
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAODRxRi5VXBbMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNTAyMjEx
MjQ0MTRaGA8yMjA0MDcyODEyNDQxNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAr24OkDrpRU1ffx1PAcHZbKu7fZkhfT/e/PDhSkp2FvOzJEqDUT23E2wp
K/44mhJ3d8blYtgBiRXjqRsAFu8ZbzXLc0gaQ9A5woxfx5b7iOMwneCajS9xS5qr
cE0MMEY9XwG8MCp9YBoDJqDJh74oQqcPROBq16L4k2Ys22n1khus4JpwT7VSRE1I
nnt7fGIYsUmNGM+T2E6ubG3FvkY0HbLvNCcGRMCnDYqloo2BthuSG58KbMAku7VD
hMxzzJte5yMuRpHBojQr9N0hZcSJCtSFo6FhlxCzxGzwoSKzqm99ULYL4lf+IORe
DaKoATZJvbnX0LYAKLtPr1Pz9SD9pQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUHpdxehvJwYL2o25SXyxsSndDW48wgY4GA1UdIwSBhjCBg4AUHpdx
ehvJwYL2o25SXyxsSndDW4+hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAODRxRi5VXBbMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFGcArNlGB3oRBaXohpnhrnVblhJJa6U7r1/
M5TAJCKCkziSz3lOZmZZ1YgSnQC1blhUD2rhuS8a0Mw1Ml48nLjIYMMK0tkJRKCD
LPxxEZp4EzogYj6PqfSubzm59MmBenIcJPaJ9y2uY1U4Q3PMfU6M1JqqQ0Lzplq0
n9eWpJK3+7UbtuyAzigO4DRWEBMxJBUU7f2LfY+qFjskoeHopX20cmn1vc1TGyAF
Qf8xdt1SaPKC26zJsrCkiMZJNm4aa8KqvhqBHVjV4NrGeVGCcdlmSDiL71Egk9kh
744eGQxNnhZNvePW2kVcSuh0HpAo4Q4vfpjN+jz2Ves3kjFsrgc=
-----END CERTIFICATE-----
```

Conformità STIG per la tua istanza EC2

Le guide tecniche per l'implementazione della sicurezza (STIGs) sono gli standard di rafforzamento della configurazione creati dalla Defense Information Systems Agency (DISA) per proteggere i sistemi informativi e il software. Per la conformità dei propri sistemi agli standard STIG, è necessario installare, configurare e testare una serie di impostazioni di sicurezza.

STIGs vengono applicati in base alle seguenti classificazioni di vulnerabilità. Quando crei un'immagine hardening STIG o applichi le impostazioni STIG a un'istanza esistente, puoi scegliere quale livello applicare per l'hardening. I livelli superiori includono le impostazioni STIG di tutti i livelli inferiori. Ad esempio, il livello Alto (Categoria I) include le impostazioni delle categorie Medio e Basso.

Livelli di conformità

- Alto (Categoria I)

  Il rischio più grave. Include qualsiasi vulnerabilità che può comportare la perdita di riservatezza, disponibilità o integrità.
- Medio (categoria II)

  Include qualsiasi vulnerabilità che può comportare la perdita di riservatezza, disponibilità o integrità, ma il rischio può essere mitigato.
- Basso (categoria III)

  Include qualsiasi vulnerabilità che degrada le misure di protezione contro la perdita di riservatezza, disponibilità o integrità.

Amazon EC2 fornisce i seguenti metodi per creare istanze hardening STIG:

- È possibile avviare istanze Windows preconfigurate per la protezione avanzata STIG da finestre pubbliche specializzate. AWS AMIs Per ulteriori informazioni, consulta STIG Hardened AWS Windows Server AMIs nel riferimento all'AWS AMI Windows.
- Puoi creare un'AMI personalizzata per avviare istanze preconfigurate create con componenti hardening STIG di EC2 Image Builder. Per ulteriori informazioni, consulta STIG hardening components nella Guida per l'utente di Image Builder.
- Puoi utilizzare il documento di comando AWSEC2-ConfigureSTIG Systems Manager per applicare le impostazioni STIG a un'istanza EC2 esistente. Il documento di comando STIG di Systems Manager analizza eventuali configurazioni errate ed esegue uno script di correzione per installare e aggiornare i certificati DoD e rimuovere i certificati non necessari per mantenere la conformità STIG. Non vengono applicati costi aggiuntivi per l'utilizzo del documento STIG di Systems Manager.

Argomenti

- Impostazioni di hardening STIG per le istanze EC2

- Download di script di hardening STIG
- AWS Systems Manager Utilizzatelo per applicare le impostazioni STIG alla vostra istanza

Impostazioni di hardening STIG per le istanze EC2

Le impostazioni STIG variano in base al sistema operativo dell'istanza e al livello di conformità scelto. Il contenuto seguente contiene dettagli specifici del sistema STIGs che vengono applicati a ciascun livello di conformità.

Indice

- Impostazioni STIG per le istanze EC2 Linux
- Impostazioni di hardening STIG per le istanze EC2 di Windows

Impostazioni STIG per le istanze EC2 Linux

Questa sezione contiene informazioni sulle impostazioni di hardening STIG per Linux supportate da Amazon EC2. Lo script di hardening applica le impostazioni STIG supportate all'infrastruttura basata sulla distribuzione Linux. Se la distribuzione Linux non dispone di impostazioni di hardening STIG proprie, Amazon EC2 utilizza le impostazioni RHEL, come segue.

- Impostazioni Red Hat Enterprise Linux (RHEL) 7
  - RHEL 7
  - CentOS 7
  - Amazon Linux (2AL2)
- Impostazioni RHEL 8 STIG
  - RHEL 8
  - CentOS 8
- Impostazioni RHEL 9 STIG
  - RHEL 9
  - CentOS Stream 9

STIG per Linux Basso (categoria III)

L'elenco seguente contiene le impostazioni STIG che Amazon EC2 supporta nella tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora la ignora

e passa alla successiva. Ad esempio, alcune impostazioni hardening STIG potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

Per un elenco completo, consulta la STIGs Document Library. Per informazioni su come visualizzare l'elenco completo, consulta Strumenti di visualizzazione STIG.

RHEL 7 STIG versione 3 rilascio 15

- RHEL 7/CentOS 7/ AL2

  V-204452, V-204576 e V-204605

RHEL 8 STIG versione 2 versione 6

- RHEL 8/CentOS 8

  V-230241, V-230269, V-230270, V-230281, V-230285, V-230346, V-230381, V-230395, V-230468, V-230469, V-230485, V-230486, V-230491, V-230494, V-230495, V-230496, V-230497, V-230498, V-230499 e V-244527

RHEL 9 STIG versione 2 Release 7

- RHEL 9/CentOS Stream 9

  V-257782, V-257795, V-257796, V-257824, V-257880, V-257946, V-257947, V-258037, V-258067, V-258069, V-258076, V-258138 e V-258173

RHEL 10 STIG versione 1 versione 1

V-280995, V-281203 e V-281292

Amazon Linux 2023 STIG versione 1 rilascio 1

V-274141

SLES 12 STIG versione 3 versione 4

V-217108, V-217113, V-217140, V-217198, V-217209, V-217211, V-217212, V-217213, V-217214, V-217215, V-217216, V-217236, V-217237, V-217238, V-217239, V-217282 e V-255915

SLES 15 STIG versione 2 versione 6

V-234811, V-234850, V-234868, V-234873, V-234905, V-234907, V-234908, V-234909, V-234933, V-234934, V-234935, V-234936, V-234955, V-234963, V-234967 e V-255921

Ubuntu 18.04 STIG versione 2 rilascio 15

V-219163, V-219164, V-219165, V-219172, V-219173, V-219174, V-219175, V-219178, V-219179, V-219180, V-219210, V-219301, V-219327, V-219332 e V-219333

Ubuntu 20.04 STIG versione 2 versione 4

V-238202, V-238203, V-238221, V-238222, V-238223, V-238224, V-238226, V-238234, V-238235, V-238237, V-238308, V-238323, V-238357, V-238362 e V-238373

Ubuntu 22.04 STIG versione 2 versione 7

V-260472, V-260476, V-260479, V-260480, V-260481, V-260520, V-260521, V-260549, V-260550, V-260551, V-260552, V-260581 e V-260596

Ubuntu 24.04 STIG versione 1 versione 4

V-270645, V-270646, V-270664, V-270677, V-270690, V-270695, V-270706, V-270710, V-270734, V-270749, V-270752, V-270818 e V-270820

STIG per Linux Medio (categoria II)

L'elenco seguente contiene le impostazioni STIG che Amazon EC2 supporta nella tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora la ignora e passa alla successiva. Ad esempio, alcune impostazioni hardening STIG potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

Per un elenco completo, consulta STIGs la Document Library. Per informazioni su come visualizzare l'elenco completo, consulta Strumenti di visualizzazione STIG.

> **Note**
>
> La categoria Medio di STIG per Linux include tutte le impostazioni di hardening STIG elencate che si applicano a STIG per Linux Basso (categoria III), oltre che alle impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria II.

RHEL 7 STIG versione 3 rilascio 15

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

- RHEL 7/CentOS 7/ AL2

  V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204415, V-204416, V-204417, V-204418, V-204420, V-204422, V-204423, V-204426, V-204427, V-204431, V-204434, V-204435, V-204437, V-204449, V-204450, V-204451, V-204457, V-204466, V-204490, V-204491, V-204503, V-204507, V-204508, V-204510, V-204511, V-204512, V-204514, V-204515, V-204516, V-204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204541, V-204542, V-204543, V-204544, V-204545, V-204546, V-204547, V-204548, V-204549, V-204550, V-204551, V-204552, V-204553, V-204554, V-204555, V-204556, V-204557, V-204558, V-204559, V-204560, V-204562, V-204563, V-204564, V-204565, V-204566, V-204567, V-204568, V-204572, V-204579, V-204584, V-204585, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204619, V-204622, V-204625, V-204630, V-204631, V-204633, V-233307, V-237634, V-237635, V-251703, V-255925, V-255279, V-255928 e V-256970

RHEL 8 STIG versione 2 versione 6

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

- RHEL 8/CentOS 8

  V-230222, V-230228, V-230231, V-230233, V-230236, V-230237, V-230238, V-230239, V-230240, V-230240, V-230243, V-230244, V-230245, V-230246, V-230247, V-230248, V-230249, V-230250, V-230255, V-230256, V-230257, V-230258, V-230259, V-230260, V-230261, V-230262, V-230266, V-230267, V-230268, V-230271, 230273, V-230275, V-230276, V-230277, V-230278, V-230279, V-230280, V-230280, V-230276 282, AV-230282, V-230286, V-230287, V-230288, V-230290, V-230291, V-230296, V-230298, V-230310, V-230311, V-230312, 230313, V-230314, V-230315, V-230316, V-230318, V-230319, -230320, V-230321, V-230322, V-230324, V-230325, V-230326, V-230327, V-230330, V-230332, V-230333, V-230335, V-230337, V-230339, V-230341, V-230343, V-230345, V-230347, V-230348, V-230352, V-230353, V-230354, V-230356, V-230357, V-230358, V-230359, V-230360, V-230361, V-230362, V-230363, V-230365, V-230366, V-230368, V-230369,

V-230370, V-230372, V-230373, V-230375, V-230376, V-230377, V-230378, V-230380, V-230382, V-230383, V-230385, V-230386, V-230387, V-230389, V-230390, V-230392, V-230393, V-230394 396, V-230397, V-230398, V-230399, V-230400, V-230401, V-230402, V-230403, V-230404, V-230405, V-230406, V-230407, V-230408, V-230409, V-230410, V-230411, V-230412, V-230413, 230418, 230419, V-230421, V-230422, V-230423, V-230424, V-230425, V-230426, V-230427, V-230428, V-230429, V-230430, V-230431, V-230432, V-230433, V-230434, V-230435, V-230436, V-230437, V-230438, V-230439, V-230444 V-230446, V-230447, V-230449, V-230455, V-230456, V-230462, V-230463, V-230464, V-230465, V-230466, V-230467, V-230470, V-230471, V-230472, V-230473, V-230474, V-230475, V-230478, V-230480, V-230481, V-230482, V-230483, V-230488, V-230489, V-230493, V-230502, V-230503, V-230505, V-230506, V-230507, V-230523, V-230524, V-230525, 230526, 230527, 230532, 230535, 230536, 230537, 30538, V-230539, V-230540, V-230541, V-230542, MA-230543, V-230544, V-230545, V-230546, V-230547, 230548, 230549, 230550, 230555, 230556, V-230557, V-230559, V-230560, V-230561, V-237640, V237642, V-237643, V-244519, V-244523, V-244524, V-244525, V-244526, V-244528, V-244531, V-244533, V-244535, V-244536, V-244538, V-244538, V-244538, V-244539, V-244542, V-244543, V-244545, V-244547, V-244550, V-244551, V-244552, V-244553, V-244554, V-250315, V-250315, V-250315, V-250316, V-250316, V-250316, V-250317, V-251707, V-251708, V-251709, V-251710, V-251711, V-251713, V-251714, V-251715, V-251716, V-251717, V-251718, V-256918 74, V-257258, V-257258, V-274877, V-279929, V-279930 e V-279931

RHEL 9 STIG versione 2 Release 7

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

- RHEL 9/CentOS Stream 9

V-257780, V-257781, V-257783, V-257786, V-257788, V-257790, V-257791, V-257792, V-257793, V-257794, V-257797, V-257798, V-257799, V-257800, V-257801, V-257802, V-257803, V-257804, V-257805, V-257806, V-257807, V-257808, V-257809, V-257810, V-257811, V-257812, V-257813, V-257814, V-257815, V-257816, V-257817, V-257818, V-257825, V-257827, V-257828, V-257829, V-257830, V-257831, V-257832, V-257833, V-257834, V-257836, V-257838, V-257839, V-257840, V-257841, V-257842, V-257849, V-257882, V-257883, V-257884, V-257885, V-257886, V-257887, V-257888, V-257889, V-257890, V-257891, V-257892, V-257893, V-257894, V-257895, V-257896, V-257897, V-257898, V-257899, V-257900, V-257901, V-257902, V-257903, V-257904, V-257905, V-257906, V-257907, V-257908, V-257909, V-257910, V-257911, V-257912, V-257913, V-257914, V-257915, V-257916, V-257917, V-257918, V-257919, V-257920, V-257921, V-257922, V-257923,

V-257924, V-257925, V-257926, V-257927, V-257928, V-257929, V-257930, V-257933, V-257934, V-257935, V-257936, V-257939, V-257940, V-257942, V-257943, V-257944, V-257948, V-257951, V-257952, V-257953, V-257954, V-257957, V-257958, V-257959, V-257960, V-257961, V-257962, V-257963, V-257964, V-257965, V-257966, V-257967, V-257968, V-257969, V-257970, V-257971, V-257972, V-257973, V-257974, V-257975, V-257976, V-257977, V-257978, V-257979, V-257980, V-257982, V-257983, V-257985, V-257987, V-257988, V-257992, V-257993, V-257994, V-257995, V-257996, V-257997, V-257998, V-257999, V-258000, V-258001, V-258002, V-258003, 258004, V-258005, V-258006, V-258007, V-258008, V-258009, V-258010, V-258011, V-258028, V-258034, V-258035, V-258038, V-258039, V-258040, V-258041, V-258043, V-258046, V-258049, V-258052, V-258054, V-258055, V-258056, V-258057, V-258060, V-258063, V-258064, V-258065, V-258066, V-258068, V-258070, V-258071, V-258072, V-258073, V-258074, V-258075, V-258077, V-258079, V-258080, V-258081, V-258082, V-258083, V-258084, V-258085, V-258088, V-258089, V-258090, V-258091, V-258092, V-258093, V-258095, V-258097, V-258098, V-258099, V-258100, V-258101, V-258102, V-258103, V-258104, V-258105, V-258107, V-258108, V-258109, V-258110, V-258111, V-258112, V-258113, V-258114, V-258115, V-258116, V-258117, V-258118, V-258119, V-258120, V-258121, V-258122, V-258123, V-258124, V-258125, V-258126, V-258128, V-258129, V-258130, V-258133, V-258137, V-258140, V-258141, V-258142, V-258144, V-258145, V-258146, V-258147, V-258148, V-258157, V-258158, V-258159, V-258160, V-258161, V-258162, V-258163, V-258164, V-258165, V-258166, V-258167, V-258168, V-258169, V-258170, V-258171, V-258172, V-258175, V-258175, V-258176, V-258177, V-258178, V-258179, V-258181, V-258182, V-258183, V-258183, V-258183, V-184, V-258185, V-258186, V-258187, V-258188, V-258189, V-258190, V-258191, V-258192, V-258193, V-258194, V-258195, V-258196, V-258197, V-258198, V-258199, V-258200, V-258201, V-258202, V-258203, V-258204, V-258205, V-258206, V-258207, V-258208, V-258208, V-258209, V-258210, V-258211, V-258212, V-258213, V-258214, V-258215, V-258215, V-258215, V-258215, V-258215, V-258214, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-258215, V-2582258216, V-258217, V-258218, V-258219, V-258220, V-258221, V-258222, V-258223, V-258224, V-258225, V-258226, V-258227, V-258228, V-258228, V-258229, V-258232, V-258233, V-258233, V-258234, V-258237, V-258239, V-270174, V-270175, V-270176, V-270177, V-272488 e V-279936

RHEL 10 STIG versione 1 Release 1

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

V-280094, V-280942, V-280943, V-280945, V-280946, V-280947, V-280948, V-280950, V-280952, V-280953, V-280954, V-280955, V-280956, V-280958, V-280959, V-280960, V-280961, V-280962,

V-280963, V-280964, V-280965, V-280966, V-280967, V-280968, V-280969, V-280970, V-280972, V-280973, V-280974, V-280975, V-280976, V-280977, V-280981, V-280983, V-280984, V-280986, V-280987, V-280988, V-280989, V-280990, V-280991, V-280992, V-280993, V-280994, V-280996, V-280997, V-280999, V-281000, V-281001, V-281002, V-281003, V-281005, V-281006, V-281017, V-281018, V-281019, V-281020, V-281021, V-281022, V-281023, V-281024, V-281025, V-281026, V-281027, V-281028, V-281029, V-281030, V-281031, V-281032, V-281033, V-281034, V-281035, V-281036, V-281037, V-281038, V-281039, V-281040, V-281041, V-281042, V-281043, V-281044, V-281045, V-281047, V-281048, V-281049, V-281050, V-281051, V-281052, V-281053, V-281054, V-281055, V-281056, V-281057, V-281058, V-281059, V-281060, V-281061, V-281062, V-281063, V-281064, V-281065, V-281066, V-281067, V-281068, V-281069, V-281070, V-281071, V-281072, V-281073, V-281074, V-281075, V-281076, V-281077, V-281078, V-281079, V-281080, V-281081, V-281082, V-281083, V-281084, V-281085, V-281086, V-281087, V-281094, V-281095, V-281096, V-281097, V-281098, V-281099, V-281100, V-281101, V-281102, V-281103, V-281104, V-281105, V-281107, V-281108, V-281109, V-281110, V-281111, V-281113, V-281114, V-281115, V-281116, V-281117, V-281118, V-281119, V-281120, V-281121, V-281122, V-281123, V-281124 281125, V-281126, V-281127, V-281128, V-281129, V-281130, V-281131, V-281132, V-281133, V-281134, V-281135, V-281136, V-281137, V-281138, V-281139, V-281140, V-281141, V-281142, V-281143, V-281144, V-281145, V-281146, V-281147, V-281148, V-281149, V-281150, V-281151, V-281152, V-281153, V-281154, V-281155, V-281156, V-281157, V-281158, V-281159, V-281160, V-281161, V-281162, V-281163, V-281164, V-281165, V-281168, V-281169, V-281171, V-281174, V-281175, V-281177, V-281178, V-281179, V-281180, V-281181, V-281182, V-281183, V-281184, V-281185, V-281187, V-281188, V-281189, V-281190, V-281191, V-281192, V-281193, V-281195, V-281196, V-281197, V-281198, V-281200, V-281201, V-281204, V-281205, V-281206, V-281209, V-281210, V-281212, V-281214, V-281215, V-281217, V-281218, V-281219, V-281220, V-281224, V-281225, V-281226, V-281249, V-281251, V-281252, V-281253, V-281254, V-281255, V-281256, V-281257, V-281258, V-281259, V-281260, V-281261, V-281262, V-281263, V-281264, V-281265, V-281266, V-281269, V-281270, V-281271, V-281272, V-281273, V-281274, V-281276, V-281277, V-281278, V-281279, V-281280, V-281281, V-281282, V-281284, V-281285, V-281286, V-281287, V-281288, V-281289, V-281290, V-281291, V-281293, V-281295, V-281296, V-281297, V-281300, V-281301, V-281302, V-281303, V-281304, V-281305, V-281306, V-281308, V-281309, V-281310, V-281311, V-281312, V-281313, V-281314, V-281315, V-281316, V-281317, V-281318, V-281319, V-281320, V-281322, V-281323, V-281324, V-281325, V-281327, V-281328, V-281331, V-281334, V-281334, V-281335, V-281337, V-281338, V-281340, V-281341, V-281342, V-281343, V-281344, V-281345, V-281346, V-281347, V-281348, V-281349, V-281350, V-281351, V-281352, V-281353, V-281354, V-281355, V-281356, V-281357, V-281358, V-281359, V-281360, V-281361, V-281363, V-281364 e V-281365

Amazon Linux 2023 STIG versione 1 versione 2

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

V-273995, V-274000, V-274001, V-274002, V-274003, V-274004, V-274005, V-274006, V-274008, V-274009, V-274010, V-274011, V-274012, V-274013, V-274014, V-274017, V-274018, V-274019, V-274020, V-274021, V-274022, V-274023, V-274024, V-274026, V-274027, V-274028, V-274030, V-274031, V-274032, V-274033, V-274034, V-274035, V-274036, V-274037, V-274040, V-274041, V-274042, V-274044, V-274045, V-274047, V-274048, V-274049, V-274050, V-274051, V-274053, V-274054, V-274059, V-274061, V-274062, V-274069, V-274070, V-274071, V-274072, V-274073, V-274074, V-274075, V-274076, V-274077, V-274078, V-274079, V-274081, V-274082, V-274083, V-274084, V-274085, V-274086, V-274087, V-274088, V-274089, V-274090, V-274091, V-274092, V-274093, V-274094, V-274095, V-274096, V-274097, V-274098, V-274099, V-274100, V-274101, V-274102, V-274103, V-274104, V-274105, V-274106, V-274107, V-274108, V-274109, V-274110, V-274111, V-274112, V-274113, V-274114, V-274115, V-274116, V-274117, V-274119, V-274120, V-274121, V-274122, V-274123, V-274124, V-274125, V-274126, V-274127, V-274128, V-274129, V-274130, V-274131, V-274132, V-274133, V-274134, V-274135, V-274136, V-274137, V-274138, V-274139, V-274140, V-274142, V-274143, V-274144, V-274145, V-274147, V-274149, V-274151, V-274152, V-274154, V-274155, V-274156, V-274157, V-274160, V-274161, V-274162, V-274163, V-274164, V-274165, V-274166, V-274167, V-274168, V-274169, V-274170, V-274173, V-274177, V-274181, V-274182, V-274185 e V-274187

SLES 12 STIG versione 3 Release 4

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

V-217102, V-217105, V-217105, V-217106, V-217106, V-217110, V-217116, V-217117, V-217118, V-217119, V-217120, -217121, V-217122, V-217124, V-217125, V-217126, V-217127, V-217128, V-217130, V-217134, V-217138, V-217143, V-217147, V-217152, V-217153, V-217154, V-217155, V-217156, V-217158, V-217161, AB-217163, V-217166, V-217167, V-217168, V-217169, V-217170, AB-217171, V-217182, V-217183, V-217188, V-217190, V-217191, V-217194, V-217195, V-217196, V-217197, V-217200, V-217201, V-217202, AB-217203, V-217204, V-217205, V-217206, V-217207, V-217208, V-217210, V-217217217, V-217218, V-217223, V-217227, V-217230, V-217240, V-217241, V-217242, V-217243, V-217244, V-217245, V-217246, V-217247, V-217248, V-217249, V-217250, V-217251, V-217252, V-217253, V-217254, V-217255, V-217257, V-217258, V-217260, V-217265, V-217266, V-217267, V-217269, V-217272, V-217273, V-217274, V-217275, V-217276,

V-217277, V-217278, V-217279, V-217280, V-217283, V-217283 V-217284, V-217286, V-217288, V-217289, V-217290, V-217291, V-217292, V-217293, V-217294, V-217295, V-217296, V-217299, V-217300, V-217301, V-217302, V-233308, V-237605, V-237606, V-237607, V-237608, V-237609, V-237610, V-237611, V-237612, V-237613, V-237614, V-237615, V-237616, V-237617, V-237618, V-237619, V-237620, V-237621, V-237622, V-237623, V-251720, V-251722, V-255914 e V-256981

SLES 15 STIG versione 2 Release 6

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

V-234802, V-234807, V-234808, V-234809, V-234813, V-234815, V-234817, V-234821, V-234822, V-234823, V-234825, V-234827, V-234828, V-234829, V-234830, V-234832, V-234833, V-234834, V-234835, V-234836, V-234837, V-234838, V-234839, V-234840, V-234841, V-234842, V-234843, V-234844, V-234845, V-234848, V-234854, V-234855, V-234856, V-234857, V-234858, V-234861, V-234862, V-234863, V-234869, V-234870, V-234875, V-234878, V-234880, V-234881, V-234882, V-234883, V-234884, V-234885, V-234886, V-234887, V-234888, V-234889, V-234891, V-234895, V-234896, V-234897, V-234899, V-234900, V-234901, V-234902, V-234903, V-234904, V-234906, V-234910, V-234911, V-234912, V-234913, V-234914, V-234918, V-234924, V-234928, V-234932, V-234937, V-234938, V-234939, V-234940, V-234941, V-234942, V-234943, V-234944, V-234945, V-234946, V-234947, V-234948, V-234949, V-234950, V-234951, V-234952, V-234954, V-234956, V-234957, V-234958, V-234959, V-234961, V-234962, V-234964, V-234966, V-234969, V-234973, V-234975, V-234976, V-234977, V-234978, V-234979, V-234981, V-234982, V-234983, V-234991, V-235002, V-235003, V-235007, V-235008, V-235009, V-235010, V-235013, V-235014, V-235015, V-235016, V-235017, V-235018, V-235019, V-235020, V-235021, V-235022, V-235023, V-235024, V-235025, V-235026, V-235028, V-235029, V-235030, V-251724, V-255920, V-256983 e V-274879

Ubuntu 18.04 STIG versione 2 rilascio 15

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

V-219149, V-219155, V-219156, V-219160, V-219166, V-219168, V-219176, V-219181, V-219184, V-219186, V-219188, V-219189, V-219190, V-219191, V-219192, V-219193, V-219194, V-219195, V-219196, V-219197, V-219198, V-219199, V-219200, V-219201, V-219202, V-219203, V-219204, V-219205, V-219206, V-219207, V-219208, V-219209, V-219213, V-219214, V-219215, V-219216, V-219217, V-219218, V-219219, V-219220, V-219221, V-219222, V-219223, V-219224, V-219225, V-219226, V-219227, V-219228, V-219229, V-219230, V-219231, V-219232, V-219233, V-219234, V-219235, V-219236, V-219238, V-219239, V-219240, V-219241, V-219242, V-219243, V-219244,

V-219250, V-219254, V-219257, V-219263, V-219264, V-219265, V-219266, V-219267, V-219268, V-219269, V-219270, V-219271, V-219272, V-219273, V-219274, V-219275, V-219276, V-219277, V-219279, V-219281, V-219287, V-219291, V-219296, V-219297, V-219298, V-219299, V-219300, V-219303, V-219304, V-219306, V-219309, V-219310, V-219311, V-219315, V-219318, V-219319, V-219323, V-219326, V-219328, V-219330, V-219331, V-219335, V-219336, V-219337, V-219338, V-219339, V-219342, V-219344, V-233779, V-233780 e V-255906

Ubuntu 20.04 STIG versione 2 Release 4

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

V-238200, V-238205, V-238207, V-238209, V-238210, V-238211, V-238212, V-238213, V-238220, V-238225, V-238227, V-238228, V-238229, V-238230, V-238231, V-238232, V-238236, V-238238, V-238239, V-238240, V-238241, V-238242, V-238244, V-238245, V-238246, V-238247, V-238248, V-238249, V-238250, V-238251, V-238252, V-238253, V-238254, V-238255, V-238256, V-238257, V-238258, V-238264, V-238268, V-238271, V-238277, V-238278, V-238279, V-238280, V-238281, V-238282, V-238283, V-238284, V-238285, V-238286, V-238287, V-238288, V-238289, V-238290, V-238291, V-238292, V-238293, V-238294, V-238295, V-238297, V-238298, V-238299, V-238300, V-238301, V-238302, V-238303, V-238304, V-238309, V-238310, V-238315, V-238316, V-238317, V-238318, V-238319, V-238320, V-238324, V-238325, V-238329, V-238330, V-238333, V-238334, V-238337, V-238338, V-238339, V-238340, V-238341, V-238342, V-238343, V-238344, V-238345, V-238346, V-238347, V-238348, V-238349, V-238350, V-238351, V-238352, V-238353, V-238355, V-238356, V-238359, V-238360, V-238369, V-238370, V-238371, V-238376, V-238377, V-238378, V-251505, V-255912, V-274852 e V-274853

Ubuntu 22.04 STIG versione 2 Release 7

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

V-260471, V-260473, V-260474, V-260475, V-260475, V-260477, V-260478, V-260485, V-260486, V-260487, V-260488, V-260489, V-260490, V-260491, V-260492, V-260493, V-260494, V-260495, V-260496, V-260496, V-260496 497, V-260498, V-260499, V-260500, V-260505, V-260506, V-260507, V-260508, V-260509, V-260510, V-260511, V-260512, V-260513, V-260514, V-260522, V-260527, V-260528, V-260530, V-260533, V-260533, V-260522 34, V-260535, V-260537, V-260538, V-260540, V-260542, V-260543, V-260545, V-260546, V-260547, V-260553, V-260554, V-260555, V-260556, V-260557, V-260560, V-260561, V-260562, V-260563, V-260564, V-260565, V-260566, V-260567, V-260569, V-260572, V-260573, V-260574, V-260575, V-260576, V-260582,

V-260584, V-260585, V-260586, V-260588, V-260589, V-260590, V-260591, V-260594, V-260597, V-260598, V-260599, V-260600, V-260601, V-260602, V-260603, V-260604, V-260605, V-260606, V-260607, V-260608, V-260609, V-260610, V-260611, V-260612, V-260613, V-260614, V-260615, V-260616, V-260617, V-260618, V-260619, V-260620, V-260621, V-260622, V-260623, V-260624, V-260625, V-260626, V-260627, V-260628, V-260629, V-260630, V-260631, V-260632, V-260633, V-260634, V-260635, V-260636, V-260637, V-260638, V-260639, V-260640, V-260641, V-260642, V-260643, V-260644, V-260645, V-260646, V-260647, V-260648, V-260649, V-274862, V-274864 e V-274866

Ubuntu 24.04 STIG Versione 1 Release 4

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

V-270649, V-270651, V-270652, V-270653, V-270654, V-270656, V-270657, V-270659, V-270660, V-270661, V-270662, V-270663, V-270669, V-270672, V-270673, V-270674, V-270676, V-270678, V-270679, V-270680, V-270681, V-270683, V-270684, V-270685, V-270686, V-270687, V-270688, V-270689, V-270692, V-270693, V-270696, V-270697, V-270698, V-270699, V-270700, V-270701, V-270702, V-270703, V-270704, V-270705, V-270709, V-270715, V-270716, V-270718, V-270720, V-270721, V-270722, V-270723, V-270724, V-270725, V-270726, V-270727, V-270728, V-270729, V-270730, V-270731, V-270732, V-270733, V-270737, V-270739, V-270740, V-270741, V-270742, V-270743, V-270746, V-270750, V-270753, V-270755, V-270756, V-270757, V-270758, V-270759, V-270760, V-270765, V-270766, V-270767, V-270768, V-270769, V-270770, V-270771, V-270772, V-270773, V-270775, V-270776, V-270777, V-270778, V-270779, V-270780, V-270781, V-270782, V-270783, V-270784, V-270785, V-270786, V-270787, V-270788, V-270789, V-270790, V-270791, V-270792, V-270793, V-270794, V-270795, V-270796, V-270797, V-270798, V-270799, V-270800, V-270801, V-270802, V-270803, V-270804, V-270805, V-270806, V-270807, V-270808, V-270809, V-270810, V-270811, V-270812, V-270813, V-270814, V-270815, V-270821, V-270822, V-270823, V-270824, V-270825, V-270826, V-270827, V-270828, V-270829, V-270830, V-270831, V-270832, V-274870, V-274871, V-274872 e V-274873

STIG per Linux Alto (categoria I)

L'elenco seguente contiene le impostazioni STIG che Amazon EC2 supporta nella tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora la ignora e passa alla successiva. Ad esempio, alcune impostazioni hardening STIG potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

Per un elenco completo, consulta la STIGs Document Library. Per informazioni su come visualizzare l'elenco completo, consulta Strumenti di visualizzazione STIG.

> **Note**
>
> La categoria Alto di STIG per Linux include tutte le impostazioni di hardening STIG elencate che si applicano a STIG per Linux Medio e Basso, oltre che alle impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria I.

RHEL 7 STIG versione 3 rilascio 15

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

- RHEL 7/CentOS 7/ AL2

  V-204424, V-204425, V-204442, V-204443, V-204447, V-204448, V-204455, V-204462, V-204497, V-204497, V-204502, V-204594, V-204620 e V-204621

RHEL 8 STIG versione 2 versione 6

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

- RHEL 8/CentOS 8

  V-230223, V-230264, V-230283, V-230284, V-230487, V-230492, V-230533, V-230558, V-244540, V-279933, V-230265, V-230226, V-230530, V-268322, V-230529 e V-230531

RHEL 9 STIG versione 2 Release 7

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

- RHEL 9/CentOS Stream 9

  V-257820, V-257821, V-257826, V-257835, V-257955, V-257956, V-258059, V-258230, V-258238, V-257984, V-257986, V-258078, V-258094, V-258235, V-257784 e V-257785

RHEL 10 versione 1 versione 1

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

V-280932, V-280933, V-280934, V-280944, V-280949, V-280951, V-280978, V-281007, V-281014, V-281015, V-281216, V-281222, V-281223, V-281267, V-281268, V-281275, V-281298, V-281299 e V-281307

Amazon Linux 2023 STIG versione 1 versione 2

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

V-273996, V-273997, V-273999, V-274007, V-274038, V-274039, V-274046, V-274052, V-274057 e V-274153

SLES 12 STIG versione 3 versione 4

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

V-217101, V-217139, V-217141, V-217142, V-217159, V-217160, V-217164, V-217264, V-217268, V-222386 e V-251721

SLES 15 STIG versione 2 versione 6

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

V-234800, V-234804, V-234818, V-234852, V-234859, V-234860, V-234898, V-234984, V-234985, V-234988, V-234989, V-234990, V-235031, V-235032 e V-251725

Ubuntu 18.04 STIG versione 2 rilascio 15

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

V-219157, V-219158, V-219177, V-219212, V-219308, V-219314, V-219316 e V-251507

Ubuntu 20.04 STIG versione 2 versione 4

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

V-238201, V-238218, V-238219, V-238326, V-238327, V-238380 e V-251504

Ubuntu 22.04 STIG versione 2 versione 7

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

V-260469, V-260482, V-260483, V-260523, V-260524, V-260526, V-260529, V-260539, V-260570, V-260571, V-260579 e V-279937

Ubuntu 24.04 STIG versione 1 versione 4

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

V-270647, V-270648, V-270665, V-270666, V-270708, V-270711, V-270712, V-270713, V-270714, V-270717, V-270736, V-270738 e V-279938

Impostazioni di hardening STIG per le istanze EC2 di Windows

Amazon EC2 supporta le basi STIG per le seguenti versioni del sistema operativo Windows:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Questa sezione elenca le impostazioni STIG correnti supportate da Amazon EC2 per l'infrastruttura Windows, seguite da un log della cronologia della versione.

Puoi applicare le impostazioni STIG a livello Basso, Medio o Alto.

STIG per Windows Basso (categoria III)

L'elenco seguente contiene le impostazioni STIG che Amazon EC2 supporta nella tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora la ignora e passa alla successiva. Ad esempio, alcune impostazioni hardening STIG potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire

l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

Per un elenco completo di Windows STIGs, consulta STIGs la Document Library. Per informazioni su come visualizzare l'elenco completo, consulta Strumenti di visualizzazione STIG.

- Windows Server 2025 STIG versione 1 versione 1

  V-278082, V-278083, V-278084, V-278085, V-278098, V-278104, V-278110 e V-278231
- Windows Server 2022 STIG versione 2 versione 7

  V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363 e V-254481
- Windows Server 2019 STIG versione 3 versione 7

  V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871 e V-205923
- Windows Server 2016 STIG versione 2 versione 10

  V-224916, V-224917, V-224918, V-224919, V-224931, V-224942 e V-225060
- Windows Server 2012 R2 MS STIG versione 3 versione 5

  V-225250, V-225318, V-225319, V-225324, V-225327, V-225328, V-225330, V-225331, V-225332, V-225333, V-225334, V-225335, V-225336, V-225342, V-225343, V-225355, V-225357, V-225358, V-225359, V-225360, V-225362, V-225363, V-225376, V-225392, V-225394, V-225412, V-225459, V-225460, V-225462, V-225468, V-225473, V-225476, V-225479, V-225480, V-225481, V-225482, V-225483, V-225484, V-225485, V-225487, V-225488, V-225489, V-225490, V-225511, V-225514, V-225525, V-225526, V-225536 e V-225537
- Microsoft.NET Framework 4.0 STIG Versione 2 Release 7

  Nessuna impostazione STIG viene applicata alle vulnerabilità di Microsoft .NET Framework per la categoria III.
- Windows Firewall STIG versione 2 versione 2

  V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007 e V-242008
- Internet Explorer 11 STIG versione 2 versione 6

  V-223056 e V-223078
- Microsoft Edge STIG versione 2 Release 4 (solo Windows Server 2022 e 2025)

V-235727, V-235731, V-235751, V-235752 e V-235765

STIG per Windows Medio (categoria II)

L'elenco seguente contiene le impostazioni STIG che Amazon EC2 supporta nella tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora la ignora e passa alla successiva. Ad esempio, alcune impostazioni hardening STIG potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

Per un elenco completo di Windows STIGs, consulta la STIGs Document Library. Per informazioni su come visualizzare l'elenco completo, consulta Strumenti di visualizzazione STIG.

> **Note**
>
> La categoria Medio di STIG per Windows include tutte le impostazioni di hardening STIG elencate che si applicano a STIG per Windows Basso (categoria III), oltre che alle impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria II.

- Windows Server 2025 STIG versione 1 versione 1

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

  V-278015, V-278016, V-278019, V-278020, V-278021, V-278022, V-278023, V-278024, V-278025, V-278026, V-278033, V-278034, V-278035, V-278036, V-278037, V-278038, V-278039, V-278047, V-278048, V-278049, V-278050, V-278051, V-278052, V-278053, V-278054, V-278055, V-278056, V-278057, V-278058, V-278059, V-278060, V-278061, V-278062, V-278063, V-278064, V-278065, V-278066, V-278067, V-278068, V-278069, V-278070, V-278071, V-278072, V-278073, V-278074, V-278075, V-278076, V-278077, V-278078, V-278079, V-278080, V-278086, V-278088, V-278089, V-278091, V-278092, V-278093, V-278094, V-278095, V-278096, V-278097, V-278102, V-278103, V-278105, V-278106, V-278107, V-278108, V-278109, V-278111, V-278112, V-278113, V-278114, V-278115, V-278116, V-278117, V-278118, V-278119, V-278120, V-278122, V-278123, V-278124, V-278126, V-278127, V-278129, V-278130, V-278131, V-278165, V-278168, V-278169, V-278170, V-278171, V-278174, V-278180, V-278181, V-278182, V-278183, V-278184, V-278185, V-278187, V-278188, V-278189, V-278192, V-278193, V-278194, V-278195, V-278198, V-278199, V-278200,

V-278201, V-278202, V-278203, V-278204, V-278205, V-278206, V-278209, V-278210, V-278211, V-278212, V-278213, V-278214, V-278218, V-278220, V-278221, V-278222, V-278223, V-278226, V-278227, V-278228, V-278229, V-278230, V-278232, V-278233, V-278234, V-278235, V-278236, V-278237, V-278238, V-278239, V-278240, V-278241, V-278243, V-278244, V-278245, V-278247, V-278248, V-278249, V-278251, V-278252, V-278253, V-278254, V-278255, V-278256, V-278257, V-278258, V-278259, V-278260, V-278261, V-278262, V-279916, V-279917, V-279918, V-279919, V-279920, V-279921, V-279922 e V-279923

- Windows Server 2022 STIG versione 2 versione 7

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

  V-254247, V-254269, V-254270, V-254271, V-254272, V-254273, V-254274, V-254275, V-254276, V-254277, V-254278, V-254285, V-254286, V-254287, V-254288, V-254289, V-254290, V-254291, V-254292, V-254296, V-254297, V-254298, V-254299, V-254300, V-254301, V-254302, V-254303, V-254304, V-254305, V-254307, V-254309, V-254311, V-254312, V-254313, V-254314, V-254315, V-254316, V-254319, V-254320, V-254321, V-254322, V-254323, V-254324, V-254325, V-254326, V-254327, V-254328, V-254329, V-254330, V-254341, V-254342, V-254333, V-254334, V-254339, V-254341, V-254342, V-254344, V-254345, V-254346, V-254347, V-254348, V-254349, V-254350, V-254355, V-254356, V-254358, V-254359, V-254360, V-254361, V-254362, V-254364, V-254366, V-254367, V-254368, V-254369, V-254370, V-254371, V-254372, V-254373, V-254375, V-254376, V-254377, V-254379, V-254380, V-254382, V-254383, V-254384, V-254431, V-254433, V-254434, V-254435, V-254436, V-254438, V-25254439, V-254440, V-254442, V-254443, V-254444, V-254445, V-254447, V-254448, V-254449, V-254450, V-254451, V-254452, V-254453, V-254454, V-254455, V-254456, V-254459, V-254460, V-254461, V-254462, V-254463, V-254464, V-254468, V-254470, V-254471, V-254472, V-254473, V-254476, V-254477, V-254478, V-254479, V-254480, V-254482, V-254483, V-254484, V-254485, V-254486, V-254487, V-254488, V-254489, V-254491, V-254493, V-254494, V-254495, V-254497, V-254498, V-254499, V-254501, V-254502, V-254503, V-254504, V-254505, V-254506, V-254507, V-254508, V-254509, V-254510, V-254511, V-254512, V-278942, V-278943, V-278944, V-278945, V-278946, V-278947, V-278948 e V-278949

- Windows Server 2019 STIG versione 3 versione 7

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

  V-205625, V-205626, V-205627, V-205629, V-205630, V-205633, V-205634, V-205635, V-205636, V-205637, V-205638, V-205639, V-205640, V-205641, V-205642, V-205643, V-205644, V-205648,

V-205649, V-205650, V-205651, V-205652, V-205655, V-205656, V-205659, V-205660, V-205662, V-205671, V-205672, V-205673, V-205675, V-205676, V-205678, V-205679, V-205680, V-205681, V-205682, V-205683, V-205683, V-205683, V-205683 V-205684, V-205685, V-205686, V-205687, V-205688, V-205689, V-205690, V-205692, V-205693, V-205694, V-205697, V-205698, V-205708, V-205709, V-205712, V-205714, V-205716, V-205717, V-205718, V-205719, V-205720, V-205722, V-205730, V-205731, V-205733, V-205747, V-205748, V-205749, V-205751, V-205752, V-205754, V-205755, V-205756, V-205758, V-205759, V-205760, V-205761, V-205762, V-205763, V-205764, V-205765, V-205766, V-205767, V-205768, V-205769, V-205770, V-205771, V-205772, V-205773, V-205774, V-205775, V-205776, V-205777, V-205778, V-205779, V-205780, V-205782051, V-205778 V-205783, V-205784, V-205795, V-205796, V-205797, V-205798, V-205801, V-205808, V-205809, V-205810, V-205811, V-205812, V-205813, V-205814, V-205815, V-205816, V-205817, V-205821, V-205822, V-205823, V-205824, V-205825, V-205826, V-205827, V-205828, V-205830, V-205832, V-205833, V-205835, V-205836, V-205837, V-205838, V-205842, V-205861, V-205863, V-205865, V-205866, V-205867, V-205868, V-205869, V-205872, V-205873, V-205874, V-205909, V-205910, V-205911, V-205912, V-205915, V-205916, V-205917, V-205918, V-205920, V-205921, V-205922, V-205925, V-257503, V-278934, V-278935, V-278936, V-278937, V-278938, V-278939, V-278940 e V-278941

- Windows Server 2016 STIG versione 2 versione 10

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

  V-224850, V-224851, V-224852, V-224853, V-224854, V-224855, V-224856, V-224857, V-224858, V-224859, V-224866, V-224867, V-224868, V-224869, V-224870, V-224871, V-224872, V-224873, V-224877, V-224878, V-224879, V-224880, V-224881, V-224882, V-224883, V-224884, V-224885, V-224886, V-224888, V-224890, V-224892, V-224893, V-224894, V-224895, V-224896, V-224897, V-224900, V-224901, V-224902, V-224903, V-224904, V-224905, V-224906, V-224907, V-224908, V-224909, V-224910, V-224911, V-224912, V-224913, V-224914, V-224915, V-224920, V-224921, V-224922, V-224924, V-224925, V-224926, V-224927, V-224928, V-224929, V-224930, V-224935, V-224936, V-224937, V-224938, V-224939, V-224940, V-224941, V-224943, V-224944, V-224945, V-224946, V-224947, V-224948, V-224949, V-224951, V-224952, V-224953, V-224955, V-224956, V-224957, V-224959, V-224960, V-224962, V-224963, V-224965, V-224966, V-224967, V-224968, V-224969, V-224987, V-224988, V-224989, V-224995, V-224996, V-224997, V-224998, V-224999, V-225000, V-225001, V-225002, V-225003, V-225004, V-225005, V-225008, V-225009, V-225010, V-225011, V-225013, V-225014, V-225015, V-225016, V-225017, V-225018, V-225019, V-225020, V-225021, V-225022, V-225023, V-225024, V-225026, V-225027, V-225028, V-225029, V-225030, V-225031, V-225032, V-225033, V-225034, V-225035, V-225038, V-225039, V-225040, V-225041,

V-225042, V-225043, V-225047, V-225049, V-225050, V-225051, V-225052, V-225055, V-225056, V-225057, V-225058, V-225059, V-225061, V-225062, V-225063, V-225064, V-225065, V-225066, V-225067, V-225068, V-225070, V-225072, V-225073, V-225074, V-225076, V-225077, V-225078, V-225080, V-225081, V-225082, V-225083, V-225084, V-225085, V-225086, V-225087, V-225088, V-225089, V-225092, V-225093 e V-257502

- Windows Server 2012 R2 MS STIG versione 3 versione 5

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

  V-225239, V-225259, V-225260, V-225261, V-225263, V-225264, V-225265, V-225266, V-225267, V-225268, V-225269, V-225270, V-225271, V-225272, V-225273, V-225275, V-225276, V-225277, V-225278, V-225279, V-225280, V-225281, V-225282, V-225283, V-225284, V-225285, V-225286, V-225287, V-225288, V-225289, V-225290, V-225291, V-225292, V-225293, V-225294, V-225295, V-225296, V-225297, V-225298, V-225299, V-225300, V-225301, V-225302, V-225303, V-225304, V-225305, V-225314, V-225315, V-225316, V-225317, V-225325, V-225326, V-225329, V-225337, V-225338, V-225339, V-225340, V-225341, V-225344, V-225345, V-225346, V-225347, V-225348, V-225349, V-225350, V-225351, V-225352, V-225353, V-225356, V-225367, V-225368, V-225369, V-225370, V-225371, V-225372, V-225373, V-225374, V-225375, V-225377, V-225378, V-225379, V-225380, V-225381, V-225382, V-225383, V-225384, V-225385, V-225386, V-225389, V-225391, V-225393, V-225395, V-225397, V-225398, V-225400, V-225401, V-225402, V-225404, V-225405, V-225406, V-225407, V-225408, V-225409, V-225410, V-225411, V-225413, V-225414, V-225415, V-225441, V-225442, V-225443, V-225448, V-225452, V-225453, V-225454, V-225455, V-225456, V-225457, V-225458, V-225461, V-225463, V-225464, V-225469, V-225470, V-225471, V-225472, V-225474, V-225475, V-225477, V-225478, V-225486, V-225494, V-225500, V-225501, V-225502, V-225503, V-225504, V-225506, V-225508, V-225509, V-225510, V-225513, V-225515, V-225516, V-225517, V-225518, V-225519, V-225520, V-225521, V-225522, V-225523, V-225524, V-225527, V-225528, V-225529, V-225530, V-225531, V-225532, V-225533, V-225534, V-225535, V-225538, V-225539, V-225540, V-225541, V-225542, V-225543, V-225544, V-225545, V-225546, V-225548, V-225549, V-225550, V-225551, V-225553, V-225554, V-225555, V-225557, V-225558, V-225559, V-225560, V-225561, V-225562, V-225563, V-225564, V-225565, V-225566, V-225567, V-225568, V-225569, V-225570, V-225571, V-225572, V-225573 e V-225574

- Microsoft.NET Framework 4.0 STIG Versione 2 Release 7

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

V-225223, V-225230, V-225235 e V-225238

- Windows Firewall STIG versione 2 versione 2

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

  V-241989, V-241990, V-241991, V-241993, V-241998, V-242003, V-242004 e V-242005

- Internet Explorer 11 STIG versione 2 versione 6

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

  V-223015, V-223017, V-223018, V-223019, V-223020, V-223021, V-223022, V-223023, V-223024, V-223025, V-223026, V-223027, V-223028, V-223029, V-223030, V-223031, V-223032, V-223033, V-223034, V-223035, V-223036, V-223037, V-223038, V-223039, V-223040, V-223041, V-223042, V-223043, V-223044, V-223045, V-223046, V-223048, V-223049, V-223050, V-223051, V-223052, V-223053, V-223054, V-223055, V-223057, V-223058, V-223059, V-223060, V-223061, V-223062, V-223063, V-223064, V-223065, V-223066, V-223067, V-223068, V-223069, V-223070, V-223071, V-223072, V-223073, V-223074, V-223075, V-223076, V-223077, V-223079, V-223080, V-223081, V-223082, V-223083, V-223084, V-223085, V-223086, V-223087, V-223088, V-223089, V-223090, V-223091, V-223092, V-223093, V-223094, V-223095, V-223096, V-223097, V-223098, V-223099, V-223100, V-223101, V-223102, V-223103, V-223104, V-223105, V-223106, V-223107, V-223108, V-223109, V-223110, V-223111, V-223112, V-223113, V-223114, V-223115, V-223116, V-223117, V-223118, V-223119, V-223120, V-223121, V-223123, V-223125, V-223126, V-223127, V-223128, V-223129, V-223130, V-223131, V-223132, V-223133, V-224313, V-223135, V-223136, V-223137, V-223138, V-223139, V-223140, V-223141, V-223142, V-223143, V-223144, V-223145, V-223146, V-223147, V-223148, V-223149, V-250540 e V-250541

- Microsoft Edge STIG versione 2 Release 4 (solo Windows Server 2022 e 2025)

  V-235720, V-235721, V-235723, V-235724, V-235725, V-235726, V-235728, V-235729, V-235730, V-235732, V-235733, V-235734, V-235735, V-235736, V-235737, V-235738, V-235739, V-235740, V-235741, V-235742, V-235743, V-235744, V-235745, V-235746, V-235747, V-235748, V-235749, V-235750, V-235754, V-235756, V-235760, V-235761, V-235763, V-235764, V-235766, V-235767, V-235768, V-235769, V-235770, V-235771, V-235772, V-235773, V-235774 e V-246736

- Microsoft Defender STIG Versione 2 Release 7

Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria III (Basso), oltre a:

V-213427, V-213429, V-213430, V-213431, V-213432, V-213433, V-213434, V-213435, V-213436, V-213437, V-213438, V-213439, V-213440, V-213441, V-213442, V-213443, V-213444, V-213445, V-213446, V-213447, V-213448, V-213449, V-213450, V-213451, V-213454, V-213455, V-213456, V-213457, V-213458, V-213459, V-213460, V-213461, V-213461, V-213461, V-213461, V-213461 2, V-213463, V-213464, V-213465, V-213466, V-278647, V-278648, V-278649, V-278650, V-278651, V-278652, V-278653, V-278654, V-278655, V-278656, V-278658, V-278659, V-278660, V-278661, V-278662, V-278668, V-278669, V-278672, V-278674, V-278675, V-278676, V-278677, V-278678, V-278679, V-278680 e V-278863

STIG per Windows Alto (categoria I)

L'elenco seguente contiene le impostazioni STIG che Amazon EC2 supporta nella tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora la ignora e passa alla successiva. Ad esempio, alcune impostazioni hardening STIG potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

Per un elenco completo di Windows, consulta la STIGs Document Library. STIGs Per informazioni su come visualizzare l'elenco completo, consulta Strumenti di visualizzazione STIG.

> **Note**
>
> La categoria Alto di STIG per Windows include tutte le impostazioni di hardening STIG elencate che si applicano a STIG per Windows Medio e Basso, oltre che alle impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità di categoria I.

- Windows Server 2025 STIG versione 1 versione 1

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

  V-278040, V-278099, V-278100, V-278101, V-278121, V-278125, V-278128, V-278196, V-278215, V-278216, V-278217, V-278219, V-278225, V-278242, V-278246 e V-278250

- Windows Server 2022 STIG versione 2 versione 7

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

  V-254250, V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254466, V-254467, V-254469, V-254474, V-254475, V-254492, V-254496 e V-254500
- Windows Server 2019 STIG versione 3 versione 7

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

  V-205653, V-205654, V-205663, V-205711, V-205713, V-205724, V-205725, V-205750, V-205753, V-205757, V-205802, V-205804, V-205805, V-205806, V-205849, V-205908, V-205914 e V-205919
- Windows Server 2016 STIG versione 2 versione 10

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

  V-224831, V-224874, V-224932, V-224933, V-224934, V-224954, V-224958, V-224961, V-225025, V-225045, V-225046, V-225048, V-225053, V-225054, V-225071, V-225079 e V-225091
- Windows Server 2012 R2 MS STIG versione 3 versione 5

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

  V-225274, V-225354, V-225364, V-225365, V-225366, V-225390, V-225396, V-225399, V-225444, V-225449, V-225491, V-225492, V-225493, V-225496, V-225497, V-225498, V-225505, V-225507, V-225547, V-225552 e V-225556
- Microsoft.NET Framework 4.0 STIG Versione 2 Release 7

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso) per Microsoft .NET Framework. Non si applicano impostazioni STIG aggiuntive per le vulnerabilità di categoria I.
- Windows Firewall STIG versione 2 versione 2

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

V-241992, V-241997 e V-242002

- Internet Explorer 11 STIG versione 2 versione 6

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

  V-252910

- Microsoft Edge STIG versione 2 Release 4 (solo Windows Server 2022 e 2025)

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

  V-235758 e V-235759

- Microsoft Defender STIG Versione 2 Release 7

  Include tutte le impostazioni di hardening STIG supportate da Amazon EC2 per le vulnerabilità delle categorie II e III (Medio e Basso), oltre a:

  V-213426, V-213428, V-213452 e V-213453

Download di script di hardening STIG

Per ogni versione, Amazon raggruppa gli script di hardening STIG in bundle relativi al sistema operativo. I bundle sono file di archivio appropriati per il sistema operativo di destinazione in cui vengono scaricati ed eseguiti. I bundle di script Linux vengono archiviati come file TAR (estensione.tgz). I bundle di script Windows vengono archiviati come file ZIP (estensione.zip).

Amazon archivia i bundle di script nel bucket `STIG` di EC2 Windows S3 in ogni Regione AWS. I bundle Linux non dispongono di un bucket separato. Da utilizzare per SSL/TLS comunicare con le AWS risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.

Argomenti

- Dettagli del bundle di download STIG
- Cronologia delle versioni STIG per Linux
- Cronologia delle versioni STIG di Windows

Dettagli del bundle di download STIG

> **Important**
>
> A parte poche eccezioni, gli script di hardening STIG scaricati dal documento Systems Manager non installano pacchetti di terzi. Se sull'istanza sono già installati pacchetti di terzi o il parametro `InstallPackage` è impostato su `yes`, vengono applicati STIG correlati supportati da Amazon EC2 per quel pacchetto.

Quando esegui il seguente comando da AWS CLI, Amazon S3 scarica il file bundle di script di hardening STIG più recente dal bucket.

```
aws s3 cp s3://aws-windows-downloads-region/STIG/operating system/Latest/bundle-name destination-directory
```

Esempio: scarica in una directory temporanea

Questo esempio mostra un bundle Linux che viene scaricato nella directory `/tmp`

```
aws s3 cp s3://aws-windows-downloads-us-east-1/STIG/Linux/
Latest/LinuxAWSConfigureSTIG.tgz /tmp
```

I modelli e gli esempi per i percorsi di archiviazione dei file scaricati e i nomi dei file dei bundle sono i seguenti:

Scarica il percorso di archiviazione dei file

`s3://aws-windows-downloads-<region>/STIG/<operating system>/Latest/<bundle file name>`

Scarica le variabili di percorso

region

Regione AWS (Ogni regione ha il proprio bucket di download.)

operating system

La piattaforma del sistema operativo dell'istanza in cui STIGs vengono applicate, `Linux` o`Windows`.

bundle file name

Il formato è*<os bundle name>*.*<file extension>*.

os bundle name

Il nome standard del prefisso per il pacchetto del sistema operativo è `LinuxAWSConfigureSTIG` o `AWSConfigureSTIG`. Per mantenere la compatibilità con le versioni precedenti, il download per Windows non include un prefisso di piattaforma.

file extension

Formato di file compresso `tgz` (Linux) o `zip` (Windows).

Esempi di nomi di file bundle

- `LinuxAWSConfigureSTIG.tgz`
- `AWSConfigureSTIG.zip`

Cronologia delle versioni STIG per Linux

Questa sezione registra la cronologia delle versioni per i bundle di script Linux che vengono aggiornati trimestralmente. Per visualizzare le modifiche e le versioni pubblicate per un trimestre, scegli il titolo per espandere le informazioni. Se non ci sono modifiche per il trimestre, lo vedrai nel titolo.

Modifiche al 1° trimestre 2026 - 04/07/2026:

È stato aggiunto il supporto per il sistema operativo RHEL 10 e aggiornato le seguenti versioni STIG e applicato STIGS per la versione del primo trimestre 2026 per tutti i livelli di conformità (): low/medium/high

STIG-Build-Linux versione 1.0.x

- RHEL 8 STIG versione 2 versione 6
- RHEL 9 STIG versione 2 versione 7
- RHEL 10 STIG versione 1 versione 1
- Amazon Linux 2023 STIG versione 1 versione 2
- SLES 12 STIG versione 3 versione 4
- SLES 15 STIG versione 2 versione 6

- Ubuntu 20.04 STIG versione 2 versione 4
- Ubuntu 22.04 STIG versione 2 Release 7
- Ubuntu 24.04 STIG versione 1 versione 4

Modifiche al terzo trimestre 2025 - 04/09/2025:

È stato aggiunto il supporto per il sistema operativo SUSE Linux Enterprise Server (SLES) e Amazon Linux 2023. Sono state aggiornate le seguenti versioni di STIG e applicato STIGS per la versione del terzo trimestre 2025 per tutti i livelli di conformità (): low/medium/high

STIG-Build-Linux versione 1.0.x

- RHEL 7 STIG versione 3 rilascio 15
- RHEL 8 STIG versione 2 rilascio 4
- RHEL 9 STIG versione 2 rilascio 5
- Amazon Linux 2023 STIG versione 1 rilascio 1
- SLES 12 STIG versione 3 rilascio 3
- SLES 15 STIG versione 2 rilascio 5
- Ubuntu 18.04 STIG versione 2 rilascio 15
- Ubuntu 20.04 STIG versione 2 rilascio 3
- Ubuntu 22.04 STIG versione 2 rilascio 5
- Ubuntu 24.04 STIG versione 1 rilascio 2

Modifiche al secondo trimestre 2025 - 26/06/2025:

Sono state aggiornate le versioni STIG seguenti, sono stati applicati STIG per il rilascio del secondo trimestre 2025:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 15
- RHEL 8 STIG versione 2 rilascio 3
- RHEL 9 STIG versione 2 rilascio 4
- Ubuntu 18.04 STIG versione 2 rilascio 15

- Ubuntu 20.04 STIG versione 2 rilascio 2
- Ubuntu 22.04 STIG versione 2 rilascio 4
- Ubuntu 24.04 STIG versione 1 rilascio 1

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 15
- RHEL 8 STIG versione 2 rilascio 3
- RHEL 9 STIG versione 2 rilascio 4
- Ubuntu 18.04 STIG versione 2 rilascio 15
- Ubuntu 20.04 STIG versione 2 rilascio 2
- Ubuntu 22.04 STIG versione 2 rilascio 4
- Ubuntu 24.04 STIG versione 1 rilascio 1

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 15
- RHEL 8 STIG versione 2 rilascio 3
- RHEL 9 STIG versione 2 rilascio 4
- Ubuntu 18.04 STIG versione 2 rilascio 15
- Ubuntu 20.04 STIG versione 2 rilascio 2
- Ubuntu 22.04 STIG versione 2 rilascio 4
- Ubuntu 24.04 STIG versione 1 rilascio 1

Modifiche al terzo trimestre 2025 - 11/04/2025:

Sono state aggiornate le seguenti versioni di STIG, sono stati applicati STIG per il rilascio del primo trimestre 2025 ed è stato aggiunto il supporto per Ubuntu 24.04:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 15
- RHEL 8 STIG versione 2 rilascio 2
- RHEL 9 STIG versione 2 rilascio 3

- Ubuntu 18.04 STIG versione 2 rilascio 15
- Ubuntu 20.04 STIG versione 2 rilascio 2
- Ubuntu 22.04 STIG versione 2 rilascio 3
- Ubuntu 24.04 STIG versione 1 rilascio 1

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 15
- RHEL 8 STIG versione 2 rilascio 2
- RHEL 9 STIG versione 2 rilascio 3
- Ubuntu 18.04 STIG versione 2 rilascio 15
- Ubuntu 20.04 STIG versione 2 rilascio 2
- Ubuntu 22.04 STIG versione 2 rilascio 3
- Ubuntu 24.04 STIG versione 1 rilascio 1

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 15
- RHEL 8 STIG versione 2 rilascio 2
- RHEL 9 STIG versione 2 rilascio 3
- Ubuntu 18.04 STIG versione 2 rilascio 15
- Ubuntu 20.04 STIG versione 2 rilascio 2
- Ubuntu 22.04 STIG versione 2 rilascio 3
- Ubuntu 24.04 STIG versione 1 rilascio 1

Modifiche al quarto trimestre 2024 - 10/12/2024:

Sono state aggiornate le seguenti versioni di STIG, sono stati applicati STIG per il rilascio del quarto trimestre 2024 e sono state aggiunte informazioni su due nuovi parametri di input per i componenti Linux:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 15

- RHEL 8 STIG versione 2 rilascio 1
- RHEL 9 STIG versione 2 rilascio 2
- Ubuntu 18.04 STIG versione 2 rilascio 15
- Ubuntu 20.04 STIG versione 2 rilascio 1
- Ubuntu 22.04 STIG versione 2 rilascio 2

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 15
- RHEL 8 STIG versione 2 rilascio 1
- RHEL 9 STIG versione 2 rilascio 2
- Ubuntu 18.04 STIG versione 2 rilascio 15
- Ubuntu 20.04 STIG versione 2 rilascio 1
- Ubuntu 22.04 STIG versione 2 rilascio 2

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 15
- RHEL 8 STIG versione 2 rilascio 1
- RHEL 9 STIG versione 2 rilascio 2
- Ubuntu 18.04 STIG versione 2 rilascio 15
- Ubuntu 20.04 STIG versione 2 rilascio 1
- Ubuntu 22.04 STIG versione 2 rilascio 2

Modifiche al terzo trimestre 2024 - 04/10/2024 (nessuna modifica):

Non sono state apportate modifiche al componente STIG per Linux per il rilascio del terzo trimestre 2024.

Modifiche al secondo trimestre 2024 - 10/05/2024:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del secondo trimestre 2024. È stato inoltre aggiunto il supporto per RHEL 9, CentOS Stream 9 e Ubuntu 22.04, come segue:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 14
- RHEL 8 STIG versione 1 rilascio 14
- RHEL 9 STIG versione 1 rilascio 3
- Ubuntu 18.04 STIG versione 2 rilascio 14
- Ubuntu 20.04 STIG versione 1 rilascio 12
- Ubuntu 22.04 STIG versione 1 rilascio 1

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 14
- RHEL 8 STIG versione 1 rilascio 14
- RHEL 9 STIG versione 1 rilascio 3
- Ubuntu 18.04 STIG versione 2 rilascio 14
- Ubuntu 20.04 STIG versione 1 rilascio 12
- Ubuntu 22.04 STIG versione 1 rilascio 1

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 14
- RHEL 8 STIG versione 1 rilascio 14
- RHEL 9 STIG versione 1 rilascio 3
- Ubuntu 18.04 STIG versione 2 rilascio 14
- Ubuntu 20.04 STIG versione 1 rilascio 12
- Ubuntu 22.04 STIG versione 1 rilascio 1

Modifiche al primo trimestre 2024 - 06/02/2024:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del primo trimestre 2024 come segue:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 14

- RHEL 8 STIG versione 1 rilascio 13
- Ubuntu 18.04 STIG versione 2 rilascio 13
- Ubuntu 20.04 STIG versione 1 rilascio 11

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 14
- RHEL 8 STIG versione 1 rilascio 13
- Ubuntu 18.04 STIG versione 2 rilascio 13
- Ubuntu 20.04 STIG versione 1 rilascio 11

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 14
- RHEL 8 STIG versione 1 rilascio 13
- Ubuntu 18.04 STIG versione 2 rilascio 13
- Ubuntu 20.04 STIG versione 1 rilascio 11

Modifiche al quarto trimestre 2023 - 07/12/2023:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del quarto trimestre 2023 come segue:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 13
- RHEL 8 STIG versione 1 rilascio 12
- Ubuntu 18.04 STIG versione 2 rilascio 12
- Ubuntu 20.04 STIG versione 1 rilascio 10

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 13
- RHEL 8 STIG versione 1 rilascio 12

- Ubuntu 18.04 STIG versione 2 rilascio 12
- Ubuntu 20.04 STIG versione 1 rilascio 10

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 13
- RHEL 8 STIG versione 1 rilascio 12
- Ubuntu 18.04 STIG versione 2 rilascio 12
- Ubuntu 20.04 STIG versione 1 rilascio 10

Modifiche al terzo trimestre 2023 - 04/10/2023:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del terzo trimestre 2023 come segue:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 12
- RHEL 8 STIG versione 1 rilascio 11
- Ubuntu 18.04 STIG versione 2 rilascio 11
- Ubuntu 20.04 STIG versione 1 rilascio 9

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 12
- RHEL 8 STIG versione 1 rilascio 11
- Ubuntu 18.04 STIG versione 2 rilascio 11
- Ubuntu 20.04 STIG versione 1 rilascio 9

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 12
- RHEL 8 STIG versione 1 rilascio 11
- Ubuntu 18.04 STIG versione 2 rilascio 11
- Ubuntu 20.04 STIG versione 1 rilascio 9

Modifiche al secondo trimestre 2023 - 03/05/2023:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del secondo trimestre 2023 come segue:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 11
- RHEL 8 STIG versione 1 rilascio 10
- Ubuntu 18.04 STIG versione 2 rilascio 11
- Ubuntu 20.04 STIG versione 1 rilascio 8

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 11
- RHEL 8 STIG versione 1 rilascio 10
- Ubuntu 18.04 STIG versione 2 rilascio 11
- Ubuntu 20.04 STIG versione 1 rilascio 8

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 11
- RHEL 8 STIG versione 1 rilascio 10
- Ubuntu 18.04 STIG versione 2 rilascio 11
- Ubuntu 20.04 STIG versione 1 rilascio 8

Modifiche al primo trimestre 2023 - 27/03/2023:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del primo trimestre 2023 come segue:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 10
- RHEL 8 STIG versione 1 rilascio 9
- Ubuntu 18.04 STIG versione 2 rilascio 10

- Ubuntu 20.04 STIG versione 1 rilascio 7

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 10
- RHEL 8 STIG versione 1 rilascio 9
- Ubuntu 18.04 STIG versione 2 rilascio 10
- Ubuntu 20.04 STIG versione 1 rilascio 7

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 10
- RHEL 8 STIG versione 1 rilascio 9
- Ubuntu 18.04 STIG versione 2 rilascio 10
- Ubuntu 20.04 STIG versione 1 rilascio 7

Modifiche al quarto trimestre 2022 - 01/02/2023:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del quarto trimestre 2022 come segue:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 9
- RHEL 8 STIG versione 1 rilascio 8
- Ubuntu 18.04 STIG versione 2 rilascio 9
- Ubuntu 20.04 STIG versione 1 rilascio 6

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 9
- RHEL 8 STIG versione 1 rilascio 8
- Ubuntu 18.04 STIG versione 2 rilascio 9
- Ubuntu 20.04 STIG versione 1 rilascio 6

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 9
- RHEL 8 STIG versione 1 rilascio 8
- Ubuntu 18.04 STIG versione 2 rilascio 9
- Ubuntu 20.04 STIG versione 1 rilascio 6

Modifiche al terzo trimestre 2022 - 30/09/2022 (nessuna modifica):

Non sono state apportate modifiche al componente STIG per Linux per il rilascio del terzo trimestre 2022.

Modifiche al secondo trimestre 2022 - 02/08/2022:

È stato introdotto il supporto a Ubuntu, sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del secondo trimestre 2022 come segue:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 7
- RHEL 8 STIG versione 1 rilascio 6
- Ubuntu 18.04 STIG versione 2 rilascio 6 (nuova)
- Ubuntu 20.04 STIG versione 1 rilascio 4 (nuova)

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 7
- RHEL 8 STIG versione 1 rilascio 6
- Ubuntu 18.04 STIG versione 2 rilascio 6 (nuova)
- Ubuntu 20.04 STIG versione 1 rilascio 4 (nuova)

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 7
- RHEL 8 STIG versione 1 rilascio 6
- Ubuntu 18.04 STIG versione 2 rilascio 6 (nuova)

- Ubuntu 20.04 STIG versione 1 rilascio 4 (nuova)

Modifiche al primo trimestre 2022 - 26/04/2022:

Rifattorizzato per includere un migliore supporto per i container. Combinato lo AL2 script precedente con RHEL 7. Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del primo trimestre 2022 come segue:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 6
- RHEL 8 STIG versione 1 rilascio 5

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 6
- RHEL 8 STIG versione 1 rilascio 5

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 6
- RHEL 8 STIG versione 1 rilascio 5

Modifiche al quarto trimestre 2021 - 20/12/2021:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del quarto trimestre 2021 come segue:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 5
- RHEL 8 STIG versione 1 rilascio 4

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 5
- RHEL 8 STIG versione 1 rilascio 4

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 5
- RHEL 8 STIG versione 1 rilascio 4

Modifiche al terzo trimestre 2021 - 30/09/2021:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del terzo trimestre 2021 come segue:

STIG per Linux Basso (categoria III)

- RHEL 7 STIG versione 3 rilascio 4
- RHEL 8 STIG versione 1 rilascio 3

STIG per Linux Medio (categoria II)

- RHEL 7 STIG versione 3 rilascio 4
- RHEL 8 STIG versione 1 rilascio 3

STIG per Linux Alto (categoria I)

- RHEL 7 STIG versione 3 rilascio 4
- RHEL 8 STIG versione 1 rilascio 3

Cronologia delle versioni STIG di Windows

Questa sezione registra la cronologia delle versioni per i bundle di script Windows che vengono aggiornati trimestralmente. Per visualizzare le modifiche e le versioni pubblicate per un trimestre, scegli il titolo per espandere le informazioni. Se non ci sono modifiche per il trimestre, lo vedrai nel titolo.

Modifiche al primo trimestre 2026 - 04/07/2026:

Aggiunto il supporto per il sistema operativo Windows Server 2025, aggiornamento delle seguenti versioni STIG e applicazione di STIGS per la versione del primo trimestre 2026 per tutti i livelli di conformità (): low/medium/high

STIG-Build-Windows versione 1.0.x

- Windows Server 2025 STIG versione 1 versione 1
- Windows Server 2022 STIG versione 2 versione 7
- Windows Server 2019 STIG versione 3 versione 7
- Microsoft.NET Framework 4.0 STIG Versione 2 Release 7
- Windows Firewall STIG versione 2 versione 2
- Internet Explorer 11 STIG versione 2 versione 6
- Microsoft Edge STIG versione 2 Release 4 (solo Windows Server 2022 e 2025)

Modifiche al quarto trimestre 2025 - 12/10/2025 (nessuna modifica):

Non sono state apportate modifiche al componente Windows STIGS per la versione del quarto trimestre 2025.

Modifiche al terzo trimestre 2025 - 04/09/2025 (nessuna modifica):

Non sono state apportate modifiche al componente STIG per Windows per il rilascio del terzo trimestre 2025.

Modifiche al secondo trimestre 2025 - 26/06/2025:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del secondo trimestre 2025 come segue:

STIG per Windows Basso (categoria III)

- Windows Server 2022 STIG versione 2 versione 4
- Windows Server 2019 STIG versione 3 rilascio 4
- Windows Server 2016 STIG versione 2 versione 10
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 6
- Windows Firewall STIG versione 2 versione 2
- Internet Explorer 11 STIG versione 2 versione 5
- Microsoft Edge STIG versione 2 rilascio 2 (solo per Windows Server 2022)

STIG per Windows Medio (categoria II)

- Windows Server 2022 STIG versione 2 versione 4
- Windows Server 2019 STIG versione 3 rilascio 4
- Windows Server 2016 STIG versione 2 versione 10
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 6
- Windows Firewall STIG versione 2 versione 2
- Internet Explorer 11 STIG versione 2 versione 5
- Microsoft Edge STIG versione 2 rilascio 2 (solo per Windows Server 2022)
- Defender STIG versione 2 rilascio 4

STIG per Windows Alto (categoria I)

- Windows Server 2022 STIG versione 2 versione 4
- Windows Server 2019 STIG versione 3 rilascio 4
- Windows Server 2016 STIG versione 2 versione 10
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 6
- Windows Firewall STIG versione 2 versione 2
- Internet Explorer 11 STIG versione 2 versione 5
- Microsoft Edge STIG versione 2 rilascio 2 (solo per Windows Server 2022)
- Defender STIG versione 2 rilascio 4

Modifiche al primo trimestre 2025 - 04/05/2025:

Sono stati aggiornati gli STIG per Internet Explorer 11 STIG versione 2 rilascio 5 per tutti i componenti STIG per la versione del primo trimestre 2025.

Modifiche al quarto trimestre 2024 - 10/12/2024:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del quarto trimestre 2024 come segue:

STIG per Windows Basso (categoria III)

- Windows Server 2022 STIG versione 2 versione 2
- Windows Server 2019 STIG versione 3 rilascio 2
- Windows Server 2016 STIG versione 2 versione 9
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 2
- Windows Firewall STIG versione 2 versione 2
- Internet Explorer 11 STIG versione 2 versione 5
- Microsoft Edge STIG versione 2 rilascio 2 (solo per Windows Server 2022)

STIG per Windows Medio (categoria II)

- Windows Server 2022 STIG versione 2 versione 2
- Windows Server 2019 STIG versione 3 rilascio 2
- Windows Server 2016 STIG versione 2 versione 9
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 2
- Windows Firewall STIG versione 2 versione 2
- Internet Explorer 11 STIG versione 2 versione 5
- Microsoft Edge STIG versione 2 rilascio 2 (solo per Windows Server 2022)
- Defender STIG versione 2 rilascio 4

STIG per Windows Alto (categoria I)

- Windows Server 2022 STIG versione 2 versione 2
- Windows Server 2019 STIG versione 3 rilascio 2
- Windows Server 2016 STIG versione 2 versione 9
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 2
- Windows Firewall STIG versione 2 versione 2
- Internet Explorer 11 STIG versione 2 versione 5

- Microsoft Edge STIG versione 2 rilascio 2 (solo per Windows Server 2022)
- Defender STIG versione 2 rilascio 4

Modifiche al terzo trimestre 2024 - 04/10/2024 (nessuna modifica):

Non sono state apportate modifiche al componente STIG per Windows per il rilascio del terzo trimestre 2024.

Modifiche al secondo trimestre 2024 - 10/05/2024 (nessuna modifica):

Non sono state apportate modifiche al componente STIG per Windows per il rilascio del secondo trimestre 2024.

Modifiche al primo trimestre 2024 - 23/02/2024 (nessuna modifica):

Non sono state apportate modifiche al componente STIG per Windows per il rilascio del primo trimestre 2024.

Modifiche al quarto trimestre 2023 - 07/12/2023 (nessuna modifica):

Non sono state apportate modifiche al componente STIG per Windows per il rilascio del quarto trimestre 2023.

Modifiche al terzo trimestre 2023 - 04/10/2023 (nessuna modifica):

Non sono state apportate modifiche al componente STIG per Windows per il rilascio del terzo trimestre 2023.

Modifiche al secondo trimestre 2023 - 03/05/2023 (nessuna modifica):

Non sono state apportate modifiche al componente STIG per Windows per il rilascio del secondo trimestre 2023.

Modifiche al primo trimestre 2023 - 27/03/2023 (nessuna modifica):

Non sono state apportate modifiche al componente STIG per Windows per il rilascio del primo trimestre 2023.

Modifiche al quarto trimestre 2022 - 01/02/2023:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del quarto trimestre 2022 come segue:

STIG per Windows Basso (categoria III)

- Windows Server 2022 STIG versione 1 rilascio 1
- Windows Server 2019 STIG versione 2 rilascio 5
- Windows Server 2016 STIG versione 2 rilascio 5
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 2
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 2 rilascio 3
- Microsoft Edge STIG versione 1 rilascio 6 (solo per Windows Server 2022)

STIG per Windows Medio (categoria II)

- Windows Server 2022 STIG versione 1 rilascio 1
- Windows Server 2019 STIG versione 2 rilascio 5
- Windows Server 2016 STIG versione 2 rilascio 5
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 2
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 2 rilascio 3
- Microsoft Edge STIG versione 1 rilascio 6 (solo per Windows Server 2022)
- Defender STIG versione 2 rilascio 4 (solo per Windows Server 2022)

STIG per Windows Alto (categoria I)

- Windows Server 2022 STIG versione 1 rilascio 1
- Windows Server 2019 STIG versione 2 rilascio 5
- Windows Server 2016 STIG versione 2 rilascio 5
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 2
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 2 rilascio 3

- Microsoft Edge STIG versione 1 rilascio 6 (solo per Windows Server 2022)
- Defender STIG versione 2 rilascio 4 (solo per Windows Server 2022)

Modifiche al terzo trimestre 2022 - 30/09/2022 (nessuna modifica):

Non sono state apportate modifiche al componente STIG per Windows per il rilascio del terzo trimestre 2022.

Modifiche al secondo trimestre 2022 - 02/08/2022:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del secondo trimestre 2022.

STIG per Windows Basso (categoria III)

- Windows Server 2019 STIG versione 2 versione 4
- Windows Server 2016 STIG versione 2 versione 4
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 1
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 1 versione 19

STIG per Windows Medio (categoria II)

- Windows Server 2019 STIG versione 2 versione 4
- Windows Server 2016 STIG versione 2 versione 4
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 1
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 1 versione 19

STIG per Windows Alto (categoria I)

- Windows Server 2019 STIG versione 2 versione 4
- Windows Server 2016 STIG versione 2 versione 4
- Windows Server 2012 R2 MS STIG versione 3 versione 3

- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 1
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 1 versione 19

Modifiche al primo trimestre 2022 - 02/08/2022 (nessuna modifica):

Non sono state apportate modifiche al componente STIG per Windows per il rilascio del primo trimestre 2022.

Modifiche al quarto trimestre 2021 - 20/12/2021:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del quarto trimestre 2021.

STIG per Windows Basso (categoria III)

- Windows Server 2019 STIG versione 2 versione 3
- Windows Server 2016 STIG versione 2 versione 3
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 1
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 1 versione 19

STIG per Windows Medio (categoria II)

- Windows Server 2019 STIG versione 2 versione 3
- Windows Server 2016 STIG versione 2 versione 3
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 1
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 1 versione 19

STIG per Windows Alto (categoria I)

- Windows Server 2019 STIG versione 2 versione 3
- Windows Server 2016 STIG versione 2 versione 3

- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 1
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 1 versione 19

Modifiche al terzo trimestre 2021 - 30/09/2021:

Sono state aggiornate le versioni STIG e sono stati applicati STIG per il rilascio del terzo trimestre 2021.

STIG per Windows Basso (categoria III)

- Windows Server 2019 STIG versione 2 versione 2
- Windows Server 2016 STIG versione 2 versione 2
- Windows Server 2012 R2 MS STIG versione 3 versione 2
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 1
- Windows Firewall STIG versione 1 rilascio 7
- Internet Explorer 11 STIG versione 1 versione 19

STIG per Windows Medio (categoria II)

- Windows Server 2019 STIG versione 2 versione 2
- Windows Server 2016 STIG versione 2 versione 2
- Windows Server 2012 R2 MS STIG versione 3 versione 2
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 1
- Windows Firewall STIG versione 1 rilascio 7
- Internet Explorer 11 STIG versione 1 versione 19

STIG per Windows Alto (categoria I)

- Windows Server 2019 STIG versione 2 versione 2
- Windows Server 2016 STIG versione 2 versione 2
- Windows Server 2012 R2 MS STIG versione 3 versione 2
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 1

- Windows Firewall STIG versione 1 rilascio 7
- Internet Explorer 11 STIG versione 1 versione 19

AWS Systems Manager Utilizzatelo per applicare le impostazioni STIG alla vostra istanza

Puoi utilizzare il documento di comando `AWSEC2-ConfigureSTIG` Systems Manager per applicare le impostazioni STIG a un'istanza EC2 esistente. Devi eseguire il documento di comando dall'istanza che viene aggiornata. Il documento di comando applica le impostazioni appropriate in base al sistema operativo e alla configurazione dell'istanza su cui viene eseguito.

Questa pagina contiene dettagli sul documento di comando `AWSEC2-ConfigureSTIG`, inclusi i parametri di input e come eseguirlo nella console Systems Manager o con `send-command`in AWS CLI.

Parametri di input AWSEC2-ConfigureSTIG

Puoi fornire i seguenti parametri di input per specificare in che modo il documento di comando deve applicare le impostazioni STIG all'istanza.

Livello (stringa, obbligatorio)

Specificate la categoria di gravità STIG da applicare. I valori validi includono quanto segue:

- Elevata
- Media
- Bassa

Se non si specifica un valore, il sistema utilizza il valore predefinito `High`.

InstallPackages(stringa, opzionale, solo Linux)

Se il valore è `No`, lo script non installa pacchetti software aggiuntivi. Se il valore è `Yes`, lo script installa i pacchetti software aggiuntivi necessari per la massima conformità. Il valore predefinito è `No`.

SetDoDConsentBanner (stringa, opzionale, solo Linux)

Se il valore è `No`, il banner di consenso DoD non viene visualizzato quando si collega a un'istanza su cui è installato uno script STIG Linux. Se il valore è `Yes`, il banner di consenso DoD viene

visualizzato prima dell'accesso quando colleghi un'istanza su cui è installato uno degli script STIG Linux. Devi confermare il banner prima di poter accedere. Il valore predefinito è `No`.

Per un esempio del banner di consenso, consulta Disclaimer Department of Defense Privacy and Consent Notice, che viene visualizzato quando accedi al sito Web DLA Document Services.

Esegui il documento di comando AWSEC2-ConfigureSTIG

Per eseguire il documento `AWSEC2-ConfigureSTIG`, segui i passaggi relativi al tuo ambiente preferito.

Console

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, seleziona Esegui comando. Questo mostra un elenco di comandi correntemente in esecuzione nel tuo account, se applicabile.
3. Seleziona Esegui comando. Si apre la finestra di dialogo Esegui un comando e viene visualizzato un elenco di documenti di comando a cui si ha accesso.
4. Seleziona `AWSEC2-ConfigureSTIG` dall'elenco dei documenti di comando. Per semplificare i risultati, puoi inserire tutto o parte del nome del documento. Puoi anche filtrare per proprietario, per tipo di piattaforma o per tag.

   Quando si seleziona un documento di comando, i dettagli vengono inseriti sotto l'elenco.
5. Seleziona `Default version at runtime` dall'elenco delle versioni del documento.
6. Configura i parametri del comando per definire come `AWSEC2-ConfigureSTIG` installerà il pacchetto di script ed eseguilo per aggiornare l'istanza. Per i dettagli dei parametri, consulta Parametri di input AWSEC2-ConfigureSTIG.
7. In Selezione della destinazione, specifica i tag o seleziona manualmente le istanze per identificare le istanze su cui eseguire questa operazione.

> **Note**
>
> Se selezioni manualmente le istanze e l'istanza prevista non è inclusa nell'elenco, consulta Dove sono le mie istanze? per suggerimenti sulla risoluzione dei problemi.

8. Per i parametri aggiuntivi per la definizione del comportamento dei comandi di esecuzione di Systems Manager, ad esempio il controllo della velocità, immetti i valori come descritto in Esecuzione di comandi dalla console.
9. Scegli Esegui.

   In caso di successo, il documento di comando installa lo script e configura l'istanza. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando di Systems Manager.

AWS CLI

Esempio 1: esegui con valori predefiniti

Esegui il comando seguente per installare lo script STIG ed eseguilo con i valori predefiniti. Per ulteriori informazioni sui parametri di input, consultare Parametri di input AWSEC2-ConfigureSTIG.

```
aws ssm send-command \
 --document-name "AWSEC2-ConfigureSTIG" \
 --instance-ids "i-1234567890abcdef0"'
```

Esempio 2: configura le impostazioni STIG di livello medio sulla tua istanza

Esegui il comando seguente per installare lo script STIG ed eseguilo con il parametro di input `Level` impostato su `Medium`. Per ulteriori informazioni sui parametri di input, consultare Parametri di input AWSEC2-ConfigureSTIG.

```
aws ssm send-command \
 --document-name "AWSEC2-ConfigureSTIG" \
 --instance-ids "i-1234567890abcdef0"
 --parameters '{"Level":"Medium"}'
```

In caso di successo, il documento di comando installa lo script e configura l'istanza. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando.

PowerShell

Esempio 1: esegui con valori predefiniti

Esegui il comando seguente per installare lo script STIG ed eseguilo con i valori predefiniti. Per ulteriori informazioni sui parametri di input, consultare Parametri di input AWSEC2-ConfigureSTIG.

```
Send-SSMCommand -DocumentName "AWSEC2-ConfigureSTIG" -InstanceId
 "i-1234567890abcdef0"}
```

Esempio 2: configura le impostazioni STIG di livello medio sulla tua istanza

Esegui il comando seguente per installare lo script STIG ed eseguilo con il parametro di input `Level` impostato su `Medium`. Per ulteriori informazioni sui parametri di input, consultare Parametri di input AWSEC2-ConfigureSTIG.

```
Send-SSMCommand -DocumentName "AWSEC2-ConfigureSTIG" -InstanceId
 "i-1234567890abcdef0" -Parameter @{'Level'='Medium'}
```

In caso di successo, il documento di comando installa lo script e configura l'istanza. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando.

Sincronizzazione precisa dell'orologio e dell'ora sull'istanza EC2

Un riferimento temporale coerente e accurato sull'istanza Amazon EC2 è fondamentale per numerosi processi e attività del server. I timestamp nei log di sistema svolgono un ruolo essenziale nell'identificazione del momento in cui si sono verificati i problemi e dell'ordine cronologico degli eventi. Quando utilizzi AWS CLI o un AWS SDK per effettuare richieste dalla tua istanza, questi strumenti firmano le richieste per tuo conto. Se le impostazioni di data e ora dell'istanza non sono accurate, può verificarsi una discrepanza tra la data della firma e la data della richiesta, con conseguente rifiuto delle richieste. AWS

Per risolvere questo importante aspetto, Amazon offre il servizio di sincronizzazione oraria di Amazon, accessibile da tutte le istanze EC2 e utilizzabile con vari Servizi AWS. Il servizio utilizza una flotta di orologi di riferimento atomici e connessi via satellite Regione AWS per fornire letture dell'ora accurate e attuali dello standard globale Coordinated Universal Time (UTC).

Per prestazioni ottimali, consigliamo di utilizzare il servizio di sincronizzazione oraria di Amazon locale sulle tue istanze EC2. Per eseguire un backup del servizio di sincronizzazione oraria di

Amazon locale sulle tue istanze o per connettere risorse esterne ad Amazon EC2 al servizio di sincronizzazione oraria di Amazon, puoi utilizzare il servizio di sincronizzazione oraria di Amazon pubblico situato all'indirizzo `time.aws.com`. Il servizio di sincronizzazione oraria di Amazon pubblico spalma in modo automatico i secondi intercalari aggiunti all'orario UTC. Il servizio pubblico Amazon Time Sync è supportato a livello globale dalla nostra flotta di orologi di riferimento atomici e connessi via satellite in ciascuno di essi. Regione AWS

Marcatura temporale dei pacchetti hardware

Puoi abilitare la marcatura temporale dei pacchetti hardware sull'istanza per aggiungere una marcatura temporale con precisione in nanosecondi a 64 bit a ogni pacchetto di rete in ingresso. Poiché la marcatura temporale dei pacchetti hardware avviene a livello hardware, prima che il pacchetto raggiunga il kernel, il socket o il livello dell'applicazione, si evitano i ritardi aggiunti dalla marcatura temporale del software. L'orologio di riferimento sottostante per la marcatura temporale dell'hardware è l'orologio hardware PTP del servizio di sincronizzazione oraria di Amazon.

Vantaggi

La marcatura temporale dei pacchetti hardware fornisce i seguenti vantaggi:

- Migliora l'ordinamento degli eventi, che può essere utilizzato anche per determinare l'ordine effettivo in cui i pacchetti arrivano all'istanza EC2, garantendo un'elaborazione corretta dei pacchetti.
- Misura la latenza di rete unidirezionale.
- Aumenta la velocità delle transazioni distribuite con maggiore precisione e accuratezza rispetto alla maggior parte delle soluzioni on-premises.

Prerequisiti e configurazione

Per abilitare la marcatura temporale dei pacchetti hardware, l'istanza deve soddisfare i seguenti prerequisiti:

- Deve essere un'istanza Linux.
- Soddisfa i requisiti per supportare l'orologio hardware PTP.

Per le istruzioni di configurazione, consulta la pagina della famiglia Hardware Packet Timestamping sul driver del kernel Linux per Elastic Network Adapter (ENA) su GitHub.

Secondi intercalari

I secondi intercalari, introdotti nel 1972, sono aggiustamenti occasionali di un secondo dell'ora UTC per tenere conto delle irregolarità nella rotazione terrestre per compensare le differenze tra l'ora atomica internazionale (TAI) e l'ora solare (Ut1). Per gestire i secondi intercalari per conto dei clienti, abbiamo progettato Leap Second Smearing all'interno del servizio di sincronizzazione oraria di Amazon. Per ulteriori informazioni, consulta Guarda prima di saltare: il secondo salto in arrivo e AWS.

I secondi intercalari stanno scomparendo e appoggiamo pienamente la decisione presa alla 27a conferenza generale sui pesi e le misure di abbandonare i secondi intercalari entro il 2035.

Per supportare questa transizione, prevediamo comunque di risparmiare tempo durante un secondo intercalare quando si accede al servizio di sincronizzazione oraria di Amazon tramite la connessione NTP locale o i nostri pool NTP pubblici (`time.aws.com`). Il clock hardware PTP, tuttavia, non offre l'opzione dei tempi spalmati. In caso di secondi intercalari, l'orologio hardware PTP aggiungerà il secondo intercalare seguendo gli standard UTC. Leap-smeared e le sorgenti del secondo orario intercalare sono le stesse nella maggior parte dei casi. Tuttavia, poiché differiscono durante un evento di secondo intercalare, si sconsiglia di utilizzare contemporaneamente sorgenti temporali spalmate e non spalmate nella configurazione del client orario durante un evento di secondo intercalare.

Argomenti

- Configurazione del rifermento temporale sull'istanza EC2 per l'utilizzo del servizio di sincronizzazione oraria di Amazon locale
- Impostazione del riferimento temporale sull'istanza EC2 o su qualsiasi dispositivo connesso a Internet per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico
- Confronto dei timestamp per le istanze Linux
- Modifica del fuso orario dell'istanza

Risorse correlate

- AWS Compute Blog: È ora: Microsecond-Accurate gli orologi sulle istanze Amazon EC2
- AWS Blog sulle operazioni e le migrazioni sul cloud: gestisci la precisione del clock delle istanze Amazon EC2 utilizzando Amazon Time Sync Service e Amazon — Parte 1 CloudWatch

- (Linux) https://chrony-project.org/

Configurazione del rifermento temporale sull'istanza EC2 per l'utilizzo del servizio di sincronizzazione oraria di Amazon locale

Il servizio Amazon Time Sync fornisce diversi metodi per la sincronizzazione dell'istanza Amazon EC2 con una fonte di ora locale. Innanzitutto, qualsiasi istanza Amazon EC2 può raggiungere una sorgente di ora locale tramite il Network Time Protocol (NTP). Inoltre, il servizio Amazon Time Sync avanzato offre sorgenti temporali locali con maggiore precisione alle istanze Amazon EC2 supportate. Avvia la tua istanza supportata in un gruppo di collocamento con la `precision-time` strategia per raggiungere una fonte NTP con maggiore precisione. Infine, le istanze Linux avviate in un gruppo di posizionamento temporale di precisione hanno accesso a un dispositivo PTP Hardware Clock (PHC) e alla capacità di recuperare i timestamp dei pacchetti hardware.

Qualsiasi istanza Amazon EC2 ha accesso alla fonte NTP locale. Puoi raggiungere la sorgente NTP tramite un indirizzo IP locale del collegamento, che limita questo traffico all'interno del tuo VPC senza la necessità di apportare modifiche specifiche alla configurazione del VPC. La tua AMI potrebbe aver già configurato il tuo demone di sincronizzazione dell'orologio per utilizzare la fonte NTP locale per impostazione predefinita. Questa fonte NTP è disponibile tramite i seguenti indirizzi IP:

- IPv4: `169.254.169.123`
- IPv6: `fd00:ec2::123` (accessibile solo su Nitro-based istanze).

Le istanze Amazon EC2 supportate hanno accesso al servizio avanzato Amazon Time Sync. Per accedere al servizio Amazon Time Sync avanzato, avvia un'istanza supportata in un gruppo di collocamento con la `precision-time` strategia. Non è necessario configurare l'istanza per beneficiare di questo miglioramento se si utilizzano gli indirizzi IP locali del collegamento NTP. Qualsiasi sistema operativo può utilizzare questo miglioramento. Puoi verificare di beneficiare della fonte NTP avanzata utilizzando il tuo client NTP preferito.

Linux-based Le AMI, in esecuzione su famiglie di istanze supportate, hanno l'opzione aggiuntiva di generare l'ora da un dispositivo PHC. Il driver ENA rende disponibile questo dispositivo. Sia la sorgente NTP avanzata che il dispositivo PHC utilizzano la stessa fonte temporale estremamente precisa. L'accesso alla sorgente temporale PHC è ottimizzato e consente una sincronizzazione più accurata dell'istanza Amazon EC2.

Considerazioni

- La sorgente temporale NTP offre una visualizzazione intermittente della scala temporale UTC, mentre la sorgente temporale PHC non mostra l'ora. Per ulteriori informazioni, consulta Secondi intercalari.
- Solo le istanze Linux hanno accesso all'orologio hardware PTP locale. Le istanze Windows devono utilizzare NTP per accedere al servizio Amazon Time Sync avanzato.
- Esiste un limite di 1024 pacchetti al secondo (PPS) per i servizi che utilizzano indirizzi link-local. Questo limite include l'aggregato delle richieste DNS Query di Route 53 Resolver, delle richieste IMDS (Instance Metadata Service), delle richieste di Amazon Time Sync Service Network Time Protocol (NTP) e delle richieste Windows Licensing Service (per istanze basate su Microsoft Windows).

Indice

- Accedi all'endpoint IPv4 del servizio Amazon Time Sync
- Accedi all'endpoint IPv6 del servizio Amazon Time Sync
- Accedi al servizio Amazon Time Sync avanzato
- Accedi al PTP Hardware Clock (PHC)

Accedi all'endpoint IPv4 del servizio Amazon Time Sync

Il tuo AMI potrebbe aver già configurato il servizio di sincronizzazione oraria di Amazon per impostazione predefinita. In caso contrario, utilizza le seguenti procedure per configurare l'istanza per l'utilizzo del servizio di sincronizzazione oraria di Amazon locale tramite l'endpoint IPv4.

Per assistenza nella risoluzione dei problemi, consulta Troubleshoot NTP synchronization issues on Linux instances o Risoluzione dei problemi di impostazione dell'ora sulle istanze Windows.

Amazon Linux

AL2023 e le recenti versioni di Amazon Linux 2 sono configurati per utilizzare l'endpoint IPv4 del servizio di sincronizzazione oraria di Amazon per impostazione predefinita. Se confermi che l'istanza è già configurata, puoi ignorare la seguente procedura.

Per verificare che chrony sia configurato per l'utilizzo dell'endpoint IPv4

Eseguire il seguente comando seguente. Nell'output, la riga che inizia con ^* indica l'origine di orario preferita.

```
[ec2-user ~]$ chronyc sources -v | grep -F ^*
```

```
^* 169.254.169.123               3   4   377    13  -4325ns[-9201ns] +/-  401us
```

Per configurare chrony per collegarlo all'endpoint IPv4 su versioni precedenti di Amazon Linux 2

1. Connetti l'istanza e disinstalla il servizio NTP.

   ```
   [ec2-user ~]$ sudo yum erase 'ntp*'
   ```

2. Installare il pacchetto `chrony`.

   ```
   [ec2-user ~]$ sudo yum install chrony
   ```

3. Aprire il file `/etc/chrony.conf` tramite un editor di testo (ad esempio vim o nano). Aggiungi la riga seguente prima di qualsiasi altra istruzione `server` o `pool` già presente nel file, quindi salva le modifiche:

   ```
   server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
   ```

4. Avvia di nuovo il daemon `chrony` (`chronyd`).

   ```
   [ec2-user ~]$ sudo service chronyd restart
   ```

   ```
   Starting chronyd:                                          [  OK  ]
   ```

   > **Note**
   >
   > In RHEL e CentOS (fino alla versione 6), il nome del servizio è `chrony` anziché `chronyd`.

5. Per configurare `chronyd` in modo da avviarlo a ogni avvio del sistema, utilizza il comando `chkconfig`.

   ```
   [ec2-user ~]$ sudo chkconfig chronyd on
   ```

6. Verifica che `chrony` utilizzi l'endpoint IPv4 `169.254.169.123` per sincronizzare l'orario.

```
[ec2-user ~]$ chronyc sources -v | grep -F ^*
```

Nell'output, `^*` indica l'origine temporale preferita.

```
^* 169.254.169.123               3   6    17    43    -30us[ -226us] +/-  287us
```

7. Verifica i parametri di sincronizzazione dell'orario indicati da `chrony`.

```
[ec2-user ~]$ chronyc tracking
```

```
Reference ID    : A9FEA97B (169.254.169.123)
Stratum         : 4
Ref time (UTC)  : Wed May 06 00:39:14 2026
System time     : 0.000002191 seconds fast of NTP time
Last offset     : +0.000002164 seconds
RMS offset      : 0.000082968 seconds
Frequency       : 3.710 ppm slow
Residual freq   : +0.002 ppm
Skew            : 0.504 ppm
Root delay      : 0.000362541 seconds
Root dispersion : 0.000225028 seconds
Update interval : 16.1 seconds
Leap status     : Normal
```

Ubuntu

Per configurare chrony per collegarlo all'endpoint IPv4 su Ubuntu

1. Connettiti all'istanza e utilizza `apt` per installare il pacchetto `chrony`.

```
ubuntu:~$ sudo apt install chrony
```

> **Note**
>
> Se necessario, prima aggiorna l'istanza eseguendo `sudo apt update`.

2. Aprire il file `/etc/chrony/chrony.conf` tramite un editor di testo (ad esempio vim o nano). Aggiungi la riga seguente prima di qualsiasi altra istruzione `server` o `pool` già presente nel file, quindi salva le modifiche:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

3. Riavvia il servizio `chrony`.

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
Restarting chrony (via systemctl): chrony.service.
```

4. Verifica che `chrony` utilizzi l'endpoint IPv4 `169.254.169.123` per sincronizzare l'orario.

```
ubuntu:~$ chronyc sources -v | grep -F ^*
```

Nell'output, la riga che inizia con `^*` indica l'origine di orario preferita.

```
^* 169.254.169.123               3   6    17    12    +15us[  +57us] +/-  320us
```

5. Verifica i parametri di sincronizzazione dell'orario indicati da `chrony`.

```
ubuntu:~$ chronyc tracking
```

```
Reference ID    : A9FEA97B (169.254.169.123)
Stratum         : 4
Ref time (UTC)  : Wed May 06 00:39:14 2026
System time     : 0.000002191 seconds fast of NTP time
Last offset     : +0.000002164 seconds
RMS offset      : 0.000082968 seconds
Frequency       : 3.710 ppm slow
Residual freq   : +0.002 ppm
Skew            : 0.504 ppm
Root delay      : 0.000362541 seconds
Root dispersion : 0.000225028 seconds
Update interval : 16.1 seconds
Leap status     : Normal
```

SUSE Linux

A partire da SUSE Linux Enterprise Server 15, `chrony` è l'implementazione predefinita di NTP.

Per configurare chrony per collegarlo a un endpoint IPv4 su SUSE Linux

1. Aprire il file `/etc/chrony.conf` tramite un editor di testo (ad esempio vim o nano).
2. Verificare che il file contenga la riga seguente:

   ```
   server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
   ```

   Aggiungere questa riga se non è presente.
3. Commentare le altre righe del server o del pool.
4. Apri YaST e abilita il servizio chrony.

Windows

A partire dal rilascio di agosto 2018, le AMI di Windows utilizzano Amazon Time Sync Service per impostazione predefinita. Non è richiesta alcuna ulteriore configurazione per le istanze avviate da queste AMI ed è possibile saltare le seguenti procedure.

Se utilizzi un'AMI che non ha il servizio di sincronizzazione oraria di Amazon configurato per impostazione predefinita, verifica innanzitutto la configurazione NTP corrente. Se la tua istanza utilizza già l'endpoint IPv4 del servizio di sincronizzazione oraria di Amazon, non è richiesta alcuna ulteriore configurazione. Se la tua istanza non utilizza il servizio di sincronizzazione oraria di Amazon, completa la procedura per modificare il server NTP in modo da utilizzare il servizio.

Per verificare la configurazione di NTP

1. Dall'istanza, aprire una finestra del prompt dei comandi.
2. Ottenere la configurazione attuale di NTP digitando il comando seguente:

   ```
   w32tm /query /configuration
   ```

   Questo comando restituisce le impostazioni della configurazione corrente dell'istanza Windows e mostra se sei connesso al servizio di sincronizzazione oraria di Amazon.
3. (Opzionale) Ottenere lo stato della configurazione attuale digitando il comando seguente:

```
w32tm /query /status
```

Questo comando restituisce informazioni come l'ultima sincronizzazione dell'istanza con il server NTP e l'intervallo di polling.

Modifica del server NTP per l'utilizzo di Amazon Time Sync Service

1. Dalla finestra del prompt dei comandi, esegui il comando seguente:

   ```
   w32tm /config /manualpeerlist:169.254.169.123 /syncfromflags:manual /update
   ```

2. Verificare le nuove impostazioni tramite il comando seguente:

   ```
   w32tm /query /configuration
   ```

   Nell'output restituito, verifica che `NtpServer` visualizzi l'endpoint IPv4 `169.254.169.123`.

Impostazioni NTP predefinite per le AMI Windows Amazon

Le Amazon Machine Image (AMI) aderiscono generalmente alle impostazioni predefinite, ad eccezione dei casi in cui è necessario apportare modifiche alla funzione sull'infrastruttura EC2. Le impostazioni seguenti sono state stabilite per il corretto funzionamento in un ambiente virtuale, nonché per mantenere qualsiasi scostamento dell'orologio entro un secondo di accuratezza:

- Intervallo di aggiornamento: determina la frequenza con cui il servizio aggiusta l'ora di sistema in base alla precisione. AWS configura l'intervallo di aggiornamento in modo che avvenga una volta ogni due minuti.
- Server NTP: a partire dalla versione di agosto 2018, le AMI utilizzeranno il servizio di sincronizzazione oraria di Amazon per impostazione predefinita. Questo servizio orario è accessibile da qualsiasi Regione AWS endpoint IPv4 169.254.169.123. Inoltre, il flag 0x9 indica che il servizio ora funziona da client e indica di utilizzare `SpecialPollInterval` per stabilire la frequenza di check-in nel server di riferimento ora configurato.
- Type – "NTP" indica che il servizio funzionerà come client NTP standalone invece che come parte di un dominio.
- Abilitato e InputProvider: il servizio orario è abilitato e fornisce l'ora al sistema operativo.

- Intervallo di polling speciale: esegue controlli a fronte del server NTP configurato ogni 900 secondi (15 minuti).

> **Note**
>
> Per le AMI di Windows Server 2025, il `SpecialPollInterval` valore è 1024 secondi anziché 900 secondi.

Percorso Registro di sistema	Nome chiave	Dati
HKL M:\System\\ services\ CurrentControlSet w32time\ Config	UpdateInterval	120
HKL M:\System\\ services\ w32timeCurrentControlSet\ Parametri	NtpServer	169.254.169.123,0x9
HKL M:\System\\ services\ w32timeCurrentControlSet\ Parameters	Tipo	NTP
HKL M:\System\\ services\ CurrentControlSet w32time\\ TimeProviders NtpClient	Abilitato	1
HKL M:\System\\ services\ CurrentControlSet w32time\\ TimeProviders NtpClient	InputProvider	1
HKL M:\System\\ services\ CurrentControlSet w32time\\ TimeProviders NtpClient	SpecialPollInterval	900 (Windows Server 2016, 2019 e 2022) o 1024 (Windows Server 2025)

Accedi all'endpoint IPv6 del servizio Amazon Time Sync

In questa sezione viene descritto come differisce la procedura riportata in Accedi all'endpoint IPv4 del servizio Amazon Time Sync nel caso della configurazione dell'istanza per l'utilizzo del servizio di sincronizzazione oraria di Amazon locale tramite l'endpoint IPv6. Non viene illustrato l'intero processo di configurazione di Amazon Time Sync Service.

L'endpoint IPv6 è accessibile solo su istanze. Nitro-based

Non è consigliabile utilizzare le voci di endpoint IPv4 e IPv6 insieme. I pacchetti NTP IPv4 e IPv6 provengono dallo stesso server locale per l'istanza. La configurazione degli endpoint IPv4 e IPv6 non è necessaria e non migliorerà la precisione dell'ora sull'istanza.

Linux

A seconda della distribuzione Linux utilizzata, quando raggiungi il passaggio per modificare il file `chrony.conf`, utilizzerai l'endpoint IPv6 del servizio di sincronizzazione oraria di Amazon (`fd00:ec2::123`) piuttosto che l'endpoint IPv4 (`169.254.169.123`):

```
server fd00:ec2::123 prefer iburst minpoll 4 maxpoll 4
```

Salva il file e verifica che chrony utilizzi l'endpoint IPv6 `fd00:ec2::123` per sincronizzare l'orario:

```
[ec2-user ~]$ chronyc sources -v
```

Nell'output, se compare l'endpoint IPv6 `fd00:ec2::123`, la configurazione è completa.

Windows

Quando raggiungi il passaggio per modificare il server NTP in modo da utilizzare il servizio di sincronizzazione oraria di Amazon, utilizzerai l'endpoint IPv6 del servizio di sincronizzazione oraria di Amazon (`fd00:ec2::123`) piuttosto che l'endpoint IPv4 (`169.254.169.123`):

```
w32tm /config /manualpeerlist:fd00:ec2::123 /syncfromflags:manual /update
```

Verifica che le nuove impostazioni utilizzino l'endpoint IPv6 `fd00:ec2::123` per sincronizzare l'ora:

```
w32tm /query /configuration
```

nell'output, verifica che `NtpServer` visualizzi l'endpoint IPv6 `fd00:ec2::123`.

Accedi al servizio Amazon Time Sync avanzato

Il servizio Amazon Time Sync migliorato offre sorgenti temporali locali con maggiore precisione alle istanze Amazon EC2 supportate. Le istanze avviate in un gruppo di collocamento con una `precision-time` strategia possono accedere a queste fonti locali. Consigliamo i gruppi di posizionamento temporale di precisione per le applicazioni che richiedono un tempo più preciso dalla fonte NTP locale del collegamento o da un dispositivo PTP Hardware Clock (PHC) su un'istanza Linux. Quando avvii le istanze in un gruppo di posizionamento temporale di precisione, le AWS colloca sull'hardware supportato con accesso diretto alle sorgenti temporali ad alta precisione nell'infrastruttura. AWS

Vantaggi principali

- Sorgente NTP migliorata per impostazione predefinita: l'istanza ha accesso immediato a un'origine temporale NTP locale avanzata, se si utilizzano gli indirizzi IP locali del collegamento NTP come descritto nella sezione precedente.
- Microsecond-accurate sincronizzazione dell'orologio: configura la tua istanza Amazon EC2 Linux per utilizzare un dispositivo PTP Hardware Clock e ottenere una sincronizzazione dell'orologio accurata al microsecondo.
- Implementazione semplificata: la strategia di posizionamento singolo garantisce che tutte le istanze abbiano funzionalità temporali di precisione.
- Timestamp dei pacchetti hardware: accedi ai timestamp dei pacchetti di basso livello per le misurazioni di rete.
- Nessun costo aggiuntivo: i gruppi Precision Time Placement sono disponibili senza costi aggiuntivi.

Regole e limitazioni

- I gruppi di collocamento cronologico di precisione sono disponibili in tutte le regioni AWS commerciali.
- I gruppi Precision Time Placement supportano le seguenti famiglie di istanze Amazon EC2 di settima generazione e successive:
  - Uso generale: M7a, M7g, M7gd, M7i,, M8a, M8g M7i-flex
  - Ottimizzato per il calcolo: C7a, C7gd, C7i,, C8g, C8gd C7i-flex
  - Memoria ottimizzata: R7a, R7g, R7i, R8g, X8g

  - Archiviazione ottimizzata: I8g, I8ge
- Se avvii o avvii un'istanza in un gruppo di collocamento temporale di precisione e l'hardware non è sufficiente per consentire l'accesso al servizio avanzato Amazon Time Sync Service, la richiesta ha esito negativo.
- Se interrompi un'istanza in un gruppo di collocamento temporale di precisione e poi la riavvii, viene comunque eseguita nel gruppo di collocamento. Tuttavia, l'avvio potrebbe fallire se l'hardware non è sufficiente per consentire l'accesso al servizio avanzato Amazon Time Sync.
- Amazon EC2 aggiunge continuamente hardware che supporta il servizio avanzato Amazon Time Sync. Se la tua richiesta non va a buon fine a causa di una capacità insufficiente, riprova più tardi o prova una zona di disponibilità diversa. Per ulteriori informazioni, consulta Risoluzione dei problemi di avvio dell'istanza Amazon EC2.
- Si applicano le regole e le limitazioni dei gruppi di collocamento. Per ulteriori informazioni, consulta Gruppi di collocamento per le tue istanze Amazon EC2

Crea un gruppo di collocamento temporale di precisione

È possibile creare un gruppo di collocazione temporale di precisione utilizzando la AWS CLI, la console di AWS gestione o AWS gli SDK, specificando la strategia. `precision-time`

Utilizzo AWS CLI

Esegui il comando seguente:

```
aws ec2 create-placement-group \
    --group-name my-precision-time-pg \
    --strategy precision-time
```

Il comando restituisce un ARN del gruppo di collocamento da utilizzare per creare prenotazioni di capacità e un nome o ID di gruppo da utilizzare per l'avvio delle istanze e il collegamento dei gruppi di collocamento.

Avvio di un'istanza

Dopo aver creato un gruppo di collocazione temporale di precisione, specificalo quando avvii le istanze per accedere al servizio Amazon Time Sync avanzato:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7g.2xlarge \
```

```
    --placement GroupId=pg-0aaa1111111111111
```

Verifica l'accesso al servizio Amazon Time Sync avanzato

Dopo aver avviato l'istanza in un gruppo di collocamento temporale di precisione, beneficerai di una fonte temporale NTP migliorata.

Ad esempio, se utilizzi il demone chronyd sulla tua istanza, puoi verificare che l'origine temporale NTP sia ora denominata Stratum 1 e abbia metriche di precisione dell'orologio migliorate:

```
[ec2-user ~]$ chronyc sources
```

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* 169.254.169.123               1   4   377     3  +3477ns[+4689ns] +/-   91us
```

Verifica i parametri di sincronizzazione dell'orario indicati da `chrony`.

```
[ec2-user ~]$ chronyc tracking
```

```
Reference ID    : A9FEA97B (169.254.169.123)
Stratum         : 2
Ref time (UTC)  : Wed May 06 01:33:43 2026
System time     : 0.000000276 seconds fast of NTP time
Last offset     : +0.000000331 seconds
RMS offset      : 0.000001929 seconds
Frequency       : 2.870 ppm fast
Residual freq   : +0.000 ppm
Skew            : 0.031 ppm
Root delay      : 0.000107584 seconds
Root dispersion : 0.000036476 seconds
Update interval : 16.2 seconds
Leap status     : Normal
```

Accedi al PTP Hardware Clock (PHC)

Il PTP Hardware Clock (PHC) fa parte del sistema Nitro. AWS È direttamente accessibile sulle istanze bare metal e virtualizzate supportate di Amazon EC2 avviate in un gruppo di collocamento temporale di precisione. Il dispositivo PHC è attualmente accessibile solo su istanze Linux. Le sezioni seguenti descrivono come configurare e verificare il dispositivo PHC sull'istanza Linux.

Requisiti

- Driver ENA versione 2.10.0 o successiva installato su un sistema operativo supportato.
- Un'istanza Amazon EC2 che esegue Linux. Per ulteriori informazioni sui sistemi operativi supportati, consulta i prerequisiti del driver su GitHub.
- Un'istanza Amazon EC2 lanciata in un gruppo di collocamento temporale di precisione (vediAccedi al servizio Amazon Time Sync avanzato).

> **Note**
>
> Il servizio Amazon Time Sync Service avanzato e il dispositivo PHC rimangono accessibili senza un gruppo di posizionamento temporale preciso nelle seguenti regioni e per le famiglie di istanze specifiche. Per un'esperienza ottimale, consigliamo invece di avviare le istanze Amazon EC2 in gruppi di posizionamento di precisione.
>
> - Accesso legacy supportato Regioni AWS: Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Asia Pacifico (Malesia), Asia Pacifico (Thailandia), Asia Pacifico (Thailandia), Asia Pacifico (Tokyo) ed Europa (Stoccolma)
> - Zone locali supportate dall'accesso alle versioni precedenti: Stati Uniti orientali (New York City)
> - Famiglie di istanze supportate dall'accesso legacy:
>   - Uso generico: M7a, M7g, M7i
>   - Memoria ottimizzata: R7a, R7g, R7i
>   - Archiviazione ottimizzata: I8g, I8ge

Compila e abilita il driver ENA con supporto PHC

Consulta sempre le istruzioni più recenti della versione più recente del driver Elastic Network Adapter (ENA) nella documentazione del driver ENA GitHub per informazioni specifiche sul tuo sistema operativo. Di seguito è riportata una panoramica dei passaggi per Amazon Linux.

Prima di iniziare, assicurati che la tua istanza soddisfi iRequisiti.

Per compilare e abilitare il driver ENA con supporto PHC

1. Prerequisiti di installazione.

```
[ec2-user ~]$ sudo yum update
[ec2-user ~]$ sudo yum install kernel-devel-$(uname -r) git
[ec2-user ~]$ sudo reboot
```

2. Carica il modulo ptp richiesto.

```
[ec2-user ~]$ sudo modprobe ptp
```

3. Recupera la versione più recente del driver ENA (versione 2.10.0 o successiva).

```
[ec2-user ~]$ git clone https://github.com/amzn/amzn-drivers.git /tmp/amzn-drivers
```

4. Crea il driver ENA `ena.ko` con il supporto PHC.

```
[ec2-user ~]$ cd /tmp/amzn-drivers/kernel/linux/ena
[ec2-user ~]$ ENA_PHC_INCLUDE=1 make
```

5. Ricarica il driver ENA e abilita il dispositivo PHC.

```
[ec2-user ~]$ sudo rmmod ena && sudo insmod ena.ko phc_enable=1
```

6. Verifica che il driver ENA caricato sia compatibile con PHC.

```
[ec2-user ~]$ modinfo ena | grep -E "phc_enable"
```

```
parm:           phc_enable:Enable PHC.
```

7. Convalida che il supporto PHC sia abilitato con il driver ENA.

```
[ec2-user ~]$ cat /sys/module/ena/parameters/phc_enable
```

```
1
```

Per istruzioni su come installare il driver e attivare l'opzione phc_enable al riavvio, consultate il file README del driver ENA attivo. https://github.com/amzn/amzn-drivers/blob/master/kernel/linux/ena/README.rst GitHub

Verificate la configurazione del dispositivo PTP

Verifica che il dispositivo dell'orologio hardware ENA PTP sia presente sulla tua istanza.

```
[ec2-user ~]$ for file in /sys/class/ptp/*; do echo -n "$file: "; cat "$file/
clock_name"; done
```

Output previsto

```
/sys/class/ptp/ptp<index>: ena-ptp-<PCI slot>
```

Dove:

- *index* è l'indice dell'orologio hardware PTP registrato nel kernel.
- *PCI slot* è lo slot PCI del controller Ethernet ENA. Si tratta dello stesso slot mostrato in `lspci | grep ENA`.

Output di esempio

```
/sys/class/ptp/ptp0: ena-ptp-05
```

Se `ena-ptp-`*<PCI slot>* non è presente nell'output, significa che il driver ENA non è stato installato correttamente. Rivedi i passaggi inCompila e abilita il driver ENA con supporto PHC.

Configurazione di collegamento simbolico PTP

Tipicamente, i dispositivi PTP sono denominati `/dev/ptp0`, `/dev/ptp1` e così via, e il loro indice dipende dall'ordine di inizializzazione dell'hardware. La creazione di un collegamento simbolico garantisce che applicazioni come chrony facciano costantemente riferimento al dispositivo corretto, indipendentemente dalle modifiche all'indice.

Le ultime AMI Amazon Linux 2023 includono una regola `udev` che crea il collegamento simbolico `/dev/ptp_ena`, che punta alla voce `/dev/ptp` corretta associata all'host ENA.

Innanzitutto, controlla se il collegamento simbolico è presente eseguendo il seguente comando.

```
[ec2-user ~]$ ls -l /dev/ptp*
```

Output di esempio

```
crw------- 1 root root 245, 0 Jan 31 2025 /dev/ptp0
lrwxrwxrwx 1 root root      4 Jan 31 2025 /dev/ptp_ena -> ptp0
```

Dove:

- `/dev/ptp<index>` è il percorso del dispositivo PTP.
- `/dev/ptp_ena` è il collegamento simbolico costante, che punta allo stesso dispositivo PTP.

Se il `/dev/ptp_ena` collegamento simbolico è presente, salta a. Configura il demone chronyd per utilizzare il dispositivo PHC Se manca, effettua quanto segue:

Per creare il collegamento simbolico PTP

1. Aggiungi la seguente regola `udev`.

   ```
   [ec2-user ~]$ echo "SUBSYSTEM==\"ptp\", ATTR{clock_name}==\"ena-ptp-*\", SYMLINK +=
    \"ptp_ena\"" | sudo tee -a /etc/udev/rules.d/53-ec2-network-interfaces.rules
   ```

2. Ricarica la regola `udev`, riavviando l'istanza o eseguendo il comando seguente.

   ```
   [ec2-user ~]$ sudo udevadm control --reload-rules && sudo udevadm trigger
   ```

Configura il demone chronyd per utilizzare il dispositivo PHC

Il demone di sincronizzazione dell'orologio chronyd deve essere configurato per utilizzare il dispositivo PHC come fonte di tempo aggiuntiva, utilizzando il collegamento simbolico per identificare il dispositivo. `/dev/ptp_ena`

Per configurare il demone chronyd per utilizzare il dispositivo PHC

1. Modifica `/etc/chrony.conf` usando un editor di testo e aggiungi la riga seguente:

   ```
   refclock PHC /dev/ptp_ena poll 0 delay 0.000010 prefer
   ```

2. Riavvia chrony.

   ```
   [ec2-user ~]$ sudo systemctl restart chronyd
   ```

3. Verifica che chrony stia usando l'orologio hardware PTP. Il dispositivo PHC0 deve essere l'origine temporale preferita con un valore Stratum 0. L'origine temporale NTP locale (se configurata) deve avere un valore Stratum 1.

```
[ec2-user ~]$ chronyc sources
```

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
#* PHC0                          0   0   377     0   +184ns[ +198ns] +/- 5032ns
^- 169.254.169.123               1   4   377     8    -18us[  -18us] +/-  115us
```

Verifica la marcatura temporale dei pacchetti hardware

Il driver ENA caricato con il supporto PHC fornisce l'accesso alla marcatura temporale dei pacchetti hardware. È possibile verificare il supporto per questa funzionalità utilizzando il comando. `ethtool -T` *`interface`*

Per ulteriori informazioni sull'uso del timestamping dei pacchetti hardware, consultate la documentazione di Linux sul timestamping dei pacchetti.

```
[ec2-user ~]$ sudo ethtool -T ens5
```

```
Time stamping parameters for ens5:
Capabilities:
        software-transmit
        hardware-receive
        software-receive
        software-system-clock
PTP Hardware Clock: 0
Hardware Transmit Timestamp Modes: none
Hardware Receive Filter Modes:
        none
        all
```

Se l'output è visualizzato `hardware-receive` nell'elenco delle funzionalità, sulla tua istanza è disponibile la marcatura temporale dei pacchetti hardware.

Impostazione del riferimento temporale sull'istanza EC2 o su qualsiasi dispositivo connesso a Internet per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico

Puoi configurare la tua istanza, o qualsiasi dispositivo connesso a Internet, come il computer locale o un server on-premises, per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico, accessibile via Internet a `time.aws.com`. Puoi utilizzare il servizio Amazon Time Sync Service pubblico come backup per il servizio Amazon Time Sync locale e per connettere risorse esterne ad Amazon Time Sync Service. AWS

> **Note**
>
> Per prestazioni ottimali, consigliamo di utilizzare il servizio di sincronizzazione oraria di Amazon locale sulle tue istanze e di utilizzare il servizio di sincronizzazione oraria di Amazon pubblico solo come backup.

Consulta le istruzioni relative al sistema operativo della tua istanza o del tuo dispositivo.

Linux

Configurazione dell'istanza o del dispositivo Linux per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico tramite chrony o ntpd

1. Utilizzando un editor di testo, modifica `/etc/chrony.conf` (se usi chrony) o `/etc/ntp.conf` (se usi ntpd) come segue:

   a. Per evitare che l'istanza o il dispositivo tenti di mischiare server "spalmati" e server non "spalmati", rimuovi o commenta le righe che iniziano con `server`, ad eccezione di qualsiasi connessione esistente al servizio di sincronizzazione oraria di Amazon locale.

   > **Important**
   >
   > Se stai configurando la tua istanza EC2 per connettersi al servizio di sincronizzazione oraria di Amazon pubblico, non rimuovere la seguente riga che imposta l'istanza per connettersi al servizio di sincronizzazione oraria di Amazon locale. Il servizio di sincronizzazione oraria di Amazon locale è una connessione più

diretta e fornirà una migliore precisione di clock. Il servizio di sincronizzazione oraria di Amazon pubblico deve essere usato solo come backup.

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

b. Aggiungi la seguente riga per connetterti al servizio di sincronizzazione oraria di Amazon pubblico.

```
pool time.aws.com iburst
```

2. Riavvia il daemon utilizzando uno dei seguenti comandi.

- chrony

```
sudo service chronyd force-reload
```

- ntpd

```
sudo service ntp reload
```

macOS

Configurazione dell'istanza o del dispositivo macOS per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico

1. Apri Preferenze di Sistema.
2. Scegli Date & Time (Data e ora), quindi scegli la scheda Date & Time (Data e ora).
3. Per apportare modifiche, scegli l'icona del lucchetto e inserisci la password quando richiesto.
4. In Imposta data e ora automaticamente, inserisci **`time.aws.com`**.

Windows

Configurazione dell'istanza o del dispositivo Windows per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico

1. Apri il Pannello di controllo.
2. Scegli l'icona Date and Time (Data e ora).

3. Scegli la scheda Internet Time (Ora Internet). Questa scheda non sarà disponibile se il PC fa parte di un dominio. In tal caso, sincronizzerà l'ora con il controller di dominio. Puoi configurare il controller per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico.
4. Scegli Change settings (Cambia impostazioni).
5. Seleziona la casella di controllo Sincronizza con un server orario su Internet.
6. Accanto a Server, inserisci **`time.aws.com`**.

Configurazione dell'istanza o del dispositivo Windows Server per utilizzare il servizio di sincronizzazione oraria di Amazon pubblico

- Segui le istruzioni di Microsoft per aggiornare il registro.

Confronto dei timestamp per le istanze Linux

Se utilizzi Amazon Time Sync Service, puoi confrontare i timestamp sulle tue istanze Amazon EC2 Linux con ClockBound per determinare l'ora vera di un evento. ClockBound misura la precisione dell'orologio della tua istanza EC2 e ti consente di verificare se un determinato timestamp è passato o futuro rispetto all'orologio corrente dell'istanza. Queste informazioni sono utili per determinare l'ordine e la coerenza degli eventi e delle transazioni tra le istanze EC2, indipendentemente dalla posizione geografica di ciascuna istanza.

ClockBound è un demone e una libreria open source. Per saperne di più ClockBound, comprese le istruzioni di installazione, vedi ClockBound su GitHub.

ClockBound è supportato solo per le istanze Linux.

Se utilizzi la connessione PTP diretta al clock hardware PTP, il tuo daemon orario, ad esempio chrony, sottovaluterà il limite di errore del clock. Questo perché un clock hardware PTP non trasmette le informazioni corrette relative all'errore a chrony come invece fa NTP. Di conseguenza, il daemon di sincronizzazione del clock presuppone che il clock sia preciso rispetto all'UTC e quindi abbia un limite di errore pari a `0`. Per misurare l'intero limite di errore, Nitro System calcola il limite di errore dell'orologio hardware PTP e lo rende disponibile all'istanza EC2 tramite il file system `sysfs` del driver ENA. Puoi leggerlo direttamente come valore, in nanosecondi.

Recupero del limite di errore dell'orologio hardware PTP

1. Per prima cosa ottieni la posizione corretta del dispositivo dell'orologio hardware PTP utilizzando uno dei seguenti comandi. Il percorso nel comando è diverso a seconda dell'AMI utilizzata per avviare l'istanza.

   - Per Amazon Linux 2:

     ```
     cat /sys/class/net/eth0/device/uevent | grep PCI_SLOT_NAME
     ```

   - Per Amazon Linux 2023:

     ```
     cat /sys/class/net/ens5/device/uevent | grep PCI_SLOT_NAME
     ```

   l'output è il nome dello slot PCI, che è la posizione dell'orologio hardware PTP. In questo esempio la posizione è `0000:00:03.0`.

   ```
   PCI_SLOT_NAME=0000:00:03.0
   ```

2. Per recuperare l'errore dell'orologio hardware PTP associato, esegui il seguente comando. Includi il nome dello slot PCI della fase precedente.

   ```
   cat /sys/bus/pci/devices/0000:00:03.0/phc_error_bound
   ```

   L'output è il limite di errore del clock hardware PTP, espresso in nanosecondi.

Per calcolare l'errore di clock corretto associato in un momento specifico quando si utilizza la connessione PTP diretta all'orologio hardware PTP, è necessario aggiungere l'errore di clock associato da chrony o ClockBound all'ora in cui viene eseguito il chrony polling dell'orologio hardware PTP. Per ulteriori informazioni sulla misurazione e il monitoraggio della precisione dell'orologio, consulta Gestire la precisione del clock delle istanze Amazon EC2 utilizzando Amazon Time Sync Service e Amazon — Parte 1. CloudWatch

Modifica del fuso orario dell'istanza

Le istanze Amazon EC2 vengono impostate sul fuso orario UTC (Coordinated Universal Time) per impostazione predefinita. È possibile modificare l'ora di un'istanza all'ora locale o a un altro fuso orario della rete.

Consulta le istruzioni relative al sistema operativo della tua istanza.

Linux

> **Important**
>
> Queste informazioni si applicano ad Amazon Linux. Per informazioni su altre distribuzioni, consulta la documentazione specifica.

Per modificare il fuso orario in Amazon Linux

1. Visualizzare l'impostazione del fuso orario corrente del sistema.

   ```
   [ec2-user ~]$ timedatectl
   ```

2. Elencare i fusi orari disponibili.

   ```
   [ec2-user ~]$ timedatectl list-timezones
   ```

3. Impostare il fuso orario scelto.

   ```
   [ec2-user ~]$ sudo timedatectl set-timezone America/Vancouver
   ```

4. (Facoltativo) Verificare che il fuso orario corrente venga aggiornato al nuovo fuso orario eseguendo di nuovo il comando timedatectl.

   ```
   [ec2-user ~]$ timedatectl
   ```

Windows

Modifica del fuso orario su un'istanza Windows

1. Dall'istanza, aprire una finestra del prompt dei comandi.
2. Identificare il fuso orario da utilizzare sull'istanza. Per ottenere un elenco dei fusi orari, utilizzare il comando seguente:

   ```
   tzutil /l
   ```

Questo comando restituisce un elenco di tutti i fusi orari disponibili nel seguente formato:

```
display name
time zone ID
```

3. Individuare l'ID del fuso orario da assegnare all'istanza.
4. Esempio: assegnare il fuso orario UTC:

```
tzutil /s "UTC"
```

Esempio: assegnare l'ora standard del Pacifico:

```
tzutil /s "Pacific Standard Time"
```

Quando modifichi il fuso orario su un'istanza Windows, è necessario assicurarsi che il fuso orario venga mantenuto a seguito dei riavvii del sistema. In caso contrario, al riavvio dell'istanza, viene ripristinato l'orario in formato UTC. Puoi mantenere l'impostazione del fuso orario aggiungendo una chiave di registro RealTimeIsUniversal. Questa chiave è impostata per impostazione predefinita su tutte le istanze della generazione attuale. Per verificare se la chiave di RealTimeIsUniversal registro è impostata, consulta il passaggio 3 nella procedura seguente. Se la chiave non è impostata attieniti alla seguente procedura dall'inizio.

Per impostare la chiave RealTimeIsUniversal di registro

1. Dall'istanza, aprire una finestra del prompt dei comandi.
2. Utilizzare il comando seguente per aggiungere la chiave di registro:

```
reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /
v RealTimeIsUniversal /d 1 /t REG_DWORD /f
```

3. (Opzionale) Verificare che il salvataggio della chiave da parte dell'istanza sia riuscito tramite il comando seguente:

```
reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
\TimeZoneInformation" /s
```

Questo comando restituisce le sottochiavi per la chiave di registro TimeZoneInformation. Alla fine dell'elenco dovrebbe essere visualizzata una chiave RealTimeIsUniversal simile alla seguente:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
    Bias                            REG_DWORD     0x1e0
    DaylightBias                    REG_DWORD     0xffffffc4
    DaylightName                    REG_SZ        @tzres.dll,-211
    DaylightStart                   REG_BINARY    00000300020002000000000000000000
    StandardBias                    REG_DWORD     0x0
    StandardName                    REG_SZ        @tzres.dll,-212
    StandardStart                   REG_BINARY    00000B0001000200000000000000000
    TimeZoneKeyName                 REG_SZ        Pacific Standard Time
    DynamicDaylightTimeDisabled     REG_DWORD     0x0
    ActiveTimeBias                  REG_DWORD     0x1a4
    RealTimeIsUniversal             REG_DWORD     0x1
```

EC2 Capacity Manager

Amazon EC2 Capacity Manager ti aiuta a monitorare, analizzare e gestire l'utilizzo della capacità tra On-Demand istanze, istanze Spot e prenotazioni di capacità da un'unica posizione. Capacity Manager semplifica il monitoraggio della capacità attraverso una dashboard unificata che aggrega i dati di utilizzo con aggiornamenti orari e opportunità di ottimizzazione.

Progettato per grandi aziende e organizzazioni con più account, Capacity Manager elimina la raccolta manuale dei dati da più fonti. Lo strumento fornisce informazioni approfondite su. Regioni AWS Puoi esplorare metriche dettagliate sulla capacità e intraprendere azioni immediate per ottimizzare le risorse cloud.

Quando abiliti l'integrazione AWS delle organizzazioni, puoi visualizzare e analizzare i dati sulla capacità di tutti gli account membri dell'organizzazione da un'unica dashboard. Senza l'integrazione con le organizzazioni, Capacity Manager monitora solo le risorse all'interno dell'individuo Account AWS in cui è abilitato.

> **Note**
>
> - È possibile abilitare Capacity Manager solo in uno Regione AWS per account.

- Tutti i costi visualizzati in Capacity Manager sono costi stimati in base ai On-Demand prezzi pubblicati. Queste stime non includono sconti come Savings Plans o istanze riservate. I costi effettivi potrebbero differire da queste stime.

Caratteristiche chiave

- Dashboard: fornisce una panoramica di alto livello di tutte le prenotazioni di On-Demand capacità On-Demand e dell'utilizzo di Spot, comprese le metriche chiave per contribuire a migliorare il livello di capacità.
- Cross-account e aggregazione interregionale: visualizza l'utilizzo della capacità in tutti gli account membri dell'organizzazione da un'unica dashboard. Capacity Manager aggrega i dati di tutte le regioni della partizione in un'unica regione in cui hai abilitato Capacity Manager, inclusi i dati dei tag. Per i dati relativi a più account, Capacity Manager fornisce anche il nome dell'account come dimensione.
- Tag-based raggruppamento e filtraggio: attiva le chiavi dei tag dalle tue risorse Amazon EC2 (ad esempio, `environment` or`team`) da utilizzare come dimensioni per raggruppare e filtrare le metriche di capacità. Manager-providedI tag di capacità per EC2 Auto Scaling Groups, i nomi dei cluster EKS, i pool di nodi EKS Kubernetes e i pool di nodi Karpenter sono inclusi per impostazione predefinita. Per ulteriori informazioni, consulta Gestione delle chiavi dei tag monitorate.
- Esportazioni di dati: esporta i dati sulla capacità in Amazon S3 in formato CSV o Parquet per ulteriori analisi e report personalizzati.
- API: metriche della capacità di interrogazione a livello di codice che utilizzano e. `GetCapacityManagerMetricData` `GetCapacityManagerMetricDimensions`
- Selettore di data: analizza i dati sulla capacità in intervalli di date da un'ora a 90 giorni.
- Oltre 30 metriche: monitora la capacità delle prenotazioni di capacità, delle istanze e On-Demand delle istanze Spot con oltre 30 metriche.

Abilitazione di EC2 Capacity Manager

Capacity Manager può essere abilitato a due livelli diversi a seconda delle esigenze. Puoi abilitarlo per un singolo Account AWS utente per monitorare le risorse solo all'interno di quell'account o integrarlo con AWS Organizations per una visibilità centralizzata su tutti gli account membri della tua organizzazione.

- Organization-level: visualizza e analizza i dati sulla capacità di tutti gli account membri dell'organizzazione da un'unica dashboard.
- Account-level: monitora l'utilizzo della capacità all'interno di un singolo dispositivo Account AWS.

Argomenti

- Abilitazione di EC2 Capacity Manager con AWS Organizations
- Abilitazione di EC2 Capacity Manager a livello di account
- Registrazione di un amministratore delegato
- Utilizzo di ruoli collegati ai servizi per EC2 Capacity Manager

Abilitazione di EC2 Capacity Manager con AWS Organizations

Puoi abilitare EC2 Capacity Manager with AWS Organizations per la visibilità a livello di organizzazione e la gestione della tua capacità su tutti gli account dei membri. Questa integrazione consente di monitorare, analizzare e gestire l'utilizzo della capacità da una posizione centralizzata.

L'account di gestione è responsabile dell'abilitazione dell'accesso a livello di organizzazione e della gestione della capacità in tutta l'organizzazione.

L'abilitazione di Capacity Manager con AWS le organizzazioni offre i seguenti vantaggi:

- Visibilità centralizzata della capacità: visualizza l'utilizzo della capacità in tutti gli account dei membri nell'organizzazione da un'unica dashboard con aggregazione multi-regione e multi-account.
- Organization-wide ottimizzazione: identifica le prenotazioni di capacità inutilizzate e le opportunità di ottimizzazione in tutti gli account dell'organizzazione.
- Amministratore delegato: consente ad account dei membri specifici di gestire Capacity Manager per un'organizzazione mantenendo al contempo controlli di accesso adeguati.

Se non abiliti l'integrazione con AWS le organizzazioni, puoi monitorare le risorse solo nella persona in Account AWS cui hai abilitato Capacity Manager.

Prerequisiti

- È necessario disporre di un' AWS organizzazione configurata con un account di gestione e uno o più account membri. Per ulteriori informazioni sui vari tipi di account, consultare Terminologia e concetti nella Guida per l'utente di AWS Organizations.
- L'account di gestione deve avere le autorizzazioni per le seguenti operazioni IAM:
  - `organizations:EnableAwsServiceAccess`
  - `organizations:RegisterDelegatedAdministrator` (se si utilizza l'amministrazione delegata)
  - `iam:CreateServiceLinkedRole`
- È necessario creare un ruolo collegato al servizio con lo AWSEC2CapacityManagerServiceRolePolicy use case per consentire l'accesso all' AWS organizzazione. Per ulteriori informazioni, consulta Creating a service-linked role for Capacity Manager.

Abilitazione di Capacity Manager con AWS Organizations

Utilizzando l'account di gestione, abilita l'accesso dell'organizzazione in Capacity Manager.

Console

Per abilitare l'accesso dell'organizzazione in Capacity Manager

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Capacity Manager.
3. Seleziona la scheda Impostazioni.
4. Nella sezione Accesso attendibile, scegli Gestisci accesso attendibile.
5. Nel prompt che appare, seleziona Abilita accesso attendibile. Poi, scegli Salva.

AWS CLI

Per abilitare l'accesso dell'organizzazione in Capacity Manager

1. Crea un ruolo collegato al servizio

```
aws iam create-service-linked-role --aws-service-name
 ec2.capacitymanager.amazonaws.com
```

2. Abilita AWS l'accesso all'organizzazione

```
aws organizations enable-aws-service-access --service-principal
 ec2.capacitymanager.amazonaws.com
```

3. Abilita Capacity Manager con AWS Organization

```
aws ec2 enable-capacity-manager --organizations-access
```

Per aggiornare l'accesso all'organizzazione per un Capacity Manager esistente, esegui il seguente comando:

```
aws ec2 update-capacity-manager-organizations-access --organizations-access
```

PowerShell

Per abilitare l'accesso dell'organizzazione in Capacity Manager

1. Creare un ruolo collegato al servizio utilizzando il cmdlet. New-IAMServiceLinkedRole

```
New-IAMServiceLinkedRole -AWSServiceName "ec2.capacitymanager.amazonaws.com"
```

2. Abilita l'accesso AWS all'organizzazione utilizzando il cmdlet. Enable-ORGAWSServiceAccess

```
Enable-ORGAWSServiceAccess -ServicePrincipal "ec2.capacitymanager.amazonaws.com"
```

3. Abilita Capacity Manager con AWS Organization utilizzando il Enable-EC2CapacityManager cmdlet.

```
Enable-EC2CapacityManager -OrganizationsAccess $true
```

Per aggiornare l'accesso dell'organizzazione per un Capacity Manager esistente, esegui il seguente Update-EC2CapacityManagerOrganizationsAccess cmdlet:

```
Update-EC2CapacityManagerOrganizationsAccess -OrganizationsAccess $true
```

La verifica di Capacity Manager è abilitata con la tua organizzazione

Console

Per verificare che Capacity Manager sia abilitato con la tua organizzazione

1. Nella console di Capacity Manager, scegli Impostazioni.
2. Nella sezione Accesso attendibile, verifica che Accesso all'organizzazione sia visualizzato come Abilitato.
3. Verifica che l'ID dell'organizzazione riporti l'ID della tua organizzazione.

AWS CLI

Per verificare che Capacity Manager sia abilitato con la tua organizzazione

Esegui il comando seguente:

```
aws ec2 get-capacity-manager-attributes
```

L'output dovrebbe mostrare:

```
{
    "CapacityManagerStatus": "enabled",
    "OrganizationsAccess": true,
    "IngestionStatus": "initial-ingestion-pending",
    "IngestionStatusMessage": "Capacity Manager is collecting historical data from
 2025-10-01T00:00:00Z. Data collection is in progress and may take several hours to
 complete."
```

```
}
```

PowerShell

Per verificare che Capacity Manager sia abilitato con la tua organizzazione

Utilizza il cmdlet Get-EC2CapacityManagerAttribute.

```
Get-EC2CapacityManagerAttribute
```

L'output dovrebbe mostrare:

```
CapacityManagerStatus      : enabled
DataExportCount            : 0
EarliestDatapointTimestamp :
IngestionStatus            : initial-ingestion-in-progress
IngestionStatusMessage     : Capacity Manager is collecting historical data from
                             2026-03-17T16:00:00Z. Data collection is in progress
 and may take
                             several hours to complete.
LatestDatapointTimestamp   :
OrganizationsAccess        : True
```

Considerazioni

- Service-linked creazione del ruolo: quando si abilita l'accesso dell'organizzazione tramite la console, Capacity Manager crea automaticamente il ruolo AWSServiceRoleForEC2CapacityManager collegato al servizio in tutti gli account dei membri. Se si abilita tramite il AWS CLI, è necessario chiamare `createServiceLinkedRole` manualmente.
- Aggregazione dei dati: dopo aver abilitato l'accesso all'organizzazione, Capacity Manager riempie 14 giorni di dati storici da tutti gli account dei membri. In genere, il completamento del processo richiede alcuni minuti.
- Limitazioni regionali: è possibile abilitare Capacity Manager solo in una regione per organizzazione, ma verranno aggregati i dati di tutte le regioni commerciali.
- Autorizzazioni: gli account dei membri non devono eseguire alcuna operazione. Capacity Manager utilizza il ruolo collegato al servizio per scoprire automaticamente le risorse in tutti gli account.

Abilitazione di EC2 Capacity Manager a livello di account

Abilita Capacity Manager a livello di account per monitorare e analizzare l'utilizzo della capacità EC2 all'interno di un singolo account. AWS Dopo averlo abilitato, Capacity Manager raccoglie i dati sulle On-Demand istanze, sulle istanze Spot e sulle prenotazioni di capacità per aiutarti a identificare le opportunità di ottimizzazione e tenere traccia dei modelli di utilizzo.

Abilita Capacity Manager a livello di account

Console

Per abilitare Capacity Manager per il tuo account

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Capacity Manager.
3. Nella pagina di Capacity Manager, scegli Abilita nella regione.

AWS CLI

Per abilitare Capacity Manager per il tuo account

Esegui il comando seguente:

```
aws ec2 enable-capacity-manager
```

PowerShell

Per abilitare Capacity Manager per il tuo account

Utilizza il cmdlet Enable-EC2CapacityManager.

```
Enable-EC2CapacityManager
```

> **Note**
>
> - Dopo la sua abilitazione, Capacity Manager raccoglie e aggrega 14 giorni di dati storici. Questo processo potrebbe richiedere alcune ore.

- Durante la raccolta dei dati storici, viene visualizzato uno `initial-ingestion-in-progress` stato. Durante questo periodo di raccolta, potresti osservare delle lacune nei dati storici. Quando la raccolta dei dati è completa, viene visualizzato uno `ingestion-complete` stato.

Registrazione di un amministratore delegato

Puoi registrare un amministratore delegato per Capacity Manager. Ciò consente a un account membro di gestire Capacity Manager per la tua AWS organizzazione. Solo l'account di gestione può registrare o rimuovere un amministratore delegato nella tua organizzazione.

> **Note**
>
> Non puoi disattivare Capacity Manager per la tua organizzazione se è presente un amministratore delegato registrato.

Argomenti

- Prerequisiti
- Registrazione di un amministratore delegato
- Rimozione di un amministratore delegato

Prerequisiti

Il tuo account di gestione deve aver abilitato Capacity Manager with AWS Organizations. Per ulteriori informazioni, consulta Abilitazione di EC2 Capacity Manager con AWS Organizations.

Registrazione di un amministratore delegato

Puoi registrare un amministratore delegato utilizzando la console Amazon EC2, o. AWS CLI PowerShell

Console

Per registrare un amministratore delegato per

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, scegli Capacity Manager.
3. Seleziona la scheda Impostazioni.
4. Nella sezione Amministratore delegato, scegli Aggiungi.
5. Nel prompt che appare, inserisci l'ID dell'account del membro dell'organizzazione che vuoi aggiungere come amministratore delegato.
6. Scegliere Add delegated administrator (Aggiungi amministratore delegato).

AWS CLI

Per registrare un amministratore delegato per

Esegui il comando seguente:

```
aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal ec2.capacitymanager.amazonaws.com
```

PowerShell

Per registrare un amministratore delegato per

Utilizza il cmdlet Register-ORGDelegatedAdministrator.

```
Register-ORGDelegatedAdministrator `
    -AccountId "123456789012" `
    -ServicePrincipal "ec2.capacitymanager.amazonaws.com"
```

Rimozione di un amministratore delegato

Puoi rimuovere un amministratore delegato utilizzando la console Amazon EC2, o. AWS CLI PowerShell

Console

Per rimuovere un amministratore delegato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, scegli Capacity Manager.
3. Seleziona la scheda Impostazioni.
4. Nella sezione Amministratore delegato, scegli Gestisci.
5. Nel prompt che appare, scegli Rimuovi amministratore delegato.

AWS CLI

Per rimuovere un amministratore delegato

Esegui il comando seguente:

```
aws organizations deregister-delegated-administrator \
    --account-id 123456789012 \
    --service-principal ec2.capacitymanager.amazonaws.com
```

PowerShell

Per rimuovere un amministratore delegato

Utilizza il cmdlet Unregister-ORGDelegatedAdministrator.

```
Unregister-ORGDelegatedAdministrator `
    -AccountId "123456789012" `
    -ServicePrincipal "ec2.capacitymanager.amazonaws.com"
```

Utilizzo di ruoli collegati ai servizi per EC2 Capacity Manager

EC2 Capacity Manager 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 Capacity Manager. Service-linked i ruoli sono predefiniti da Capacity Manager e includono tutte le autorizzazioni necessarie al servizio per chiamare altri AWS servizi per conto dell'utente.

Un ruolo collegato al servizio semplifica la configurazione di Capacity Manager perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Capacity Manager definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, solo Capacity

Manager potrà assumere i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato al servizio solo dopo avere eliminato le risorse correlate. Questa procedura protegge le risorse di Capacity Manager 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 dei ruoli. 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 Capacity Manager

Capacity Manager utilizza il ruolo collegato al servizio denominato AWSServiceRoleForEC2CapacityManager per consentire all'utente di gestire le risorse di capacità e di integrarsi con le AWS organizzazioni per conto dell'utente.

Il ruolo AWSServiceRoleForEC2CapacityManager collegato ai servizi prevede che i seguenti servizi assumano il ruolo:

- `ec2.capacitymanager.amazonaws.com`

La politica di autorizzazione del ruolo denominata AWSEC2CapacityManagerServiceRolePolicy consente a Capacity Manager di completare le seguenti azioni:

- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListChildren`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta le autorizzazioni dei Service-linked ruoli nella IAM User Guide.

Creazione di un ruolo collegato ai servizi per Capacity Manager

Puoi utilizzare la console IAM per creare un ruolo collegato al servizio con il AWSEC2CapacityManagerServiceRolePolicy caso d'uso. Nell'API AWS CLI o nell' AWS API, crea un ruolo collegato al servizio con il nome del servizio. `ec2.capacitymanager.amazonaws.com` Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, è possibile utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato ai servizi per Capacity Manager

Capacity Manager non consente di modificare il ruolo collegato al AWSServiceRoleForEC2CapacityManager servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Capacity Manager

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare quel ruolo. 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 Capacity Manager 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 rimuovere le risorse di Capacity Manager utilizzate da AWSServiceRoleForEC2CapacityManager

1. Tutti gli amministratori delegati devono aver disabilitato il proprio Capacity Manager prima di rimuovere l'accesso alle organizzazioni.
2. Devi eliminare tutte le esportazioni di dati attive prima di disabilitare un gestore di capacità.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Usa la console IAM AWS CLI, l'API o l' AWS API per eliminare il ruolo AWSServiceRoleForEC2CapacityManager collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi di Capacity Manager

Capacity Manager supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per maggiori informazioni, consulta Regioni ed endpoint di AWS.

Capacity Manager non supporta l'utilizzo di ruoli collegati ai servizi in ogni regione nella quale è disponibile il servizio. Puoi utilizzare il AWSServiceRoleForEC2CapacityManager ruolo nelle seguenti regioni.

Nome della Regione	Identità della Regione	Supporto in Capacity Manager
Stati Uniti orientali (Virginia settentrionale)	us-east-1	Sì
Stati Uniti orientali (Ohio)	us-east-2	Sì
Stati Uniti occidentali (California settentrionale)	us-west-1	Sì
Stati Uniti occidentali (Oregon)	us-west-2	Sì
Africa (Città del Capo)	af-south-1	No
Asia Pacific (Hong Kong)	ap-east-1	No
Asia Pacifico (Giacarta)	ap-southeast-3	No
Asia Pacifico (Mumbai)	ap-south-1	Sì
Asia Pacifico (Osaka)	ap-northeast-3	Sì
Asia Pacifico (Seoul)	ap-northeast-2	Sì
Asia Pacifico (Singapore)	ap-southeast-1	Sì
Asia Pacifico (Sydney)	ap-southeast-2	Sì

Nome della Regione	Identità della Regione	Supporto in Capacity Manager
Asia Pacifico (Tokyo)	ap-northeast-1	Sì
Canada (Centrale)	ca-central-1	Sì
Europa (Francoforte)	eu-central-1	Sì
Europa (Irlanda)	eu-west-1	Sì
Europa (Londra)	eu-west-2	Sì
Europe (Milan)	eu-south-1	No
Europa (Parigi)	eu-west-3	Sì
Europa (Stoccolma)	eu-north-1	Sì
Medio Oriente (Bahrein)	me-south-1	No
Medio Oriente (Emirati Arabi Uniti)	me-central-1	No
Sud America (San Paolo)	sa-east-1	Sì
AWS GovCloud (US-East)	us-gov-east-1	No
AWS GovCloud (US-West)	us-gov-west-1	No

Organizzazione dei dati in Capacity Manager

Capacity Manager utilizza una combinazione di metriche, punti dati, dimensioni, intervalli di date e periodi per organizzare i dati sulla capacità. Questo può aiutarti ad analizzare i modelli di utilizzo e a prendere decisioni informate sulle tue risorse.

Metriche e punti dati

Una metrica è un set di punti dati in ordine cronologico. Ad esempio, se vuoi monitorare l'utilizzo di spot in vCPU, utilizzeresti la metrica `SpotTotalUsageHrsVcpu`.

Ogni ora, la metrica genera un punto dati con timestamp con l'utilizzo di spot in ore vCPU. Ad esempio, se hai utilizzato 100 vCPU durante l'ora 10:00, Capacity Manager crea un punto dati con un timestamp delle 10:00 e un valore di 100.

Per l'elenco completo delle metriche analizzate da Capacity Manager, consulta Metriche di EC2 Capacity Manager.

Dimensioni

Le dimensioni sono coppie nome-valore che aiutano a classificare e identificare diversi aspetti di una metrica. Ad esempio, il nome di una dimensione in Capacity Manager è AccountID, dove il valore è l'ID effettivo dell'account. Capacity Manager fornisce dimensioni per segmentare e raggruppare i dati, ad esempio Famiglia di istanze, ARN della prenotazione, tipo di prenotazione e tenancy.

Oltre alle dimensioni integrate, puoi attivare le chiavi dei tag dalle tue risorse Amazon EC2 da utilizzare come dimensioni personalizzate. Ad esempio, se le tue istanze sono contrassegnate con `environment oteam`, puoi attivare quelle chiavi di tag e quindi raggruppare e filtrare le metriche di capacità in base ai relativi valori.

Capacity Manager fornisce anche Manager-provided tag Capacity, come EC2 Auto Scaling Group (`aws:autoscaling:groupName`), EKS cluster name (`aws:eks:cluster-name`), pool di nodi EKS Kubernetes () e pool di nodi Karpenter (`eks:kubernetes-node-pool-name`), disponibili per impostazione predefinita senza essere conteggiati ai `karpenter.sh/nodepool` fini del limite delle chiavi dei tag.

Per l'elenco completo delle dimensioni, consulta Metriche di EC2 Capacity Manager. Per informazioni sull'attivazione e la gestione delle dimensioni dei tag, vedere. Gestione delle chiavi dei tag monitorate

Intervallo di date e periodo

L'intervallo di date specifica la quantità di tempo desiderata per l'analisi, da un'ora a 90 giorni.
Il periodo determina in che modo Capacity Manager aggrega i dati nel tempo e quanti punti dati restituire. Ad esempio, se l'intervallo di date è di una settimana e il periodo è di 1 giorno, Capacity Manager restituisce 7 punti dati. Ciascun punto dati rappresenta un giorno di dati aggregati. Il periodo deve essere un intervallo di un'ora e dividersi equamente nell'intervallo di date.

Argomenti

- Metriche di EC2 Capacity Manager
- Raggruppamento e filtraggio dei dati

- Gestione delle chiavi dei tag monitorate

Metriche di EC2 Capacity Manager

Capacity Manager offre una selezione completa di metriche per monitorare la capacità tra diversi tipi di risorse. Le metriche possono essere misurate utilizzando unità diverse a seconda delle esigenze di analisi.

I nomi delle metriche in Capacity Manager utilizzano quattro prefissi diversi per categorizzare il tipo di capacità misurata:

- `Reservation`: le prenotazioni della capacità stesse, tra cui la capacità riservata totale, i tassi di utilizzo, la capacità inutilizzata e il numero di prenotazioni.
- `Reserved`— Utilizzo dell' On-Demand istanza coperto dalle tue prenotazioni di capacità.
- `Unreserved`— Utilizzo dell' On-Demand istanza che non rientra nelle prenotazioni di capacità.
- `Spot`: specificamente per l'utilizzo delle istanze spot, compresi il runtime e i costi stimati. Queste metriche sono separate dalla capacità basata sulle prenotazioni.

La tabella seguente fornisce anche le dimensioni disponibili per ogni metrica. Le categorie di dimensioni sono suddivise nel modo seguente:

- Dimensioni generali della capacità: ID dell'account, nome dell'account, regione, famiglia di istanze, zona di disponibilità, tipo di istanza, piattaforma e locazione
- Dimensioni della prenotazione della capacità: ID della prenotazione (ID della prenotazione della capacità), ARN della prenotazione, proprietario finanziario inutilizzato, tipo di prenotazione (ODCR/ Capacity blocco), data e ora di creazione, timestamp di inizio, timestamp di fine, stato e criteri di corrispondenza dell'istanza.
- Dimensioni di utilizzo riservate: ID di prenotazione (CRID), ARN della prenotazione, tipo di prenotazione
- Dimensioni dei tag: chiavi dei tag e tag di capacità. Customer-managed Manager-provided È necessario attivare una chiave tag prima di poterla utilizzare come dimensione. Per ulteriori informazioni, consulta Gestione delle chiavi dei tag monitorate.

Parametro	Description	Dimensioni disponibili	Unità disponibili
`ReservationAvgCommittedSize`	La quantità totale media di capacità in uno stato attivo o pianificato con un impegno. La dimensione viene sommata tra le dimensioni e calcolata come media nel tempo.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza
`ReservationAvgFutureSize`	Il numero medio di prenotazioni della capacità programmate per l'avvio in futuro ma che non sono ancora diventate attive durante il periodo selezionato. La dimensione viene sommata tra le dimensioni e calcolata come media nel tempo.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza
`ReservationAvgUtilization`	La percentuale media della capacità riservata utilizzata nel periodo selezionato.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza
`ReservationMaxCommittedSize`	La capacità totale massima in uno stato attivo o pianificato con un impegno. La dimensione viene sommata tra le dimensioni e viene preso il valore massimo per il periodo.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza
`ReservationMaxFutureSize`	Il numero massimo di prenotazioni della capacità programmate per l'avvio in futuro ma che non sono ancora diventate attive durante il periodo selezionato.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza

Parametro	Description	Dimensioni disponibili	Unità disponibili
	La dimensione viene sommata tra le dimensioni e viene preso il valore massimo per il periodo.		
`ReservationMaxSize`	La dimensione massima raggiunta dalla prenotazione della capacità in qualsiasi momento durante il periodo selezionato. ID di prenotazione obbligatorio.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza
`ReservationMaxUnusedSize`	La quantità massima di capacità non utilizzata nella prenotazione della capacità in qualsiasi momento durante il periodo selezionato. ID di prenotazione obbligatorio.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza
`ReservationMaxUtilization`	La percentuale di utilizzo massima ottenuta dalla prenotazione della capacità in qualsiasi momento durante il periodo selezionato. ID di prenotazione obbligatorio.	Dimensione della capacità generale e della prenotazione della capacità	
`ReservationMinCommittedSize`	La quantità totale minima di capacità in uno stato attivo o pianificato con un impegno. La dimensione viene sommata tra le dimensioni e viene preso il valore minimo per il periodo.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza

Parametro	Description	Dimensioni disponibili	Unità disponibili
`ReservationMinFutureSize`	Il numero minimo di prenotazioni della capacità programmate per l'avvio in futuro ma che non sono ancora diventate attive in qualsiasi momento durante il periodo selezionato. La dimensione viene sommata tra le dimensioni e viene preso il valore minimo per il periodo.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza
`ReservationMinSize`	La dimensione minima raggiunta dalla prenotazione della capacità in qualsiasi momento durante il periodo selezionato. ID di prenotazione obbligatorio.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza
`ReservationMinUnusedSize`	La quantità minima di capacità non utilizzata nella prenotazione della capacità in qualsiasi momento durante il periodo selezionato. ID di prenotazione obbligatorio.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza
`ReservationMinUtilization`	La percentuale di utilizzo minima ottenuta dalla prenotazione della capacità in qualsiasi momento durante il periodo selezionato. ID di prenotazione obbligatorio.	Dimensione della capacità generale e della prenotazione della capacità	

Parametro	Description	Dimensioni disponibili	Unità disponibili
`ReservationTotalCapacityHrs`	Quantità totale di capacità prenotata tramite Prenotazioni della capacità durante il periodo selezionato.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza
`ReservationTotalCount`	Il numero totale di prenotazioni della capacità diverse disponibili durante il periodo selezionato.	Dimensione della capacità generale e della prenotazione della capacità	
`ReservationTotalEstimatedCost`	Costo stimato delle ore di capacità totali riservate nel periodo selezionato.	Dimensione della capacità generale e della prenotazione della capacità	
`ReservationUnusedTotalCapacityHrs`	Quantità totale di capacità riservata disponibile ma non utilizzata durante il periodo selezionato.	Dimensione della capacità generale e della prenotazione della capacità	vCPU, istanza
`ReservationUnusedTotalEstimatedCost`	Costo stimato della capacità riservata che avevi ma non hai utilizzato durante il periodo selezionato (calcolato utilizzando On-Demand le tariffe).	Dimensione della capacità generale e della prenotazione della capacità	
`ReservedTotalEstimatedCost`	Costo stimato dell'utilizzo dell' On-Demand istanza coperto da una prenotazione di capacità durante il periodo selezionato. Questo esclude l'utilizzo spot.	Dimensione della capacità generale e dell'utilizzo riservato	

Parametro	Description	Dimensioni disponibili	Unità disponibili
`ReservedTotalUsageHrs`	Ore totali di utilizzo dell' On-Demand istanza coperte da una prenotazione di capacità durante il periodo selezionato. Questo esclude l'utilizzo spot.	Dimensione della capacità generale e dell'utilizzo riservato	vCPU, istanza
`SpotAvgRunTimeBeforeInterruption`	Durata media in ore per le istanze interrotte nel periodo selezionato.	Solo dimensioni di regione, zona di disponibilità e ID account	Istanza
`SpotInterruptionRate`	Percentuale di istanze Spot in esecuzione che sono state interrotte nel periodo selezionato.	Solo dimensioni di regione, zona di disponibilità e ID account	vCPU, istanza
`SpotMaxRunTimeBeforeInterruption`	Durata massima in ore per le istanze interrotte nel periodo selezionato.	Solo dimensioni di regione, zona di disponibilità e ID account	Istanza
`SpotMinRunTimeBeforeInterruption`	Durata minima in ore per le istanze interrotte nel periodo selezionato.	Solo dimensioni di regione, zona di disponibilità e ID account	Istanza
`SpotTotalCount`	Numero di istanze Spot o vCPU in esecuzione durante il periodo selezionato.	Solo dimensioni di regione, zona di disponibilità e ID account	vCPU, istanza
`SpotTotalEstimatedCost`	Costo stimato dell'utilizzo dell'istanza spot nel periodo selezionato (calcolato utilizzando le tariffe spot pubblicate).	Dimensioni generali della capacità	

Parametro	Description	Dimensioni disponibili	Unità disponibili
`SpotTotal Interruptions`	Numero di istanze Spot o vCPU interrotte durante il periodo selezionato.	Solo dimensioni di regione, zona di disponibilità e ID account	vCPU, istanza
`SpotTotal UsageHrs`	Ore totali di utilizzo dell'ista nza Spot durante il periodo selezionato.	Dimensioni generali della capacità	vCPU, istanza
`Unreserve dTotalEst imatedCost`	Costo stimato dell'utilizzo delle On-Demand istanze non coperto da una prenotazione di capacità durante il periodo selezionato. Questo esclude l'utilizzo spot.	Dimensioni generali della capacità	
`Unreserve dTotalUsageHrs`	Ore totali di utilizzo dell' On-Demand istanza non coperte da una prenotazione di capacità durante il periodo selezionato. Questo esclude l'utilizzo spot.	Dimensioni generali della capacità	vCPU, istanza

> **Note**
>
> Se includi istanze nelle tue unità, ti consigliamo di includere il tipo di istanza nelle dimensioni.

Dimensioni dei tag

Oltre alle dimensioni integrate nella sezione precedente, Capacity Manager supporta le dimensioni dei tag. Le dimensioni dei tag consentono di raggruppare e filtrare le metriche utilizzando le chiavi dei tag delle risorse Amazon EC2.

Customer-managed dimensioni dei tag

È possibile attivare fino a cinque tasti tag da utilizzare come dimensioni. Dopo l'attivazione e `activated` lo stato, le dimensioni dei tag sono disponibili per le metriche che supportano le dimensioni di capacità generale. Per l'elenco completo delle categorie di dimensioni, vedereMetriche di EC2 Capacity Manager.

Dimensione	Description	Valori di esempio
Nome chiave di tag	Una chiave tag gestita dal cliente proveniente dalle tue risorse Amazon EC2.	`environment` , `team`, `cost-center`

Dimensioni del tag di capacità Manager-provided

Per impostazione predefinita, Capacity Manager fornisce i seguenti Manager-provided tag Capacity. I Manager-provided tag di capacità sono sempre disponibili e non vengono conteggiati ai fini del limite chiave dei tag.

Dimensione	Description
`tag:aws:autoscaling:groupName`	Il nome del gruppo EC2 Auto Scaling associato all'istanza.
`tag:aws:eks:cluster-name`	Il nome del cluster EKS associato all'istanza.
`tag:eks:kubernetes-node-pool-name`	Il pool di nodi EKS Kubernetes associato all'istanza.
`tag:karpenter.sh/nodepool`	Il pool di nodi Karpenter associato all'istanza.

> **Note**
>
> Quando si raggruppa in base a una dimensione del tag, le risorse che non hanno un valore per quel tag vengono incluse in un bucket separato con un valore di stringa vuoto. Ciò garantisce che i totali tengano conto di tutte le risorse.

Raggruppamento e filtraggio dei dati

Capacity Manager aggrega le metriche in base alle dimensioni e al periodo di date scelti. Se non viene scelta alcuna dimensione, Capacity Manager aggrega i dati e restituisce un punto dati per periodo nell'intervallo di date. Puoi raggruppare i tuoi dati in aggregazioni più piccole aggiungendo dimensioni, incluse le dimensioni dei tag dalle tue risorse Amazon EC2.

- Raggruppamento: suddividi i dati sulla capacità in base a dimensioni come regione, famiglia di istanze, ID account o chiavi di tag. Puoi raggruppare le metriche in base a più dimensioni per suddividere ulteriormente i dati. Ad esempio, se raggruppi per regione e zona di disponibilità, ottieni un punto dati per ogni regione e combinazione AZ dove disponi di utilizzo.
- Filtraggio: mostra solo sottoinsiemi specifici delle dimensioni selezionate. Ad esempio, se raggruppi per famiglia di istanze, otterrai punti dati per tutte le famiglie in cui disponi di utilizzo. Tuttavia, se filtri anche per p5, vedrai solo i punti dati per la famiglia di istanze p5. Puoi anche filtrare in base ai valori dei tag, ad esempio `environment=prod` per visualizzare solo le risorse di produzione. Per filtrare le risorse che non hanno un valore per un tag selezionato, filtra in base a un valore vuoto.
- Unità delle metriche: visualizza i risultati per unità diverse come vCPU, istanze o costi stimati. Ad esempio, dopo il raggruppamento per regione e il filtro per una famiglia di istanze specifica, puoi passare dal totale delle vCPU utilizzate, al numero di istanze in esecuzione o ai costi stimati.

Come raggruppare e filtrare i dati nella console

Per raggruppare e filtrare i dati in Capacity Manager

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Capacity Manager.
3. Scegli la scheda relativa al tipo di risorsa che vuoi analizzare: Utilizzo, Prenotazioni o Spot.
4. Nella sezione Filtro data, scegli un intervallo di date, il fuso orario e l'intervallo.
5. Nella sezione Filtro dimensione, scegli una dimensione dal menu a discesa Seleziona una dimensione. Le opzioni di dimensione sono diverse per ogni tipo di risorsa. Per ulteriori informazioni, consulta Metriche di EC2 Capacity Manager.

   Per raggruppare in base alla dimensione del tag, scegli la chiave del tag dal menu a discesa (ad esempio,`environment`). Sono disponibili solo le chiavi dei tag nello `activated` stato. Per ulteriori informazioni sull'attivazione dei tag key, vedereGestione delle chiavi dei tag monitorate.

Puoi aggiungere più dimensioni, incluse più dimensioni di tag, per creare raggruppamenti più granulari.

6. Per filtrare in base alle dimensioni selezionate, scegli un'opzione di filtro dal menu a discesa Filtra per dimensione.

   Per le dimensioni dei tag, il filtro mostra i valori dei tag presenti nei tuoi dati. Per filtrare le risorse senza un valore per il tag selezionato, scegli l'opzione con valore vuoto.

7. Nella sezione Aggregazioni, scegli un'unità per visualizzare i risultati per vCPU, istanze o costi stimati.

> **Note**
>
> Quando si raggruppa in base a una dimensione del tag, le risorse che non hanno un valore per quel tag vengono incluse in un gruppo separato con un valore vuoto. Ciò garantisce che i totali tengano conto di tutte le risorse, non solo di quelle con tag.

Gestione delle chiavi dei tag monitorate

Amazon EC2 Capacity Manager ti consente di selezionare le chiavi di tag dalle tue risorse Amazon EC2 (ad esempio, `environment` o `team`) da utilizzare come dimensioni durante l'analisi dei dati sulla capacità. Dopo l'attivazione di una chiave di tag, puoi raggruppare e filtrare le metriche in base ai valori di quel tag, proprio come puoi fare con la regione, il tipo di istanza o la zona di disponibilità.

Ogni account può monitorare fino a cinque tag key. Manager-provided I tag di capacità non vengono conteggiati ai fini di questo limite.

Argomenti

- Manager-provided Tag di capacità
- Ciclo di vita dei tag
- Attiva e disattiva le chiavi dei tag monitorate
- Visualizza le chiavi dei tag monitorate
- Metriche di interrogazione che utilizzano le dimensioni dei tag
- Tag nelle esportazioni di dati
- Organizzazioni e amministratore delegato

- Considerazioni

Manager-provided Tag di capacità

Capacity Manager include un set di tag predefiniti per ogni account. Questi non vengono conteggiati ai fini del limite di tag key. I Manager-provided tag di capacità rappresentano le dimensioni di raggruppamento più utilizzate e includono:

- `aws:autoscaling:groupName`— Gruppo EC2 Auto Scaling
- `aws:eks:cluster-name`— Nome del cluster EKS
- `eks:kubernetes-node-pool-name`— pool di nodi EKS Kubernetes
- `karpenter.sh/nodepool`— Pool di nodi Karpenter

Manager-provided I tag di capacità vengono visualizzati `GetCapacityManagerMonitoredTagKeys` con `CapacityManagerProvided` impostato su `true` e non possono essere attivati o disattivati dal cliente. Quando Capacity Manager viene abilitato per la prima volta, `activating` lo stato dei Manager-provided tag di capacità inizia e passa a `activated` dopo che Capacity Manager riceve il primo data point che include un Manager-provided tag di capacità, in genere entro una o due ore.

Ciclo di vita dei tag

Le chiavi dei tag monitorate passano attraverso i seguenti stati:

Stato	Description
`activating`	La chiave del tag è registrata. Capacity Manager si sta preparando a raccogliere i dati per questo tag. Non è possibile interrogare le metriche utilizzando un tag in questo stato.
`activated`	I dati dei tag vengono inseriti e possono essere interrogati tramite le API delle metriche e nelle esportazioni di dati.
`suspended`	La chiave del tag ha superato la soglia di 100.000 valori di tag univoci. Il tag viene comunque conteggiato ai fini del limite, ma Capacity Manager non inserisce più i relativi dati. Se l'utilizzo del valore del tag scende

Stato	Description
	al di sotto della soglia per un periodo prolungato, il tag viene riattivato automaticamente.
`deactivating`	La chiave del tag viene rimossa. Non apparirà più in una volta completat a `GetCapacityManagerMonitoredTagKeys` la disattivazione.

Quando un tag è in `suspended` stato, `GetCapacityManagerMonitoredTagKeys` restituisce il seguente messaggio di stato: «Tag sospeso a causa di troppi valori di tag. Riduci l'uso del tag o disattivalo».

> **Note**
>
> Se si disattiva una chiave tag e successivamente si riattiva la stessa chiave, è possibile interrogare solo i dati inseriti dopo la riattivazione. I dati storici dell'attivazione precedente non sono accessibili. I `EarliestDatapointTimestamp` ripristini ad ogni nuova attivazione.

Attiva e disattiva le chiavi dei tag monitorate

Puoi attivare i tag key per iniziare a monitorarli come dimensioni oppure disattivare i tag key che non ti servono più. L'attivazione è asincrona: il tag entra in uno `activating` stato e passa a `activated` dopo che Capacity Manager inizia a ricevere i dati per quel tag. La disattivazione rimuove la chiave del tag dal set monitorato.

> **Note**
>
> Quando si attiva una chiave tag, immettete solo il nome della chiave (ad esempio,`environment`). Capacity Manager lo rende automaticamente disponibile come dimensione per il raggruppamento e il filtraggio delle metriche.

Console

Per attivare o disattivare le chiavi dei tag monitorate

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, scegli Capacity Manager.
3. Seleziona la scheda Impostazioni.
4. Nella sezione Chiavi dei tag monitorati, scegli Gestisci le chiavi dei tag.
5. Per attivare un tag key, inserisci il nome del tag key e scegli Aggiungi. Per disattivare un tag key, seleziona il tag key e scegli Rimuovi.
6. Scegli Save changes (Salva modifiche).

AWS CLI

Per attivare i tag keys

Utilizzate il seguente comando per attivare uno o più tag key:

```
aws ec2 update-capacity-manager-monitored-tag-keys \
    --activate-tag-keys "environment" "teamId"
```

L'output mostra le chiavi dei tag e i loro stati iniziali:

```
{
    "CapacityManagerTagKeys": [
        {
            "TagKey": "environment",
            "Status": "activating"
        },
        {
            "TagKey": "teamId",
            "Status": "activating"
        }
    ]
}
```

Per disattivare i tag keys

Usa il seguente comando per disattivare una o più chiavi di tag:

```
aws ec2 update-capacity-manager-monitored-tag-keys \
    --deactivate-tag-keys "project"
```

L'output mostra gli stati aggiornati:

```
{
    "CapacityManagerTagKeys": [
        {
            "TagKey": "project",
            "Status": "deactivating"
        }
    ]
}
```

Puoi attivare e disattivare le chiavi dei tag nella stessa richiesta:

```
aws ec2 update-capacity-manager-monitored-tag-keys \
    --activate-tag-keys "environment" "teamId" \
    --deactivate-tag-keys "project"
```

Visualizza le chiavi dei tag monitorate

Puoi visualizzare tutti i tag key monitorati per il tuo account, incluso il loro stato attuale e il primo timestamp a cui sono disponibili i dati.

Console

Per visualizzare le chiavi dei tag monitorate

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Capacity Manager.
3. Seleziona la scheda Impostazioni.
4. Nella sezione Chiavi dei tag monitorate, visualizza le chiavi dei tag, il loro stato e se sono Manager-provided tag di capacità.

AWS CLI

Per visualizzare le chiavi dei tag monitorate

Esegui il comando seguente:

```
aws ec2 get-capacity-manager-monitored-tag-keys
```

L'output elenca tutte le chiavi dei tag, inclusi i Manager-provided tag Capacity e i tag gestiti dal cliente:

```
{
    "CapacityManagerTagKeys": [
        {
            "TagKey": "aws:autoscaling:groupName",
            "Status": "activated",
            "CapacityManagerProvided": true,
            "earliestDatapointTimestamp": "2026-04-08T00:00:00"
        },
        {
            "TagKey": "environment",
            "Status": "activated",
            "CapacityManagerProvided": false,
            "earliestDatapointTimestamp": "2025-08-11T22:00:00"
        }
    ]
}
```

Il `CapacityManagerProvided` campo indica se un tag è un tag Capacity (`true`) o un Manager-provided tag gestito dal cliente (). `false` Manager-provided I tag di capacità non vengono conteggiati ai fini del limite chiave dei tag. `EarliestDatapointTimestamp`Indica il primo momento a partire dal quale i dati sono disponibili per quella chiave del tag.

Metriche di interrogazione che utilizzano le dimensioni dei tag

Dopo che una chiave del tag ha raggiunto `activated` lo stato, puoi utilizzarla come dimensione in `GetCapacityManagerMetricDimensions` e`GetCapacityManagerMetricData`.

Per interrogare le metriche raggruppate in base a una dimensione del tag

Utilizza il seguente comando:

```
aws ec2 get-capacity-manager-metric-dimensions \
    --group-by tag:environment account-id \
    --filter-by
 'DimensionCondition={Dimension=tag:environment,Comparison=equals,Values=[prod]}'
```

Quando esegui il raggruppamento in base a una dimensione del tag, i risultati includono tutte le risorse del tuo account, non solo quelle che hanno il tag. Le risorse che non hanno un valore per il tag vengono raggruppate in un bucket separato con un valore di stringa vuoto. Ad esempio, se il tuo account ha utilizzato 800 ore di vCPU in un determinato periodo e solo alcune di queste risorse hanno un `environment` tag, il raggruppamento in base alla chiave del `environment` tag potrebbe restituire:

- `prod`— 300 ore di vCPU
- `staging`— 200 ore di vCPU
- `""`(stringa vuota) — 300 ore di vCPU da risorse senza tag `environment`

Ciò garantisce che i totali relativi a tutti i bucket rappresentino l'utilizzo completo. Puoi filtrare in modo esplicito le risorse senza tag passando una stringa vuota come valore del filtro:

```
--filter-by
 'DimensionCondition={Dimension=tag:environment,Comparison=equals,Values=[""]}'
```

> **Note**
>
> Se esegui una query con una chiave tag che è ancora in `activating` stato, la query viene rifiutata con un errore 400. Attendi che lo stato del tag passi a `activated` prima di eseguire l'interrogazione. Puoi controllare lo stato usando`GetCapacityManagerMonitoredTagKeys`.

> **Note**
>
> Le interrogazioni con un'ora di inizio precedente a quella `EarliestDatapointTimestamp` di qualsiasi dimensione del tag fornita vengono rifiutate.

`GetCapacityManagerMonitoredTagKeys`Da utilizzare per verificare quando i dati sono diventati disponibili per ogni tag.

Tag nelle esportazioni di dati

Quando abiliti il monitoraggio dei tag, le esportazioni dei dati includono le chiavi dei tag attivate e i Manager-provided tag Capacity come colonne aggiuntive. Le colonne dei tag vengono visualizzate dopo tutte le colonne standard con intestazioni come `tag:environment` `etag:team`. Le colonne dei tag sono ordinate alfabeticamente.

Le esportazioni includono solo i tag in `activated` stato. Capacity Manager esclude `activating` i `deactivating` tag con `suspended` stato o.

> **Note**
>
> Se si attiva una nuova chiave di tag, le esportazioni di dati esistenti non includono automaticamente il nuovo tag. È necessario creare una nuova esportazione di dati per includere la chiave tag appena attivata come colonna.

Organizzazioni e amministratore delegato

Quando il tuo account fa parte di un' AWS organizzazione con un Capacity Manager a livello di organizzazione abilitato, ogni account (l'amministratore dell'organizzazione e l'amministratore delegato) può attivare, disattivare e interrogare le chiavi dei tag in modo indipendente. Ogni account mantiene il proprio stato di tag e il proprio limite di tag key`EarliestDatapointTimestamp`.

Un account può richiedere i dati metrici solo per le chiavi di tag che l'account stesso ha attivato. Se sia l'amministratore dell'organizzazione che un amministratore delegato attivano la stessa chiave di tag (ad esempio`environment`), ogni account monitora il proprio stato di attivazione e la disponibilità dei dati in modo indipendente.

Quando l'amministratore delegato disattiva una chiave tag, l'amministratore delegato non può più richiedere i dati per quel tag, anche se l'amministratore dell'organizzazione ha ancora la stessa chiave di tag attivata.

Considerazioni

- Aggiornamenti dei valori dei tag: i valori dei tag per le nuove risorse e i tag appena applicati alle risorse esistenti sono disponibili entro poche ore. Se modifichi il valore di un tag esistente su una risorsa, il valore aggiornato può richiedere fino a 24 ore per essere visualizzato in Capacity Manager.
- Tempo di attivazione: dopo aver attivato un tag key, possono essere necessarie fino a 24 ore prima che il tag passi allo `activated` stato e i dati diventino interrogabili. `EarliestDatapointTimestamp`Indica quando i dati sono disponibili, non quando il tag è stato attivato.
- Limite delle chiavi dei tag: ogni account può monitorare fino a cinque tag key. Manager-provided I tag di capacità non vengono conteggiati ai fini di questo limite.
- Requisiti relativi ai caratteri chiave dei tag: Le chiavi dei tag possono contenere lettere Unicode, cifre, spazi bianchi e i seguenti caratteri:. `_ . : / = + @ -` Le chiavi dei tag non devono superare i 128 caratteri.
- Re-activation: se disattivi e riattivi la stessa chiave tag, sono disponibili solo nuovi dati. I `EarliestDatapointTimestamp` ripristini ad ogni attivazione.
- Tag sospesi: ogni tag key supporta fino a 100.000 valori di tag univoci. Se una chiave tag supera questa soglia, viene spostata allo `suspended` stato. Il tag viene comunque conteggiato ai fini del limite, ma i dati non vengono più inseriti. Riduci il numero di valori univoci per il tag o disattivalo per liberare spazio per un'altra chiave del tag.

Navigando in Capacity Manager nel AWS console

La console Capacity Manager è organizzata in schede che forniscono diverse visualizzazioni dei dati sulla capacità:

- Dashboard: fornisce una panoramica di alto livello di tutte le prenotazioni di On-Demand capacità On-Demand e dell'utilizzo di Spot, comprese le metriche chiave per contribuire a migliorare il livello di capacità.
- Utilizzo: fornisce una panoramica dei modelli di utilizzo delle istanze On-Demand e delle istanze Spot. Analizza la copertura tramite le prenotazioni della capacità e identifica le opportunità di ottimizzazione attraverso operazioni flessibili di raggruppamento e filtraggio.
- Prenotazioni: fornisce un'analisi dell'utilizzo della prenotazione della capacità, delle funzionalità di gestione e delle metriche dettagliate sulle prenotazioni tra account e regioni.

- Spot: monitora i modelli di utilizzo di spot e fornisce analisi dei costi per le istanze spot tra account e regioni.
- Esportazioni di dati: gestisce la configurazione di esportazione dei dati in Amazon S3, che include la pianificazione, la formattazione e la selezione dei modelli.
- Impostazioni: fornisce opzioni di configurazione del servizio, tra cui l'accesso all'organizzazione, le impostazioni regionali e la gestione monitorata delle chiavi dei tag. Puoi attivare le chiavi di tag dalle tue risorse Amazon EC2 da utilizzare come dimensioni per raggruppare e filtrare le metriche di capacità. Per ulteriori informazioni, consulta Gestione delle chiavi dei tag monitorate.

Nelle schede Utilizzo e Prenotazioni, Capacity Manager offre una struttura di navigazione gerarchica che consente di approfondire dalle panoramiche di alto livello alle informazioni dettagliate sulle risorse. La comprensione di questo modello di navigazione consente di analizzare i dati sulla capacità in modo efficiente e identificare le opportunità di ottimizzazione.

Argomenti

- Gerarchia di navigazione
- Visualizza la suddivisione e i dettagli per Utilizzo e Prenotazioni

Gerarchia di navigazione

Capacity Manager utilizza una struttura di navigazione a tre livelli per Utilizzo e Prenotazioni:

1. Pagina panoramica: High-level riepilogo con metriche aggregate.
2. Pagina di analisi: analisi dettagliata con opzioni di filtraggio e raggruppamento
3. Pagine dei dettagli:
   - Dettagli sull'utilizzo: informazioni sulla combinazione di dimensioni selezionata, che forniscono statistiche e dati di serie temporali per aiutarti a comprendere i modelli di utilizzo.
   - Dettagli sulla prenotazione: informazioni su una specifica prenotazione della capacità, che include statistiche di utilizzo, modelli di utilizzo nel tempo e dettagli di configurazione.

> **Note**
>
> Spot segue una struttura semplificata soltanto con la pagina di panoramica.

Visualizza la suddivisione e i dettagli per Utilizzo e Prenotazioni

Entrambe le schede Utilizzo e Prenotazioni seguono la stessa struttura di navigazione a tre livelli, che consente di passare dalla panoramica alla suddivisione fino alle pagine dei dettagli. I processi per accedere alle pagine dettagliate e alla suddivisione sono simili, con solo piccole differenze nella posizione in cui si trovano i link di navigazione all'interno di ciascuna scheda.

Per accedere alle pagine di suddivisione delle risorse

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Capacity Manager.
3. Scegli la scheda relativa al tipo di risorsa che vuoi analizzare: Utilizzo o Prenotazioni.
4. Nella sezione Aggregazioni, individua il link di suddivisione:
   - Utilizzo: nella colonna Operazioni, scegli Visualizza suddivisione.

     > **Note**
     >
     > A seconda delle dimensioni dello schermo o del numero di dimensioni applicate, potresti dover scorrere orizzontalmente lungo la pagina per trovare il link Visualizza suddivisione.

   - Prenotazioni: nella colonna Prenotazioni, scegli il numero (il numero è un link) della prenotazione che vuoi visualizzare.

Per accedere alle pagine dei dettagli

1. Nella pagina della suddivisione, vai alla sezione pertinente:
   - Utilizzo: la sezione Combinazioni di dimensioni uniche.
   - Prenotazioni: la sezione Prenotazioni.
2. Nella sezione pertinente delle risorse scelte, accedi alla pagina dei dettagli.
   - Utilizzo: nella colonna Operazioni, scegli Visualizza dettagli.

> **Note**
>
> A seconda delle dimensioni dello schermo o del numero di dimensioni applicate, potresti dover scorrere orizzontalmente lungo la pagina per trovare il link Visualizza dettagli.

- Prenotazioni: nella colonna ID prenotazione, scegli la prenotazione che vuoi visualizzare.

Esportazione dei dati di Capacity Manager

Puoi esportare i dati sulla capacità da EC2 Capacity Manager ad Amazon S3 per consentire ulteriori analisi, creare report personalizzati o integrarli con altri servizi. AWS Puoi esportare i tuoi dati in formato CSV o Parquet. Nelle sezioni seguenti, troverai informazioni su come esportare i dati di Capacity Manager.

> **Note**
>
> Capacity Manager consente solo un'esportazione di dati per Account AWS.

> **Note**
>
> Nel raro caso in cui un'esportazione di dati debba essere reindirizzata a causa di un problema relativo ai dati, il nuovo file sovrascrive il file esistente per quell'ora.

Argomenti

- Configurazione di un bucket Amazon S3 per le esportazioni di dati di Capacity Manager
- Creazione di un'esportazione di dati per i dati di Capacity Manager

Configurazione di un bucket Amazon S3 per le esportazioni di dati di Capacity Manager

Per ricevere le esportazioni di dati di Capacity Manager, devi disporre di un bucket Amazon S3 Account AWS per ricevere e archiviare i file di esportazione. Quando crei un'esportazione di dati nella

console di Capacity Manager, puoi selezionare un bucket Amazon S3 esistente di tua proprietà o creare un nuovo bucket.

In entrambi i casi, devi applicare la policy di bucket richiesta per consentire a Capacity Manager di fornire i file di esportazione. La modifica di questa policy nella console Amazon S3 o la modifica del proprietario del bucket dopo aver creato un'esportazione di dati impedirà a Capacity Manager di fornire le esportazioni.

Per creare un bucket Amazon S3, consulta Creating an S3 bucket nella Guida per l'utente di Amazon Simple Storage Service.

La policy seguente deve essere applicata al bucket S3 per consentire a Capacity Manager di fornire le esportazioni di dati:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.capacitymanager.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111122223333:capacity-
manager-data-export/*"
                }
            }
        }
    ]
}
```

Questa policy di bucket aiuta a garantire che i file di esportazione dei dati di Capacity Manager possano essere forniti in modo sicuro al bucket. Nello specifico:

- Ogni volta che viene fornita un'esportazione di dati di Capacity Manager, conferma AWS innanzitutto se il bucket è ancora di proprietà dell'account che ha impostato l'esportazione. Se la proprietà del bucket è cambiata, l'esportazione non verrà fornita. Ciò aiuta a garantire la sicurezza dei dati di Capacity Manager. Questa policy del bucket consente a AWS (`"Effect": "Allow"`) di verificare a quale account appartiene il bucket (). `"Action": ["s3:ListBucket"]`
- La policy concede al servizio Capacity Manager (`"Service": "ec2.capacitymanager.amazonaws.com"`) l'autorizzazione a scrivere file di esportazione (`"Action": "s3:PutObject"`) e leggere oggetti (`"Action": "s3:GetObject"`) per copiare i dati nel bucket.

Creazione di un'esportazione di dati per i dati di Capacity Manager

Per creare un'esportazione di dati, puoi utilizzare la pagina Esportazioni dati nella console di Capacity Manager o la AWS CLI.

Prerequisiti

Devi creare un bucket Amazon Simple Storage Service (Amazon S3). Devi assicurarti di quanto segue:

- Il bucket S3 deve trovarsi nello stesso in Regione AWS cui è stato abilitato Capacity Manager.
- Il bucket S3 dispone della policy di autorizzazioni necessaria affinché il servizio Capacity Manager fornisca i file.

Per ulteriori informazioni, consulta Configurazione di un bucket Amazon S3 per le esportazioni di dati di Capacity Manager.

Procedura

È possibile esportare i dati di Capacity Manager utilizzando la AWS Console, il AWS CLI, o. PowerShell

Console

Per creare un'esportazione di dati

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Capacity Manager.
3. Scegli la scheda Esportazioni dati.
4. Seleziona Crea esportazione di dati.
5. Configura le proprietà di esportazione, il luogo di consegna e i tag (opzionale).
6. Scegli Create (Crea).

AWS CLI

Per creare un'esportazione di dati

Per creare una esportazione di dati con la configurazione specificata, utilizza il comando seguente:

```
aws ec2 create-capacity-manager-data-export \
    --s3-bucket-name my-exports-bucket \
    --s3-bucket-prefix capacity-data-exports \
    --schedule hourly \
    --output-format parquet/CSV \
    --tag-specifications 'ResourceType=capacity-manager-data-
export,Tags=[{Key=environment,Value=production}]'
```

> **Note**
>
> Il `--tag-specifications` parametro nel comando precedente applica i tag delle risorse alla risorsa di esportazione dei dati stessa (ad esempio, per l'allocazione dei costi o l'organizzazione). Questi sono separati dalle chiavi dei tag monitorate, che determinano le colonne di tag incluse nei dati esportati. Per ulteriori informazioni sulle chiavi dei tag monitorate, vedereGestione delle chiavi dei tag monitorate.

PowerShell

Per creare un'esportazione di dati

Utilizza il cmdlet New-EC2CapacityManagerDataExport.

```
New-EC2CapacityManagerDataExport `
    -S3BucketName "my-exports-bucket" `
    -S3BucketPrefix "capacity-data-exports" `
    -Schedule "hourly" `
    -OutputFormat "parquet" `
    -TagSpecification @([Amazon.EC2.Model.TagSpecification]@{
        ResourceType = "capacity-manager-data-export"
        Tags = @([Amazon.EC2.Model.Tag]@{
            Key   = "environment"
            Value = "production"
        })
    })
```

Colonne di tag nelle esportazioni di dati

Le esportazioni di dati appena create includono i valori dei tag come colonne aggiuntive per le chiavi dei tag monitorate attivate e i Manager-provided tag Capacity. Per ulteriori informazioni, consulta Tag nelle esportazioni di dati in Gestione delle chiavi dei tag monitorate.

> **Note**
>
> Se non hai attivato alcuna chiave di tag monitorata, le tue esportazioni includeranno comunque colonne per i Manager-provided tag Capacity (ad esempio `aws:autoscaling:groupNameaws:eks:cluster-name`,`eks:kubernetes-node-pool-name`,, `ekarpenter.sh/nodepool`).

Gestione dei driver di dispositivo per l'istanza EC2

I driver di dispositivo sono componenti software che comunicano con l'hardware virtualizzato dell'istanza Amazon EC2. Per prevenire errori di sistema, problemi di prestazioni e altri comportamenti imprevisti, è importante mantenere i driver aggiornati. L'aggiornamento è particolarmente importante per i driver che possono avere un forte impatto sulle prestazioni del

sistema a seconda dell'utilizzo, come i driver di rete, i driver grafici e i driver dei dispositivi di archiviazione. Le nuove versioni dei driver possono includere correzioni di problemi o introdurre funzionalità estese da poter sfruttare per le istanze attualmente in esecuzione.

Driver di rete

Le distribuzioni Linux possono incorporare funzionalità di rete come Adattatore elastico di rete (ENA) o Elastic Fabric Adapter (EFA) all'interno del kernel. Tuttavia, i tempi di implementazione delle funzionalità dei driver del kernel all'interno delle diverse distribuzioni possono variare.

I driver del kernel Linux ENA ed EFA sono disponibili nell'archivio Amazon Drivers GitHub . Per ulteriori informazioni e collegamenti ai driver disponibili, consulta Amazon Drivers su GitHub.

Per ulteriori informazioni sui driver ENA, consultare Abilitazione delle reti avanzate con ENA su istanze EC2. Per ulteriori informazioni sui driver ENA, consultare Nozioni di base nella sezione Elastic Fabric Adapter per AI/ML carichi di lavoro HPC su Amazon EC2 di questa guida.

Per installare o aggiornare i driver di rete sulle istanze Windows, consultare i seguenti argomenti:

- Installa il driver ENA su Windows
- Installa la versione più recente AWS Driver PV

  Per ulteriori informazioni, consulta Driver paravirtuali per le istanze Windows.

> **Note**
>
> EFA non è supportato sulle istanze Windows.

Driver grafici

Per installare o aggiornare i driver grafici, consultare i seguenti argomenti:

- Driver AMD per la tua istanza EC2
- Driver NVIDIA per la tua istanza Amazon EC2

Driver dei dispositivi di archiviazione

Per installare o aggiornare i driver di archiviazione, consultare i seguenti argomenti:

- Per le istanze Linux, consultare Installare o aggiornare il driver NVMe nella Guida per l'utente di Amazon EBS.
- Per le istanze Windows, consultare Driver NVMe.

Altri driver di dispositivo Windows

Per installare o aggiornare altri driver di dispositivi Windows, consulta i seguenti argomenti:

- Altri driver di dispositivo Windows

Driver AMD per la tua istanza EC2

Un'istanza con una GPU AMD collegata, ad esempio un'istanza G4ad, deve avere installato il driver AMD appropriato. A seconda delle esigenze, è possibile utilizzare una AMI con il driver preinstallato o scaricare un driver da Amazon S3.

Per installare i driver NVIDIA su un'istanza con una GPU NVIDIA collegata, ad esempio un'istanza G4dn, consulta Driver NVIDIA.

Indice

- Driver AMD Radeon Pro Software for Enterprise
- AMI con driver AMD installato
- Download del driver AMD

Driver AMD Radeon Pro Software for Enterprise

Il driver AMD Radeon Pro Software for Enterprise è progettato per fornire supporto nei casi d'uso di grafica a livello professionale. Utilizzando il driver, è possibile configurare le istanze con due display 4K per GPU.

API supportate

- OpenGL, OpenCL
- Vulkan
- AMD Advanced Media Framework
- API di accelerazione video

- DirectX 9 e versioni successive
- Microsoft Media Foundation Transform hardware

AMI con driver AMD installato

AWS offre diverse Amazon Machine Images (AMI) fornite con i driver AMD installati. Apri leofferte nel Marketplace con driver AMD.

Download del driver AMD

Se non si utilizza una AMI con driver AMD installato, è possibile scaricare il driver AMD e installarlo sull'istanza. Solo le versioni dei sistemi operativi seguenti supportano i driver AMD:

- Amazon Linux 2 con versione del kernel 5.10
- Ubuntu 24.04
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Questi download sono disponibili solo per AWS i clienti. Eseguendo il download, accetti di utilizzare il software scaricato solo per sviluppare AMIs da utilizzare con l'hardware AMD Radeon Pro V520. Installando il software, sarai vincolato dai termini del contratto di licenza con l'utente finale AMD End User License Agreement.

Installare il driver AMD sull'istanza Linux di Amazon Linux 2

1. Connessione a un'istanza Linux.
2. Installali AWS CLI sulla tua istanza Linux e configura le credenziali predefinite. Per ulteriori informazioni, consulta Installazione dell' AWS CLI nella Guida per l'utente dell'AWS Command Line Interface .

> **Important**
>
> All'utente o al ruolo devono essere concesse le autorizzazioni che contengono la AmazonS3ReadOnlyAccess policy. Per ulteriori informazioni, consulta AWS managed policy: AmazonS3ReadOnlyAccess nella Amazon Simple Storage Service User Guide.

3. Installa e gcc makedialog, se non sono già installati.

```
$ sudo yum install -y gcc make dialog
```

4. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
$ sudo amazon-linux-extras install epel -y
$ sudo yum update -y
```

5. Riavviare l'istanza.

```
$ sudo reboot
```

6. Riconnettersi all'istanza dopo il riavvio.
7. Scaricare il driver AMD più recente.

```
$ aws s3 cp --recursive s3://ec2-amd-linux-drivers/latest/ .
```

8. Estrarre il file.

```
$ tar -xzf amdgpu-pro-*rhel*.tar.gz
```

9. Installare il pacchetto amdgpu-install. Sostituisci *version* con il nome della directory della versione creata quando hai estratto il driver.

```
$ cd rhel_7/version/x86_64/a/
$ sudo yum install -y ./amdgpu-install-*.el7.noarch.rpm
```

10. Modificare `/etc/yum.repos.d/amdgpu.repo`. `baseurl`Impostato sulla `x86_64` directory estratta (ad esempio,`baseurl=file:///home/ec2-user/rhel_7/version/x86_64/`). Imposta `gpgcheck=0`.
11. Modificare `/etc/yum.repos.d/amdgpu-proprietary.repo`. `baseurl`Impostato sulla stessa directory. Imposta `gpgcheck=0` e`enabled=1`.
12. Modificare `/etc/yum.repos.d/rocm.repo`. `baseurl`Impostato nella stessa directory. Imposta `gpgcheck=0`.
13. Installa il driver GPU AMD per Amazon Linux 2.

```
$ sudo amdgpu-install --usecase=workstation --vulkan=pro --accept-eula -y
```

14. Riavviare l'istanza.

```
$ sudo reboot
```

15. Verificare che il driver funzioni.

```
$ sudo dmesg | grep amdgpu
```

La risposta dovrebbe essere simile alla seguente:

```
Initialized amdgpu
```

Installare il driver AMD sull'istanza Linux di Ubuntu

1. Connessione a un'istanza Linux.
2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
$ sudo apt-get update -y && sudo apt-get upgrade -y
```

3. Installa il firmware e i moduli del kernel Linux.

```
$ sudo apt install -y linux-firmware linux-modules-extra-$(uname -r)
```

4. Riavviare l'istanza.

```
$ sudo reboot
```

5. Riconnettersi all'istanza dopo il riavvio.
6. Scarica il pacchetto driver AMD più recente per Ubuntu 24.04 da Linux® Drivers for AMD Radeon™ Graphics dal sito Web AMD. Nel comando seguente, sostituisci *version* con la stringa della versione dal nome del file scaricato (ad esempio,). `31.30.313000-1_all`

```
$ sudo apt install -y ./amdgpu-install_version.deb
```

7. Installa il driver GPU AMD per Ubuntu.

```
$ sudo amdgpu-install --usecase=graphics --vulkan=radv -y
```

8. Riavviare l'istanza.

```
$ sudo reboot
```

9. Verificare che il driver funzioni.

```
$ sudo dmesg | grep amdgpu
```

La risposta dovrebbe essere simile alla seguente:

```
Initialized amdgpu
```

Installare il driver AMD sull'istanza di Windows

1. Connettiti alla tua istanza Windows e apri una PowerShell finestra.
2. Configura le credenziali predefinite per l' AWS Tools for Windows PowerShell istanza di Windows. Per ulteriori informazioni, consulta Nozioni di base su AWS Tools for Windows PowerShell nella Guida per l'utente di AWS Strumenti per PowerShell .

> **Important**
>
> All'utente o al ruolo devono essere concesse le autorizzazioni che contengono la AmazonS3ReadOnlyAccess policy. Per ulteriori informazioni, consulta AWS managed policy: AmazonS3ReadOnlyAccess nella Amazon Simple Storage Service User Guide.

3. Imposta il prefisso della chiave in base alla tua versione di Windows:

- Windows 10 e Windows 11

```
$KeyPrefix = "latest/AMD_GPU_WINDOWS10"
```

- Windows Server 2016

```
$KeyPrefix = "archives"
```

- Windows Server 2019

```
$KeyPrefix = "latest/AMD_GPU_WINDOWS_2K19" # use "archives" for Windows Server
 2016
```

- Windows Server 2022

```
$KeyPrefix = "latest/AMD_GPU_WINDOWS_2K22"
```

4. Scarica i driver da Amazon S3 sul desktop utilizzando i seguenti PowerShell comandi.

```
$Bucket = "ec2-amd-windows-drivers"
$LocalPath = "$home\Desktop\AMD"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
    }
}
```

5. Decomprimi il file del driver scaricato ed esegui il programma di installazione utilizzando i seguenti comandi. PowerShell

```
Expand-Archive $LocalFilePath -DestinationPath "$home\Desktop\AMD\$KeyPrefix" -
Verbose
```

Ora, controlla il nome della nuova directory. Il nome della directory può essere recuperato utilizzando il comando. `Get-ChildItem` PowerShell

```
Get-ChildItem "$home\Desktop\AMD\$KeyPrefix"
```

L'output visualizzato dovrebbe essere simile al seguente:

```
Directory: C:\Users\Administrator\Desktop\AMD\latest

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       10/13/2021  12:52 AM                210414a-365562C-Retail_End_User.2
```

Installa i driver AMD:

```
pnputil /add-driver $home\Desktop\AMD\$KeyPrefix\*.inf /install /subdirs
```

6. Seguire le istruzioni per installare il driver e riavviare l'istanza come necessario.
7. Per verificare che la GPU funzioni correttamente, controllare in Gestione dispositivi. "AMD Radeon Pro V520 MxGPU" dovrebbe elencata come scheda video.
8. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni Amazon DCV.

Driver NVIDIA per la tua istanza Amazon EC2

Un'istanza con una GPU NVIDIA collegata, come tipi di istanza della serie P o G, deve avere installato il driver NVIDIA appropriato. A seconda del tipo di istanza, puoi scaricare un driver NVIDIA pubblico, scaricare un driver da Amazon S3 disponibile solo per AWS i clienti o utilizzare un' AWS AMI con il driver preinstallato.

Per installare i driver AMD su un'istanza con una GPU AMD collegata, ad esempio un'istanza G4ad, consulta Driver AMD.

Argomenti

- Tipi di driver NVIDIA
- Driver disponibili per tipo di istanza
- Opzioni di installazione
- Utilizza AMI che includono driver NVIDIA
- Installa i driver pubblici NVIDIA
- Installa i driver NVIDIA GRID (istanze G7e, G6, Gr6, G6e, G6f, Gr6f, G5, G4dn e G3)
- Installa i driver di gioco NVIDIA (istanze G7e, G6, G6e, G5 e G4dn)

Tipi di driver NVIDIA

Di seguito sono riportati i principali tipi di driver NVIDIA che possono essere utilizzati con le istanze. GPU-based

Driver Tesla

> Questi driver sono destinati principalmente ai carichi di lavoro di calcolo che utilizzano le GPU per attività come calcoli in virgola mobile parallelizzati per il machine learning e le trasformazioni veloci di Fourier per applicazioni di calcolo ad alte prestazioni.

Driver GRID

Questi driver sono certificati per fornire prestazioni ottimali per le applicazioni di visualizzazione professionali che eseguono il rendering di contenuti come modelli 3D o video ad alta risoluzione. Puoi configurare i driver GRID per supportare due modalità. Le Quadro Virtual Workstation forniscono l'accesso a quattro display 4K per GPU. Le vApps GRID forniscono funzionalità di hosting di app RDSH.

Driver di gioco

Questi driver contengono ottimizzazioni per il gioco e vengono aggiornati frequentemente per migliorare le prestazioni. Supportano un singolo display 4K per GPU.

Modalità configurata

In Windows, i driver Tesla sono configurati per l'esecuzione in modalità Tesla Compute Cluster (TCC). I driver GRID e di gioco sono configurati per l'esecuzione in modalità WDDM (Windows Display Driver Model). In modalità TCC, la scheda è dedicata ai carichi di lavoro di calcolo. In modalità WDDM, la scheda supporta sia i carichi di lavoro di calcolo che quelli grafici.

Pannello di controllo NVIDIA

Il pannello di controllo NVIDIA è supportato con i driver GRID e Gaming. Non è supportato con i driver Tesla.

API supportate per i driver Tesla, GRID e di gioco

- OpenCL, OpenGL e Vulkan
- NVIDIA CUDA e librerie correlate (ad esempio, cuDNN, TensorRT, nvJPEG e cuBLAS)
- NVENC per la codifica video e NVDEC per la decodifica video
- Windows-only API: DirectX, Direct2D, DirectX Video Acceleration, DirectX Raytracing

Driver disponibili per tipo di istanza

Nella tabella seguente vengono riepilogati i driver NVIDIA supportati per ogni tipo di istanza GPU.

Tipo di istanza	Driver Tesla	Driver GRID	Driver di gioco
G3	Sì	Sì	No

Tipo di istanza	Driver Tesla	Driver GRID	Driver di gioco
G4dn	Sì	Sì	Sì
G5	Sì	Sì	Sì
G5g	Sì [1]	No	No
G6	Sì	Sì	Sì
G6e	Sì	Sì	Sì
G6f	No	Sì	No
Gr6	Sì	Sì	No
Gr6f	No	Sì	No
G7e	Sì	Sì	Sì
P3	Sì	No	No
P4d	Sì	No	No
P4de	Sì	No	No
P5	Sì	No	No
P5e	Sì	No	No
P5en	Sì	No	No
P6-B200	Sì	No	No
P6e-GB200	Sì	No	No
P6-B300	Sì	No	No

[1] Questo driver Tesla supporta anche applicazioni grafiche ottimizzate specifiche per la piattaforma ARM64

Opzioni di installazione

Utilizza una delle seguenti opzioni per ottenere i driver NVIDIA necessari per l'istanza GPU.

Opzioni

1. Utilizza AMI che includono driver NVIDIA
2. Installa i driver pubblici NVIDIA
3. Installa i driver NVIDIA GRID (istanze G7e, G6, Gr6, G6e, G6f, Gr6f, G5, G4dn e G3)
4. Installa i driver di gioco NVIDIA (istanze G7e, G6, G6e, G5 e G4dn)

Utilizza AMI che includono driver NVIDIA

AWS e NVIDIA offrono diverse Amazon Machine Images (AMI) fornite con i driver NVIDIA installati.

- Offerte di Marketplace con il driver Tesla pubblico
- Offerte di Marketplace con il driver GRID
- Offerte di Marketplace con il driver di gioco

Per esaminare le considerazioni che dipendono dalla piattaforma del sistema operativo (OS), scegli la scheda relativa alla tua AMI.

Linux

Per aggiornare la versione del driver installata utilizzando una di queste AMI, è necessario disinstallare i pacchetti NVIDIA dall'istanza per evitare conflitti di versione. Utilizza questo comando per disinstallare i pacchetti NVIDIA:

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

Il pacchetto di kit di strumenti CUDA presenta dipendenze sui driver NVIDIA. Disinstallando i pacchetti NVIDIA, il kit di strumenti CUDA viene cancellato. Devi reinstallare questo kit di strumenti dopo avere installato il driver NVIDIA.

Windows

Se crei un'AMI Windows personalizzata utilizzando una delle offerte Marketplace AWS , l'AMI deve essere un'immagine standardizzata creata con Windows Sysprep per garantire che il

driver GRID funzioni. Per ulteriori informazioni, consulta Creare un'AMI Amazon EC2 utilizzando Windows Sysprep.

Installa i driver pubblici NVIDIA

Se le Marketplace AWS AMI descritte in Utilizza AMI che includono driver NVIDIA non sono adatte al tuo caso d'uso, puoi installare i driver pubblici e portare la tua licenza. Le opzioni di installazione sono:

- Driver-only Opzione 1: installazione
- Opzione 2: Installazione con il toolkit CUDA (consigliato per le distribuzioni Linux)

P6-B200 e considerazioni sul tipo di P6-B300 istanza

Le P6-B300 piattaforme P6-B200 e sono uniche in quanto espongono le schede di interfaccia di rete (NIC) Mellanox ConnectX all'istanza come dispositivi PCIe. Queste NIC non agiscono come tipiche interfacce di rete ma funzionano invece come bridge NVSwitch che forniscono un percorso di controllo per inizializzare e configurare NvFabric, che è la topologia NVLink dell'interconnessione GPU.

Per inizializzare completamente il sistema, NVIDIA Fabric Manager deve configurare `NVFabric` e stabilire la topologia NVSwitch. Ciò InfiniBand consente ai moduli del kernel di comunicare con le NIC Mellanox ConnectX.

NVIDIA Fabric Manager è incluso nel toolkit CUDA. Consigliamo Opzione 2: Installazione con il toolkit CUDA per questo tipo di istanza.

Driver-only Opzione 1: installazione

Per installare un driver specifico, accedi alla tua istanza e scarica il driver pubblico NVIDIA a 64 bit per il tipo di istanza da http://www.nvidia.com/Download/Find.aspx. Per Tipo di prodotto, Serie di prodotti e Prodotto, utilizza le opzioni mostrate nella seguente tabella.

Quindi segui le istruzioni per l'installazione del repository locale nella Guida all'installazione dei driver NVIDIA.

> **Note**
>
> P6-B200 e i tipi di P6-B300 istanza richiedono l'installazione e la configurazione di pacchetti aggiuntivi forniti in bundle con NVIDIA CUDA Toolkit. Per ulteriori informazioni, consulta le istruzioni per la distribuzione Linux in Opzione 2: Installazione con il toolkit CUDA.

Istanza	Tipo di prodotto	Serie di prodotti	Prodotto	Versione driver minima
G3	Tesla	M-Class	M60	--
G4dn	Tesla	T-Series	T4	--
G5	Tesla	A-Series	A10	470.00 o versioni successive
G5g[1]	Tesla	T-Series	T4G	470.82.01 o versioni successive
G6	Tesla	L-Series	L4	525.0 o versioni successive
G6e	Tesla	L-Series	L40S	535.0 o versioni successive
Gr6	Tesla	L-Series	L4	525.0 o versioni successive
G7	Tesla	Serie RTX	RTX PRO 4500 Blackwell	595 o successivo
G7e	Tesla	Serie RTX	RTX PRO 6000 Blackwell	575.0 o successivo
P3	Tesla	V-Series	V100	--
P4d	Tesla	A-Series	A100	--

Istanza	Tipo di prodotto	Serie di prodotti	Prodotto	Versione driver minima
P4de	Tesla	A-Series	A100	--
P5	Tesla	H-Series	H100	530 o versioni successive
P5e	Tesla	H-Series	H200	550 o versioni successive
P5en	Tesla	H-Series	H200	550 o versioni successive
P6-B200[2]	Tesla	HGX-Series	B200	570 o successivo
P6e-GB200	Tesla	HGX-Series	B200	570 o successivo
P6-B300[2]	Tesla	HGX-Series	B300	580 o successivo

[1] Il sistema operativo per le istanze G5g è Linux aarch64.

[2] Per P6-B200 i tipi di P6-B300 istanza, esistono requisiti di installazione aggiuntivi per configurare NVIDIA Fabric Manager.

Opzione 2: Installazione con il toolkit CUDA

Le istruzioni di installazione variano leggermente in base al sistema operativo. Per installare driver pubblici sulla tua istanza con il toolkit NVIDIA CUDA, segui le istruzioni relative al sistema operativo dell'istanza. Ad esempio, per i sistemi operativi non mostrati qui, segui le istruzioni per il tuo sistema operativo e l'architettura del tipo di istanza sul sito web di NVIDIA Developer. Per ulteriori informazioni, consulta CUDA Toolkit Downloads.

Per l'architettura del tipo di istanza o altre specifiche, consulta le specifiche sul calcolo accelerato nella documentazione di riferimento Amazon EC2 Instance Types.

Amazon Linux 2023

Questa sezione tratta l'installazione di un toolkit NVIDIA CUDA su un'istanza Amazon Linux 2023. Gli esempi di comandi in questa sezione si basano su un'architettura `x86_64`.

Per i comandi `arm64-sbsa`, consulta CUDA Toolkit Downloads e seleziona le opzioni che si applicano alla tua distribuzione. Le istruzioni vengono visualizzate dopo aver effettuato la selezione finale.

Prerequisito

Prima di installare il toolkit e i driver, esegui il seguente comando per assicurarti di avere la versione corretta delle intestazioni kernel e dei pacchetti di sviluppo.

```
[ec2-user ~]$ sudo dnf install kernel-devel-$(uname -r) kernel-headers-$(uname -r) -y
```

Scarica il toolkit e i driver

Scegli il tipo di installazione da utilizzare per la tua istanza e segui i passaggi associati.

AL2023 NVIDIA repository

Amazon Linux 2023 fornisce driver per GPU NVIDIA e pacchetti di toolkit CUDA tramite un repository dedicato che mantiene. AWS AWS qualifica questo repository con le release candidate AL2023 e fornisce avvisi di sicurezza tramite Amazon Linux Security Center. Consigliamo questa opzione per le istanze AL2023 perché semplifica l'installazione e mantiene i driver aggiornati tramite il flusso di lavoro standard. `dnf update`

Per istruzioni, consulta i driver NVIDIA nella Guida per l'utente di Amazon Linux 2023.

RPM local installation

Puoi seguire queste istruzioni per scaricare il bundle del repository di installazione del toolkit CUDA sulla tua istanza, poi estrarre e registrare il bundle specificato.

Per visualizzare le istruzioni sul sito web per sviluppatori NVIDIA, consulta CUDA Toolkit Downloads.

```
[ec2-user ~]$ wget https://developer.download.nvidia.com/compute/cuda/13.0.0/
local_installers/cuda-repo-amzn2023-13-0-local-13.0.0_580.65.06-1.x86_64.rpm
[ec2-user ~]$ sudo rpm -i cuda-repo-amzn2023-13-0-
local-13.0.0_580.65.06-1.x86_64.rpm
```

RPM network installation

Puoi seguire queste istruzioni per registrare il repository CUDA con il gestore di pacchetti sulla tua istanza. Quando esegui i passaggi di installazione, il gestore di pacchetti scarica solo i pacchetti necessari.

Per visualizzare le istruzioni sul sito web per sviluppatori NVIDIA, consulta CUDA Toolkit Downloads.

```
[ec2-user ~]$ sudo dnf config-manager --add-repo https://
developer.download.nvidia.com/compute/cuda/repos/amzn2023/x86_64/cuda-amzn2023.repo
```

I passaggi rimanenti sono gli stessi sia per l'installazione locale di RPM che per quella di rete RPM.

1. Completa l'installazione del toolkit CUDA

```
[ec2-user ~]$ sudo dnf clean all
[ec2-user ~]$ sudo dnf install cuda-toolkit -y
```

2. Installa la variante del driver relativa al modulo open kernel

```
[ec2-user ~]$ sudo dnf module install nvidia-driver:open-dkms -y
```

3. Installa GPUDirect Storage e Fabric Manager

```
[ec2-user ~]$ sudo dnf install nvidia-gds -y
[ec2-user ~]$ sudo dnf install nvidia-fabric-manager -y
```

4. Abilita Fabric Manager e la persistenza dei driver

```
[ec2-user ~]$ sudo systemctl enable nvidia-fabricmanager
[ec2-user ~]$ sudo systemctl enable nvidia-persistenced
```

5. (P6-B200 e P6-B300 solo) Questi tipi di istanze richiedono l'installazione e la configurazione di pacchetti aggiuntivi forniti in bundle con NVIDIA CUDA Toolkit.

   1. Installa NVIDIA Link Subnet Manager e `ibstat`.

      ```
      [ec2-user ~]$ sudo dnf install nvlink5
      ```

   2. Abilita il caricamento automatico del modulo Infiniband all'avvio.

```
[ec2-user ~]$ echo "ib_umad" | sudo tee -a /etc/modules-load.d/modules.conf
```

6. Riavvia l'istanza

```
[ec2-user ~]$ sudo reboot
```

Ubuntu 24.04

Questa sezione tratta l'installazione di un toolkit NVIDIA CUDA su un'istanza Ubuntu 24.04. Gli esempi di comandi in questa sezione si basano su un'architettura `x86_64`.

Per i comandi `arm64-sbsa`, consulta CUDA Toolkit Downloads e seleziona le opzioni che si applicano alla tua distribuzione. Le istruzioni vengono visualizzate dopo aver effettuato la selezione finale.

Prerequisito

Prima di installare il toolkit e i driver, esegui il seguente comando per assicurarti di avere la versione corretta delle intestazioni kernel e dei pacchetti di sviluppo.

```
$ apt install linux-headers-$(uname -r)
```

Scarica il toolkit e i driver

Scegli il tipo di installazione da utilizzare per la tua istanza e segui i passaggi associati.

Deb local installation

Puoi seguire queste istruzioni per scaricare il bundle del repository di installazione del toolkit CUDA sulla tua istanza, poi estrarre e registrare il bundle specificato.

Per visualizzare le istruzioni sul sito web per sviluppatori NVIDIA, consulta CUDA Toolkit Downloads.

```
$ wget https://developer.download.nvidia.com/compute/cuda/repos/ubuntu2404/
x86_64/cuda-ubuntu2404.pin
$ sudo mv cuda-ubuntu2404.pin /etc/apt/preferences.d/cuda-repository-pin-600
$ wget https://developer.download.nvidia.com/compute/cuda/13.0.0/
local_installers/cuda-repo-ubuntu2404-13-0-local_13.0.0-580.65.06-1_amd64.deb
```

```
$ sudo dpkg -i cuda-repo-ubuntu2404-13-0-local_13.0.0-580.65.06-1_amd64.deb
$ sudo cp /var/cuda-repo-ubuntu2404-13-0-local/cuda-*-keyring.gpg /usr/share/
keyrings/
```

Deb network installation

Puoi seguire queste istruzioni per registrare il repository CUDA con il gestore di pacchetti sulla tua istanza. Quando esegui i passaggi di installazione, il gestore di pacchetti scarica solo i pacchetti necessari.

Per visualizzare le istruzioni sul sito web per sviluppatori NVIDIA, consulta CUDA Toolkit Downloads.

```
$ wget https://developer.download.nvidia.com/compute/cuda/repos/ubuntu2404/x86_64/
cuda-keyring_1.1-1_all.deb
$ sudo dpkg -i cuda-keyring_1.1-1_all.deb
```

I passaggi rimanenti sono gli stessi sia per l'installazione locale che per quella di rete.

1. Completa l'installazione del toolkit CUDA

```
$ sudo apt update
$ sudo apt install cuda-toolkit -y
```

2. Installa la variante del driver relativa al modulo open kernel

```
$ sudo apt install nvidia-open -y
```

3. Installa GPUDirect Storage e Fabric Manager

```
$ sudo apt install nvidia-gds -y
$ sudo apt install nvidia-fabricmanager -y
```

4. Abilita Fabric Manager e la persistenza dei driver

```
$ sudo systemctl enable nvidia-fabricmanager
$ sudo systemctl enable nvidia-persistenced
```

5. (P6-B200 e P6-B300 solo) Questi tipi di istanze richiedono l'installazione e la configurazione di pacchetti aggiuntivi forniti in bundle con NVIDIA CUDA Toolkit.

1. Installa il driver di InfiniBand-specific dispositivo e le utilità di diagnostica più recenti.

```
$ sudo apt install linux-modules-extra-$(uname -r) -y
$ sudo apt install infiniband-diags -y
```

2. Installa NVIDIA Link Subnet Manager.

```
$ sudo apt install nvlsm -y
```

6. Riavvia l'istanza

```
sudo reboot
```

7. Aggiorna il percorso e aggiungi la seguente variabile di ambiente.

```
$ export PATH=${PATH}:/usr/local/cuda-13.0/bin
$ export LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/usr/local/cuda-13.0/lib64
```

Sistemi operativi Windows

Per installare il driver NVIDIA su Windows, segui questi passaggi:

1. Aprire la cartella in cui è stato scaricato il driver e avviare il file di installazione. Seguire le istruzioni per installare il driver e riavviare l'istanza come necessario.
2. Disabilita la scheda video denominata Scheda video di base Microsoft contrassegnata da un'icona di avviso utilizzando Gestione dispositivi. Installare le funzionalità Windows Media Foundation e Quality Windows Audio Video Experience.

> **Important**
>
> Non disattivare la scheda video denominata Scheda video remota di Microsoft. Se la Scheda video remota di Microsoft è disabilitata, la connessione potrebbe essere interrotta e i tentativi di connessione all'istanza dopo il riavvio potrebbero fallire.

3. Aprire Gestione dispositivi per verificare che la GPU funzioni correttamente.
4. Per ottenere prestazioni ottimali dalla GPU, completare le fasi di ottimizzazione in Ottimizza le impostazioni GPU sulle istanze Amazon EC2.

Installa i driver NVIDIA GRID (istanze G7e, G6, Gr6, G6e, G6f, Gr6f, G5, G4dn e G3)

Questi AWS download sono disponibili solo per i clienti. Scaricando, per rispettare i requisiti della AWS soluzione indicati nel Contratto di licenza per l'utente finale (EULA) di NVIDIA GRID Cloud, l'utente accetta di utilizzare il software scaricato solo per sviluppare AMI da utilizzare con l'hardware NVIDIA L4, NVIDIA L40S, NVIDIA A10G, NVIDIA Tesla T4 o NVIDIA Tesla M60. È possibile utilizzare AWS i driver GRID per creare e utilizzare le AMI all'interno dell'ambiente. Installando il software, sarai vincolato dai termini del contratto di licenza con l'utente finale NVIDIA GRID Cloud End User License Agreement. Per informazioni sulla versione del driver NVIDIA GRID per il sistema operativo in uso, consulta NVIDIA® Virtual GPU (vGPU) Software sul sito web di NVIDIA.

Considerazioni

- Le istanze G7e richiedono GRID 19.1 o successivo per Linux e 19.4 (582.16) o successivo per Windows.
- Le istanze G6f e Gr6f richiedono da GRID 18.4 a GRID 19.5.
- Le istanze G6e richiedono GRID 17.4 o versioni successive.
- Le istanze G6 e Gr6 richiedono GRID 17.1 o versioni successive.
- Le istanze G5 richiedono GRID 13.1 o successivo (o GRID 12.4 o successivo).
- Le istanze G3 richiedono AWS una risoluzione DNS fornita per il funzionamento delle licenze GRID.
- IMDSv2 è supportato solo con il driver NVIDIA versione 14.0 o superiore.
- Per le istanze Windows, se si avvia l'istanza da una AMI Windows personalizzata, l'AMI deve essere un'immagine standardizzata creata con Windows Sysprep per garantire che il driver GRID funzioni. Per ulteriori informazioni, consulta Creare un'AMI Amazon EC2 utilizzando Windows Sysprep.
- GRID 17.0 e versioni successive non supportano Windows Server 2019.
- GRID 14.2 e versioni successive non supportano Windows Server 2016.
- GRID 17.0 e versioni successive non sono supportati con le istanze G3.
- Per le istanze Linux, potresti dover installare o aggiornare pacchetti, come gcc, se il programma di installazione NVIDIA ha esito negativo e viene visualizzato un messaggio di errore. Le specifiche dipendono dalle versioni del sistema operativo e del kernel. Per ulteriori informazioni, consulta il portale NVIDIA Enterprise Support.

Prerequisiti

- (Linux) Verifica che AWS CLI sia installato sulla tua istanza e configurato con credenziali predefinite. Per ulteriori informazioni, consulta Installazione dell' AWS CLI nella Guida per l'utente dell'AWS Command Line Interface .
- (Windows) Configura le credenziali predefinite per la tua AWS Tools for Windows PowerShell istanza. Per ulteriori informazioni, consulta Nozioni di base su AWS Tools for Windows PowerShell nella Guida per l'utente di AWS Strumenti per PowerShell .
- All'utente o al ruolo devono essere concesse le autorizzazioni che contengono la AmazonS3ReadOnlyAccess policy.

Amazon Linux 2023

Come installare il driver NVIDIA GRID sull'istanza

1. Connettiti alla tua istanza. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo dnf update -y
```

2. Installare gcc e make, se non sono già installati.

```
[ec2-user ~]$ sudo dnf install gcc make
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installa i pacchetti delle intestazioni kernel.

```
[ec2-user ~]$ sudo dnf install -y kernel-devel kernel-modules-extra
```

6. Scaricare l'utilità di installazione del driver GRID utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   In questo bucket vengono archiviate più versioni di un driver GRID. È possibile visualizzare tutte le versioni disponibili con il comando seguente.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Eseguire lo script di installazione automatica come segue per installare il driver GRID scaricato. Ad esempio:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

   Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

9. Verificare che il driver funzioni. La risposta al seguente comando elenca la versione del driver NVIDIA installata e i dettagli sulle GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Se utilizzi il software vGPU NVIDIA versione 14.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consulta la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

12. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

    a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni Amazon DCV.

b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze Amazon EC2 GPU-based.

Amazon Linux 2

Come installare il driver NVIDIA GRID sull'istanza

1. Connettiti alla tua istanza. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

2. Installare gcc e make, se non sono già installati.

```
[ec2-user ~]$ sudo yum install gcc make
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installa il pacchetto delle intestazioni kernel per la versione del kernel in esecuzione.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

6. Scaricare l'utilità di installazione del driver GRID utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

In questo bucket vengono archiviate più versioni di un driver GRID. È possibile visualizzare tutte le versioni disponibili con il comando seguente.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Eseguire lo script di installazione automatica come segue per installare il driver GRID scaricato. Ad esempio:

   ```
   [ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
   ```

   Se si utilizza Amazon Linux 2 con kernel versione 5.10, utilizzare il comando seguente per installare il driver GRID.

   ```
   [ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
   ```

   Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

9. Verificare che il driver funzioni. La risposta al seguente comando elenca la versione del driver NVIDIA installata e i dettagli sulle GPU.

   ```
   [ec2-user ~]$ nvidia-smi -q | head
   ```

10. Se utilizzi il software vGPU NVIDIA versione 14.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consulta la documentazione di NVIDIA.

    ```
    [ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    [ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
    etc/modprobe.d/nvidia.conf
    ```

11. Riavviare l'istanza.

    ```
    [ec2-user ~]$ sudo reboot
    ```

12. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

    a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni Amazon DCV.

b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze Amazon EC2 GPU-based.

CentOS 7 e Red Hat Enterprise Linux 7

Come installare il driver NVIDIA GRID sull'istanza

1. Connettiti alla tua istanza. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

2. Installare gcc e make, se non sono già installati.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installa il pacchetto delle intestazioni kernel per la versione del kernel in esecuzione.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

6. Disattivare il driver open source `nouveau` per le schede grafiche NVIDIA.

   a. Aggiungere `nouveau` al file di blacklist `/etc/modprobe.d/blacklist.conf`. Copiare il seguente blocco di codice e incollarlo in un terminale.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

b. Modificare il file `/etc/default/grub` e aggiungere la seguente riga:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

c. Ricompilare il file di configurazione di Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Scaricare l'utilità di installazione del driver GRID utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

In questo bucket vengono archiviate più versioni di un driver GRID. È possibile visualizzare tutte le versioni disponibili con il comando seguente.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

8. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

9. Eseguire lo script di installazione automatica come segue per installare il driver GRID scaricato. Ad esempio:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

10. Verificare che il driver funzioni. La risposta al seguente comando elenca la versione del driver NVIDIA installata e i dettagli sulle GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. Se utilizzi il software vGPU NVIDIA versione 14.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consulta la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

12. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

13. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

    a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni Amazon DCV.

    b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze Amazon EC2 GPU-based.

    c. Installa il pacchetto GUI desktop/workstation .

    ```
    [ec2-user ~]$ sudo yum groupinstall -y "Server with GUI"
    ```

Per CentOS Stream 8 e Red Hat Enterprise Linux 8

Come installare il driver NVIDIA GRID sull'istanza

1. Connettiti alla tua istanza. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

2. Installare gcc e make, se non sono già installati.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installa il pacchetto delle intestazioni kernel per la versione del kernel in esecuzione.

```
[ec2-user ~]$ sudo dnf install -y elfutils-libelf-devel libglvnd-devel kernel-
devel-$(uname -r)
```

6. Scaricare l'utilità di installazione del driver GRID utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   In questo bucket vengono archiviate più versioni di un driver GRID. È possibile visualizzare tutte le versioni disponibili con il comando seguente.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Eseguire lo script di installazione automatica come segue per installare il driver GRID scaricato. Ad esempio:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

   Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

9. Verificare che il driver funzioni. La risposta al seguente comando elenca la versione del driver NVIDIA installata e i dettagli sulle GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Se utilizzi il software vGPU NVIDIA versione 14.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consulta la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

12. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

    a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni Amazon DCV.

    b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze Amazon EC2 GPU-based.

    c. Installare il pacchetto workstation della GUI.

    ```
    [ec2-user ~]$ sudo dnf groupinstall -y workstation
    ```

Rocky Linux 8

Per installare il driver NVIDIA GRID sull'istanza Linux

1. Connettiti alla tua istanza. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

2. Installare gcc e make, se non sono già installati.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installa il pacchetto delle intestazioni kernel per la versione del kernel in esecuzione.

```
[ec2-user ~]$ sudo dnf install -y elfutils-libelf-devel libglvnd-devel kernel-
devel-$(uname -r)
```

6. Scaricare l'utilità di installazione del driver GRID utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   In questo bucket vengono archiviate più versioni di un driver GRID. È possibile visualizzare tutte le versioni disponibili con il comando seguente.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Eseguire lo script di installazione automatica come segue per installare il driver GRID scaricato. Ad esempio:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

   Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

9. Verificare che il driver funzioni. La risposta al seguente comando elenca la versione del driver NVIDIA installata e i dettagli sulle GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Se utilizzi il software vGPU NVIDIA versione 14.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consulta la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

12. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

    a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni Amazon DCV.

    b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze Amazon EC2 GPU-based.

Ubuntu e Debian

Come installare il driver NVIDIA GRID sull'istanza

1. Connettiti alla tua istanza. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
$ sudo apt-get update -y
```

2. Installare gcc e make, se non sono già installati.

```
$ sudo apt-get install -y gcc make
```

3. (Ubuntu) Aggiornare il pacchetto `linux-aws` per ricevere la versione più recente.

```
$ sudo apt-get upgrade -y linux-aws
```

   (Debian) Aggiornare il pacchetto per ricevere la versione più recente.

```
$ sudo apt-get upgrade -y
```

4. Riavviare l'istanza per caricare la versione più recente del kernel.

```
$ sudo reboot
```

5. Riconnettersi all'istanza dopo averla riavviata.
6. Installare il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
$ sudo apt-get install -y linux-headers-$(uname -r) linux-modules-extra-$(uname -r)
```

7. Disattivare il driver open source `nouveau` per le schede grafiche NVIDIA.

   a. Aggiungere `nouveau` al file di blacklist `/etc/modprobe.d/blacklist.conf`. Copiare il seguente blocco di codice e incollarlo in un terminale.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Modificare il file `/etc/default/grub` e aggiungere la seguente riga:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Ricompilare il file di configurazione di Grub.

```
$ sudo update-grub
```

8. Scaricare l'utilità di installazione del driver GRID utilizzando il seguente comando:

```
$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   In questo bucket vengono archiviate più versioni di un driver GRID. È possibile visualizzare tutte le versioni disponibili con il comando seguente.

```
$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente.

```
$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Eseguire lo script di installazione automatica come segue per installare il driver GRID scaricato. Ad esempio:

```
$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

11. Verificare che il driver funzioni. La risposta al seguente comando elenca la versione del driver NVIDIA installata e i dettagli sulle GPU.

```
$ nvidia-smi -q | head
```

12. Se utilizzi il software vGPU NVIDIA versione 14.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consulta la documentazione di NVIDIA.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

13. Riavviare l'istanza.

```
$ sudo reboot
```

14. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

    a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni Amazon DCV.

b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze Amazon EC2 GPU-based.

c. Installa il pacchetto GUI desktop/workstation .

```
$ sudo apt-get install -y lightdm ubuntu-desktop
```

Sistemi operativi Windows

Per installare il driver NVIDIA GRID sull'istanza di Windows

1. Connettiti alla tua istanza di Windows e apri una PowerShell finestra.
2. Scarica i driver e il contratto di licenza per l'utente finale di NVIDIA GRID Cloud da Amazon S3 sul desktop utilizzando i seguenti PowerShell comandi.

```
$Bucket = "ec2-windows-nvidia-drivers"
$KeyPrefix = "latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
$LocalFilePath = Join-Path $LocalPath $LocalFileName
Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

In questo bucket, vengono archiviate più versioni di un driver NVIDIA GRID. È possibile scaricare tutte le versioni di Windows disponibili nel bucket rimuovendo l'opzione `-KeyPrefix $KeyPrefix`. Per informazioni sulla versione del driver NVIDIA GRID per il sistema operativo in uso, consulta NVIDIA® Virtual GPU (vGPU) Software sul sito web di NVIDIA.

A partire da GRID versione 11.0 puoi utilizzare i driver in `latest` per le istanze G3 e G4dn. Non verranno aggiunte versioni successive alla 11.0 a `g4/latest`, ma la versione 11.0 e le versioni precedenti specifiche di G4dn continueranno a stare in `g4/latest`.

Le istanze G5 richiedono GRID 13.1 o successivo (o GRID 12.4 o successivo).

3. Accedi al desktop e apri il file di installazione per avviarlo (scegli la versione del driver che corrisponde alla versione del sistema operativo della tua istanza). Seguire le istruzioni per installare il driver e riavviare l'istanza come necessario. Per verificare che la GPU funzioni correttamente, controllare in Gestione dispositivi.
4. (Opzionale) Utilizzare il seguente comando per disabilitare la pagina di licenza nel pannello di controllo per evitare che gli utenti modifichino accidentalmente il tipo di prodotto (NVIDIA GRID Virtual Workstation è abilitata per impostazione predefinita). Per ulteriori informazioni, consulta il documento GRID Licensing User Guide.

   PowerShell

   Esegui i seguenti PowerShell comandi per creare il valore di registro per disabilitare la pagina delle licenze nel pannello di controllo. L'impostazione predefinita delle AMI AWS Strumenti per PowerShell in AWS Windows è la versione a 32 bit e questo comando ha esito negativo. Utilizza invece la versione a 64 bit PowerShell inclusa nel sistema operativo.

   ```
   New-Item -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name GridLicensing
   New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" -
   Name "NvCplDisableManageLicensePage" -PropertyType "DWord" -Value "1"
   ```

   Prompt dei comandi

   Esegui il seguente comando di registro per creare il valore di registro al fine di disabilitare la pagina delle licenze nel pannello di controllo. È possibile eseguirlo utilizzando la finestra del prompt dei comandi o una versione a 64 bit diPowerShell.

   ```
   reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" /v
    NvCplDisableManageLicensePage /t REG_DWORD /d 1
   ```

5. (Facoltativo) A seconda del caso d'uso, potresti completare le fasi facoltative riportate di seguito. Se non è necessaria questa funzionalità, non completare le fasi.

   a. Per utilizzare i quattro display con risoluzione fino a 4K, imposta il protocollo di visualizzazione ad alte prestazioni Amazon DCV.

   b. La modalità NVIDIA Quadro Virtual Workstation è abilitata per impostazione predefinita. Per attivare le funzionalità di hosting di applicazioni virtualizzate GRID per applicazioni

RDSH, completare la procedura di attivazione dell'applicazione virtualizzata GRID in Attiva le applicazioni virtuali NVIDIA GRID sulle tue istanze Amazon EC2 GPU-based.

Installa i driver di gioco NVIDIA (istanze G7e, G6, G6e, G5 e G4dn)

Questi driver AWS sono disponibili solo per i clienti. Scaricandoli, l'utente accetta di utilizzare il software scaricato solo per sviluppare AMI da utilizzare con l'hardware RTX PRO 6000 Blackwell, NVIDIA L4, NVIDIA L40S, NVIDIA A10G, NVIDIA Tesla T4 o NVIDIA Tesla M60. AWS È possibile utilizzare i driver GRID per creare e utilizzare le AMI all'interno dell'ambiente. Installando il software, sarai vincolato dai termini del contratto di licenza con l'utente finale NVIDIA GRID Cloud End User License Agreement.

Considerazioni

- Le istanze G3 richiedono una risoluzione DNS AWS fornita per il funzionamento delle licenze GRID.
- IMDSv2 è supportato solo con il driver NVIDIA versione 495.x o superiore.

Prerequisiti

- (Linux) Verifica che AWS CLI sia installato sulla tua istanza e configurato con credenziali predefinite. Per ulteriori informazioni, consulta Installazione dell' AWS CLI nella Guida per l'utente dell'AWS Command Line Interface .
- All'utente o al ruolo devono essere concesse le autorizzazioni che contengono la AmazonS3ReadOnlyAccess policy.

Amazon Linux 2023

Come installare il driver di gioco NVIDIA sull'istanza

1. Connettiti alla tua istanza. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

   ```
   [ec2-user ~]$ sudo dnf update -y
   ```

2. Installare gcc e make, se non sono già installati.

```
[ec2-user ~]$ sudo dnf install gcc make
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettiti alla tua istanza dopo averla riavviata.
5. Installa i pacchetti delle intestazioni kernel.

```
[ec2-user ~]$ sudo dnf install -y kernel-devel kernel-modules-extra kernel-devel-
$(uname -r) kernel-headers-$(uname -r) dkms
```

6. Scaricare l'utilità di installazione del driver di gioco utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   In questo bucket, vengono archiviate più versioni di un driver di gioco. È possibile visualizzare tutte le versioni disponibili con il comando seguente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Estrarre l'utilità di installazione del driver di gioco dall'archivio `.zip` scaricato.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

8. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Eseguire il programma di installazione utilizzando l'URL seguente:

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

   Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

10. Per creare il file di configurazione richiesto, utilizza i comandi seguenti.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Utilizza il comando seguente per scaricare e rinominare il file certificato.
    - Per la versione 590.48 o successiva:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert_2026_03_02.cert"
      ```

    - Per le versioni da 575.64 a 580.105.08:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2025_07_01.cert"
      ```

    - Per le versioni da 460.39 a 575.57:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
      ```

    - Per le versioni da 440.68 a 445.48:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Per le versioni precedenti:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

12. Se utilizzi il driver NVIDIA versione 510.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consulta la documentazione di NVIDIA.

    ```
    [ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    [ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
    ```

13. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

14. Verificare la licenza NVIDIA Gaming utilizzando il seguente comando:

```
[ec2-user ~]$ nvidia-smi.exe -q
```

Nell'output, cerca per `vGPU Software Licensed Product`.

15. (Facoltativo) Per utilizzare un display singolo con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni Amazon DCV.

Amazon Linux 2

Come installare il driver di gioco NVIDIA sull'istanza

1. Connettiti alla tua istanza. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

2. Installare gcc e make, se non sono già installati.

```
[ec2-user ~]$ sudo yum install gcc make
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettiti alla tua istanza dopo averla riavviata.
5. Installare il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

6. Scaricare l'utilità di installazione del driver di gioco utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

In questo bucket, vengono archiviate più versioni di un driver di gioco. È possibile visualizzare tutte le versioni disponibili con il comando seguente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Estrarre l'utilità di installazione del driver di gioco dall'archivio `.zip` scaricato.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

8. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Eseguire il programma di installazione utilizzando l'URL seguente:

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Se si utilizza Amazon Linux 2 con kernel versione 5.10, utilizzare il comando seguente per installare i driver di gioco NVIDIA.

```
[ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

10. Per creare il file di configurazione richiesto, utilizza i comandi seguenti.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Utilizza il comando seguente per scaricare e rinominare il file certificato.

    - Per la versione 590.48 o successiva:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
      gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert_2026_03_02.cert"
      ```

    - Per le versioni da 575.64 a 580.105.08:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2025_07_01.cert"
```

- Per le versioni da 460.39 a 575.57:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

- Per le versioni da 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Per le versioni precedenti:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Se utilizzi il driver NVIDIA versione 510.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consulta la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

14. Verificare la licenza NVIDIA Gaming utilizzando il seguente comando:

```
[ec2-user ~]$ nvidia-smi.exe -q
```

Nell'output, cerca per `vGPU Software Licensed Product`.

15. (Facoltativo) Per utilizzare un display singolo con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni Amazon DCV.

CentOS 7 e Red Hat Enterprise Linux 7

Come installare il driver di gioco NVIDIA sull'istanza

1. Connessione a un'istanza Linux. Installare gcc e make, se non sono già installati.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installare il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
[ec2-user ~]$ sudo yum install -y unzip kernel-devel-$(uname -r)
```

6. Disattivare il driver open source `nouveau` per le schede grafiche NVIDIA.

   a. Aggiungere `nouveau` al file di blacklist `/etc/modprobe.d/blacklist.conf`. Copiare il seguente blocco di codice e incollarlo in un terminale.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Modificare il file `/etc/default/grub` e aggiungere la seguente riga:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Ricompilare il file di configurazione di Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Scaricare l'utilità di installazione del driver di gioco utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   In questo bucket, vengono archiviate più versioni di un driver di gioco. È possibile visualizzare tutte le versioni disponibili con il comando seguente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Estrarre l'utilità di installazione del driver di gioco dall'archivio `.zip` scaricato.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

9. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

10. Eseguire il programma di installazione utilizzando l'URL seguente:

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

    Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

11. Per creare il file di configurazione richiesto, utilizza i comandi seguenti.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Utilizza il comando seguente per scaricare e rinominare il file certificato.
    - Per la versione 590.48 o successiva:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert_2026_03_02.cert"
```

    - Per le versioni da 575.64 a 580.105.08:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2025_07_01.cert"
```

- Per le versioni da 460.39 a 575.57:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

- Per le versioni da 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Per le versioni precedenti:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

13. Se utilizzi il driver NVIDIA versione 510.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consulta la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

14. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

15. (Facoltativo) Per utilizzare un display singolo con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni Amazon DCV. Se non è necessaria questa funzionalità, non completare questa fase.

Per CentOS Stream 8 e Red Hat Enterprise Linux 8

Come installare il driver di gioco NVIDIA sull'istanza

1. Connessione a un'istanza Linux. Installare gcc e make, se non sono già installati.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installare il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
[ec2-user ~]$ sudo yum install -y unzip kernel-devel-$(uname -r)
```

6. Scaricare l'utilità di installazione del driver di gioco utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   In questo bucket, vengono archiviate più versioni di un driver di gioco. È possibile visualizzare tutte le versioni disponibili con il comando seguente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Estrarre l'utilità di installazione del driver di gioco dall'archivio `.zip` scaricato.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Eseguire il programma di installazione utilizzando l'URL seguente:

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

10. Per creare il file di configurazione richiesto, utilizza i comandi seguenti.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Utilizza il comando seguente per scaricare e rinominare il file certificato.

- Per la versione 590.48 o successiva:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert_2026_03_02.cert"
```

- Per le versioni da 575.64 a 580.105.08:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2025_07_01.cert"
```

- Per le versioni da 460.39 a 575.57:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

- Per le versioni da 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Per le versioni precedenti:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Se utilizzi il driver NVIDIA versione 510.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consulta la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

14. (Facoltativo) Per utilizzare un display singolo con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni Amazon DCV.

Rocky Linux 8

Come installare il driver di gioco NVIDIA sull'istanza

1. Connessione a un'istanza Linux. Installare gcc e make, se non sono già installati.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
[ec2-user ~]$ sudo yum update -y
```

3. Riavviare l'istanza per caricare la versione più recente del kernel.

```
[ec2-user ~]$ sudo reboot
```

4. Riconnettersi all'istanza dopo averla riavviata.
5. Installare il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
[ec2-user ~]$ sudo dnf install -y unzip elfutils-libelf-devel libglvnd-devel
 kernel-devel-$(uname -r)
```

6. Scaricare l'utilità di installazione del driver di gioco utilizzando il seguente comando:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

In questo bucket, vengono archiviate più versioni di un driver di gioco. È possibile visualizzare tutte le versioni disponibili con il comando seguente:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Estrarre l'utilità di installazione del driver di gioco dall'archivio `.zip` scaricato.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Eseguire il programma di installazione utilizzando l'URL seguente:

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

10. Per creare il file di configurazione richiesto, utilizza i comandi seguenti.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Utilizza il comando seguente per scaricare e rinominare il file certificato.
    - Per la versione 590.48 o successiva:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
      gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert_2026_03_02.cert"
      ```

    - Per le versioni da 575.64 a 580.105.08:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
      gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2025_07_01.cert"
      ```

- Per le versioni da 460.39 a 575.57:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

- Per le versioni da 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Per le versioni precedenti:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Se utilizzi il driver NVIDIA versione 510.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consulta la documentazione di NVIDIA.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Riavviare l'istanza.

```
[ec2-user ~]$ sudo reboot
```

14. (Facoltativo) Per utilizzare un display singolo con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni Amazon DCV.

Ubuntu e Debian

Come installare il driver di gioco NVIDIA sull'istanza

1. Connessione a un'istanza Linux. Installare gcc e make, se non sono già installati.

```
$ sudo apt-get install -y gcc make build-essential
```

2. Aggiornare la cache dei pacchetti e ottenere gli aggiornamenti dei pacchetti per l'istanza.

```
$ sudo apt-get update -y
```

3. Aggiornare il pacchetto `linux-aws` per ricevere la versione più recente.

```
$ sudo apt-get upgrade -y linux-aws
```

4. Riavviare l'istanza per caricare la versione più recente del kernel.

```
$ sudo reboot
```

5. Riconnettersi all'istanza dopo averla riavviata.
6. Installare il pacchetto delle intestazioni kernel per la versione del kernel correntemente in esecuzione.

```
$ sudo apt install -y unzip dkms linux-headers-$(uname -r)
```

7. Disattivare il driver open source `nouveau` per le schede grafiche NVIDIA.

   a. Aggiungere `nouveau` al file di blacklist `/etc/modprobe.d/blacklist.conf`. Copiare il seguente blocco di codice e incollarlo in un terminale.

   ```
   $ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   EOF
   ```

   b. Modificare il file `/etc/default/grub` e aggiungere la seguente riga:

   ```
   GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
   ```

   c. Ricompilare il file di configurazione di Grub.

   ```
   $ sudo update-grub
   ```

8. Scaricare l'utilità di installazione del driver di gioco utilizzando il seguente comando:

```
$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

In questo bucket, vengono archiviate più versioni di un driver di gioco. È possibile visualizzare tutte le versioni disponibili con il comando seguente:

```
$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Estrarre l'utilità di installazione del driver di gioco dall'archivio `.zip` scaricato.

```
$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

10. Aggiungere autorizzazioni per eseguire l'utilità di installazione del driver utilizzando il comando seguente:

```
$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

11. Eseguire il programma di installazione utilizzando l'URL seguente:

```
$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Quando richiesto, accettare il contratto di licenza e specificare le opzioni di installazione come necessario (è possibile accettare le opzioni predefinite).

12. Per creare il file di configurazione richiesto, utilizza i comandi seguenti.

```
$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Utilizza il comando seguente per scaricare e rinominare il file certificato.

- Per la versione 590.48 o successiva:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert_2026_03_02.cert"
```

- Per le versioni da 575.64 a 580.105.08:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2025_07_01.cert"
```

- Per le versioni da 460.39 a 575.57:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

- Per le versioni da 440.68 a 445.48:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Per le versioni precedenti:

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

14. Se utilizzi il driver NVIDIA versione 510.x o superiore sulle istanze G4dn, G5 o G5g, disabilita GSP con i seguenti comandi. Per ulteriori informazioni sul motivo per cui questa azione è necessaria, consulta la documentazione di NVIDIA.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

15. Riavviare l'istanza.

```
$ sudo reboot
```

16. (Facoltativo) Per utilizzare un display singolo con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni Amazon DCV. Se non è necessaria questa funzionalità, non completare questa fase.

Sistemi operativi Windows

Prima di installare un driver di gioco NVIDIA sulla tua istanza, devi assicurarti che siano soddisfatti i seguenti prerequisiti, oltre alle considerazioni menzionate per tutti i driver di gioco.

- Se si avvia l'istanza di Windows utilizzando una AMI Windows personalizzata, l'AMI deve essere un'immagine standardizzata creata con Windows Sysprep per garantire che il driver di gioco funzioni. Per ulteriori informazioni, consulta Creare un'AMI Amazon EC2 utilizzando Windows Sysprep.

- Configura le credenziali predefinite per l' AWS Tools for Windows PowerShell istanza di Windows. Per ulteriori informazioni, consulta Nozioni di base su AWS Tools for Windows PowerShell nella Guida per l'utente di AWS Strumenti per PowerShell .

Per installare il driver di gioco NVIDIA sull'istanza di Windows

1. Connettiti alla tua istanza Windows e apri una PowerShell finestra.
2. Scarica e installa il driver di gioco utilizzando i seguenti PowerShell comandi.

```
$Bucket = "nvidia-gaming"
$KeyPrefix = "windows/latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
$LocalFilePath = Join-Path $LocalPath $LocalFileName
Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

   In questo bucket S3 vengono archiviate più versioni di un driver NVIDIA GRID. Puoi scaricare tutte le versioni disponibili nel bucket modificando il valore della `$KeyPrefix` variabile da "windows/latest" a «windows».
3. Accedi al desktop e apri il file di installazione per avviarlo (scegli la versione del driver che corrisponde alla versione del sistema operativo della tua istanza). Seguire le istruzioni per installare il driver e riavviare l'istanza come necessario. Per verificare che la GPU funzioni correttamente, controlla in Gestione dispositivi.
4. Per registrare il driver, utilizza uno dei seguenti metodi.

   Version 527.27 or above

   Crea la seguente chiave di registro con la versione a 64 bit di PowerShell, o la finestra del prompt dei comandi.

   chiave: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global`

nome: v GamingMarketplace

tipo: DWord

valore: 2

PowerShell

Esegui il PowerShell comando seguente per creare questo valore di registro. L'impostazione predefinita delle AMI AWS Strumenti per PowerShell in AWS Windows è la versione a 32 bit e questo comando ha esito negativo. Utilizza invece la versione a 64 bit PowerShell inclusa nel sistema operativo.

```
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global"
 -Name "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Prompt dei comandi

Esegui il seguente comando di registro per creare questo valore di registro. È possibile eseguirlo utilizzando la finestra del prompt dei comandi o una versione a 64 bit di PowerShell.

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global" /v
 vGamingMarketplace /t REG_DWORD /d 2
```

Earlier versions

Crea la seguente chiave di registro con la versione a 64 bit di PowerShell, o la finestra del prompt dei comandi.

chiave: `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global`

nome: v GamingMarketplace

tipo: DWord

valore: 2

PowerShell

Esegui il PowerShell comando seguente per creare questo valore di registro. L'impostazione predefinita delle AMI AWS Strumenti per PowerShell in AWS Windows è la versione a 32 bit e questo comando ha esito negativo. Utilizza invece la versione a 64 bit PowerShell inclusa nel sistema operativo.

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name
 "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Prompt dei comandi

Esegui il seguente comando di registro per creare questa chiave di registro con la finestra del prompt dei comandi. È inoltre possibile utilizzare questo comando nella versione a 64 bit diPowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global" /v vGamingMarketplace /t
 REG_DWORD /d 2
```

5. Esegui il comando seguente in PowerShell. In tal modo, viene scaricato il file del certificato, viene rinominato il file `GridSwCert.txt` e viene spostato il file nella cartella Documenti pubblici dell'unità di sistema. In genere, il percorso della cartella è `C:\Users\Public\Documents`.

   - Per la versione 591.59 o successiva:

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCert_2026_03_02.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   - Per le versioni da 576.80 a 581.80:

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCertWindows_2025_07_01.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   - Per le versioni da 460.39 a 576.72:

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCertWindows_2024_02_22.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   - Per la versione 445.87:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCert-Windows_2020_04.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

- Per le versioni precedenti:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCert-Windows_2019_09.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

Se ricevi un errore durante il download del file e stai utilizzando Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il tuo terminale. PowerShell Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il comando seguente e riprovare:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

6. Riavviare l'istanza.
7. Individua il file `nvidia-smi.exe` sull'istanza.

```
Get-ChildItem -Path C:\ -Recurse -Filter "nvidia-smi.exe"
```

Verificare la licenza NVIDIA Gaming utilizzando il seguente comando: Sostituisci *`path`* con il nome della cartella nell'output del comando precedente.

```
C:\Windows\System32\DriverStore\FileRepository\path\nvidia-smi.exe -q
```

L'output visualizzato dovrebbe essere simile al seguente.

```
vGPU Software Licensed Product
Product Name              : NVIDIA Cloud Gaming
License Status            : Licensed (Expiry: N/A)
```

8. (Facoltativo) Per utilizzare i quattro display con risoluzione fino a 4K, configurare il protocollo di visualizzazione ad alte prestazioni Amazon DCV. Se non è necessaria questa funzionalità, non completare questa fase.

Installa il driver ENA su istanze EC2 Windows

Se l'istanza non è basata su una delle più recenti Amazon Machine Image (AMI) di Windows fornite da Amazon, utilizza la seguente procedura per installare il driver ENA corrente sull'istanza. Devi eseguire questo aggiornamento quando è opportuno riavviare l'istanza. Se lo script di installazione non riavvia automaticamente l'istanza, riavvia l'istanza come fase finale.

Se si utilizza un volume di archivio dell'istanza per memorizzare i dati mentre l'istanza è in esecuzione, tali dati vengono cancellati quando si arresta l'istanza. Prima di arrestare la tua istanza, verifica di aver copiato tutti i dati necessari dai volumi di archivio dell'istanza nell'archiviazione persistente, ad esempio Amazon EBS o Amazon S3.

Prerequisiti

Per installare o aggiornare il driver ENA, l'istanza Windows deve soddisfare i seguenti prerequisiti:

- PowerShell è installata la versione 3.0 o successiva.
- I comandi mostrati in questa sezione devono essere eseguiti nella versione a 64 bit diPowerShell. Non utilizzare la x86 versione di PowerShell. Questa è la versione a 32 bit della shell e non è supportata per questi comandi.

Fase 1: esegui il backup dei dati

Crea un'AMI di backup, nel caso in cui non riesci a eseguire il rollback delle modifiche tramite Gestione dispositivi. Per creare un'AMI di backup con Console di gestione AWS, segui questi passaggi:

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza che richiede l'aggiornamento del driver e scegli Arresta istanza dal menu di stato dell'istanza.
4. Dopo l'arresto dell'istanza, selezionala di nuovo. Per creare il backup, scegli Immagine e modelli dal menu Azioni, quindi scegli Crea immagine.
5. Per riavviare l'istanza, scegli Avvia istanza dal menu Stato dell'istanza.

Fase 2: installazione o aggiornamento del driver ENA

È possibile installare o aggiornare il driver ENA con AWS Systems Manager Distributor o con i PowerShell cmdlet. Per ulteriori istruzioni, selezionare la scheda corrispondente al metodo che vuoi utilizzare.

Systems Manager Distributor

Puoi utilizzare la funzione Systems Manager Distributor per distribuire i pacchetti ai nodi gestiti da Systems Manager. Con Systems Manager Distributor puoi installare il pacchetto di driver ENA una sola volta o con aggiornamenti programmati. Per ulteriori informazioni su come installare il pacchetto driver ENA (`AwsEnaNetworkDriver`) con Systems Manager Distributor, consulta Installare o aggiornare i pacchetti nella Guida per l'AWS Systems Manager utente.

PowerShell

Questa sezione spiega come scaricare e installare i pacchetti di driver ENA sull'istanza con i cmdlet. PowerShell

Opzione 1: scarica ed estrai l'ultima versione

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. Usa il cmdlet invoke-webrequest per scaricare il pacchetto driver più recente:

```
PS C:\> invoke-webrequest https://ec2-windows-drivers-
downloads.s3.amazonaws.com/ENA/Latest/AwsEnaNetworkDriver.zip -
outfile $env:USERPROFILE\AwsEnaNetworkDriver.zip
```

> **Note**
>
> Se ricevi un errore durante il download del file e stai utilizzando Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il tuo terminale. PowerShell Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il comando seguente e riprovare:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

In alternativa, puoi scaricare il pacchetto driver più recente da una finestra del browser dell'istanza.

3. Utilizza il cmdlet expand-archive per estrarre l'archivio zip che hai scaricato nella tua istanza:

```
PS C:\> expand-archive $env:userprofile\AwsEnaNetworkDriver.zip -
DestinationPath $env:userprofile\AwsEnaNetworkDriver
```

Opzione 2: scarica ed estrai una versione specifica

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. Scarica il pacchetto driver ENA per la versione specifica che desideri dal link della versione nella tabella Cronologia della versione del driver ENA Windows.
3. Estrai l'archivio .zip nella tua istanza.

Installa il driver ENA con PowerShell

Le fasi di installazione sono le stesse indipendentemente dal fatto che tu abbia scaricato il driver più recente o una versione specifica. Per installare il driver ENA, segui questi passaggi.

1. Per installare il driver, esegui `install.ps1` PowerShell lo script dalla `AwsEnaNetworkDriver` directory sulla tua istanza. Se ricevi un errore, assicurati di utilizzare la PowerShell versione 3.0 o successiva.
2. Se il programma di installazione non riavvia automaticamente l'istanza, esegui il cmdlet. Restart-Computer PowerShell

```
PS C:\> Restart-Computer
```

Fase 3 (opzionale): verifica la versione del driver ENA dopo l'installazione

Per assicurarti che il pacchetto driver ENA sia stato installato correttamente sulla tua istanza, puoi verificare la nuova versione come segue:

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.

3. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
4. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
5. Scegliere il nome o aprire il menu contestuale per Adattatore elastico di rete Amazon e quindi Proprietà. In questo modo si apre la finestra di dialogo delle proprietà di Amazon Elastic Network Adapter.

   > **Note**
   >
   > Gli adattatori ENA utilizzano tutti lo stesso driver. Se disponi di più adattatori ENA, puoi selezionarne uno qualsiasi per aggiornare il driver per tutti gli adattatori ENA.

6. Per verificare la versione corrente installata, apri la scheda Driver e controlla la versione del driver. Se la versione corrente non corrisponde alla versione di interesse, consulta Risoluzione dei problemi del driver dell'Adattatore elastico di rete per Windows.

Roll back di un driver ENA

Se qualcosa va storto durante l'installazione, potrebbe essere necessario tornare alla versione precedente del driver. Segui questi passaggi per ripristinare la versione precedente del driver ENA installata sull'istanza.

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
4. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
5. Scegliere il nome o aprire il menu contestuale per Adattatore elastico di rete Amazon e quindi Proprietà. In questo modo si apre la finestra di dialogo delle proprietà di Amazon Elastic Network Adapter.

   > **Note**
   >
   > Gli adattatori ENA utilizzano tutti lo stesso driver. Se disponi di più adattatori ENA, puoi selezionarne uno qualsiasi per aggiornare il driver per tutti gli adattatori ENA.

6. Per ripristinare il driver, apri la scheda Driver e scegli Roll back dei driver. In questo modo si apre la finestra di dialogo di rollback dei Pacchetti driver.

> **Note**
>
> Se la scheda Driver non mostra l'azione Rollback dei driver o se l'azione non è disponibile, significa che l'Archivio dei driver dell'istanza non contiene il pacchetto driver installato in precedenza. Per risolvere questo problemaScenari per la risoluzione dei problemi, consulta ed espandi la sezione Installazione della versione non prevista del driver ENA. Per ulteriori informazioni sul processo di selezione dei pacchetti driver del dispositivo, consulta Modalità con cui Windows seleziona un pacchetto driver per un dispositivo nel sito web della documentazione Microsoft.

Traccia rilasci della versione del driver ENA Windows

Le AMI di Windows includono il driver ENA Windows per abilitare le reti avanzate.

Per le versioni di Windows Server 2016 e successive, consigliamo di utilizzare la versione più recente del driver. Per le versioni precedenti di Windows Server, consulta la tabella seguente per determinare quale versione del driver ENA utilizzare.

Versione di Windows Server	Versione driver ENA
Windows Server 2012 R2	2.6.0 e precedenti
Windows Server 2012	2.6.0 e precedenti
Windows Server 2008 R2	versioni 2.2.3 e precedenti

Cronologia della versione del driver ENA Windows

Nella tabella seguente sono riepilogate le modifiche relative a ciascuna versione.

Versione driver	Dettagli	Data di rilascio
2.11.0	Nuove funzionalità •	1 agosto 2025

Versione driver	Dettagli	Data di rilascio
	È stato aggiunto il supporto per l'allocazione dinamica delle code con scalabilità fino a 64 I/O code, soggetto ai limiti del tipo di istanza. Correzioni di bug • È stata corretta la gestione mancante delle condizioni di errore durante il recupero della larghezza dell'indirizzo DMA fisico dal dispositivo.	
2.10.0	Correzioni di bug • È stata risolta la gestione impropria degli errori di allocazione della memoria durante l'inizializzazione della coda per evitare riavvii imprevisti. • È stata risolta una possibile configurazione errata degli offload di rete in cui le funzionalità del dispositivo venivano ignorate.	24 giugno 2025

Versione driver	Dettagli	Data di rilascio
2.9.0	Nuove funzionalità • È stato aggiunto il supporto per le richieste di ripristino asincrone avviate dal dispositivo. • È stato aggiunto il supporto per la gestione del valore massimo di profondità LLQ fornito dal dispositivo. • È stato aggiunto l'ID evento `58001` in Windows Event Viewer per migliorare la visibilità in caso di transizioni impreviste dello stato di alimentazione causate da un'errata configurazione del dispositivo. Correzioni di bug • È stata risolta la gestione impropria degli errori di allocazione della memoria durante l'inizializzazione del dispositivo per evitare riavvii imprevisti. • È stato risolto un problema nella routine del servizio di interruzione che poteva mettere in coda un DPC durante l'arresto del dispositivo, impedendo riavvii imprevisti.	12 dicembre 2024

Versione driver	Dettagli	Data di rilascio
2.8.0	Correzioni di bug • Correzione di una race condition nel flusso completo di elaborazione della lista di buffer di rete (NBL) in uscita, che poteva portare al danneggiamento della memoria causato dal tentativo di rilasciare una NBL già rilasciata. • Correzione dell'errato rilevamento del protocollo L3 durante la disabilitazione di tutti gli offload di LSO e checksum che poteva portare a comportamenti imprevisti.	30 settembre 2024

Versione driver	Dettagli	Data di rilascio
2.7.0	Nuove funzionalità • Rimozione del supporto per Windows Server 2012 (Windows 8) e Windows Server 2012 R2 (Windows 8.1). Queste versioni del sistema operativo hanno raggiunto la fine del supporto da AWS. L'installazione del driver avrà esito negativo in Windows Server 2012 e versioni precedenti. • Aggiunta del supporto per l'offload del calcolo del checksum Tx IPv6 sul dispositivo. • Aggiunta di un ampio supporto per Low Latency Queuing (LLQ). Questa funzione è abilitata in modo dinamico in base alle raccomandazioni del dispositivo. Puoi sovrascrivere questa impostazione con la nuova chiave di registro "WideLLQ". • Aggiunta della segnalazione di perdite di pacchetti dovute al sovraccarico di Rx, che indica uno spazio insufficiente nell'anello Rx per i pacchetti in entrata. • Aggiunta del supporto per le notifiche di configura zione non ottimali provenienti dal dispositivo. Vedi l'ID dell'evento `59000` nel visualizzatore eventi di Windows. Correzioni di bug • Evita il ripristino innecessario del dispositivo causato da pacchetti Tx con intestazioni che superano la dimensione massima dell'intestazione Low Latency Queuing (LLQ).	1º maggio 2024

Versione driver	Dettagli	Data di rilascio

2.6.0	Nuove funzionalità
	• Aggiunge i seguenti parametri delle prestazioni di rete per i tipi di istanze che supportano ENA Express.
	  • `ena_srd_mode`
	  • `ena_srd_tx_pkts`
	  • `ena_srd_eligible_tx_pkts`
	  • `ena_srd_rx_pkts`
	  • `ena_srd_resource_utilization`
	• Aggiunge il parametro delle prestazioni di rete `conntrack_allowance_available` per i tipi di istanze basati su Nitro.
	• Aggiunge un nuovo motivo di ripristino dell'adattatore dovuto al rilevamento di un danneggiamento dei dati RX.
	• Aggiorna l'infrastruttura di registrazione dei driver.
	
	Correzioni di bug
	• Impedisce il ripristino dell'adattatore nel caso in cui l'esaurimento della CPU causi il fallimento dell'aggi ornamento dei parametri delle prestazioni di rete.
	• Impedisce la falsa rilevazione di un'interruzione dell'heartbeat del dispositivo.
		20 giugno 2023

Versione driver	Dettagli	Data di rilascio
	• Corregge lo script di installazione del driver per supportare l'operazione di downgrade. • Corregge la statistica del conteggio degli errori di ricezione.	
2.5.0	Annuncio È stata ripristinata la versione 2.5.0 del driver ENA per Windows a causa della mancata inizializzazione sul controller di dominio Windows. Windows Client e Windows Server non sono stati interessati.	17 febbraio 2023

Versione driver	Dettagli	Data di rilascio
2.4.0	Nuove funzionalità • Aggiunto il supporto per Windows Server 2022. • Rimosso il supporto per Windows Server 2008 R2. • Imposta LLQ (Low Latency Queuing) su sempre attivo per migliorare le prestazioni delle istanze Amazon EC2 di sesta generazione. Correzioni di bug • Corregge la mancata pubblicazione dei parametri delle prestazioni di rete nel sistema PCW di unità di conteggio delle prestazioni di Windows. • Corregge una perdita di memoria durante l'operazione di lettura della chiave di registro. • Impedisce un ciclo di ripristino infinito in caso di errore irrecuperabile durante il processo di ripristino dell'adattatore.	28 aprile 2022

Versione driver	Dettagli	Data di rilascio
2.2.4	Annuncio È stato eseguito il ripristino dello stato precedente del driver ENA Windows versione 2.2.4 a causa del potenziale peggioramento delle prestazioni nelle istanze EC2 di sesta generazione. È consigliabile eseguire il downgrade del driver, usando uno dei metodi seguenti: • Installazione della versione precedente 1. Scarica la versione precedente del pacchetto dal collegamento in questa tabella (versione 2.2.3). 2. Esegui lo script install.ps1 PowerShell di installazione. Per ulteriori dettagli sulle fasi di pre-installazione e post-installazione, consulta Abilitazione delle reti avanzate su Windows. • Utilizzo di Amazon EC2 Systems Manager per un aggiornamento in blocco • Esegui un aggiornamento in blocco tramite il documento SSM `AWS-ConfigureAWSPackage` , con i seguenti parametri: • Nome: AwsEnaNetworkDriver • Versione: 2.2.3	26 ottobre 2021

Versione driver	Dettagli	Data di rilascio
2.2.3	Nuove funzionalità • Aggiunge il supporto per le nuove schede Nitro con reti di istanze fino a 400 Gbps. Correzioni di bug • Corregge la race condition tra la modifica dell'ora di sistema e la query sull'ora di sistema da parte del driver ENA, che causa il rilevamento di falsi positivi della mancata risposta dell'hardware. Annuncio Il driver Windows ENA versione 2.2.3 è la versione finale che supporta Windows Server 2008 R2. I tipi di istanza attualmente disponibili che utilizzano ENA continuer anno a essere supportati su Windows Server 2008 R2 e i driver sono disponibili per download. Nessun tipo di istanza futuro supporta Windows Server 2008 R2 e non è possibile avviare, importare o migrare immagini di Windows Server 2008 R2 a tipi di istanza futuri.	25 marzo 2021

Versione driver	Dettagli	Data di rilascio
2.2.2	Nuove funzionalità • Aggiunge il supporto per interrogare le metriche delle prestazioni degli adattatori di rete con CloudWatch e i contatori delle prestazioni per utenti Windows. Correzioni di bug • Risolve i problemi di prestazioni nelle istanze bare metal.	21 dicembre 2020
2.2.1	Nuove funzionalità • Aggiunge un metodo per consentire all'host di eseguire query sulla Elastic Network Adapter per le metriche delle prestazioni di rete.	1 ottobre 2020

Versione driver	Dettagli	Data di rilascio
2.2.0	Nuove funzionalità • Aggiunge il supporto per i tipi di hardware di nuova generazione. • Migliora il tempo di avvio dell'istanza dopo la ripresa dall'arresto correlato all'ibernazione ed elimina i messaggi di errore ENA falsi positivi. Ottimizzazione delle prestazioni • Ottimizza l'elaborazione del traffico in entrata. • Migliora la gestione della memoria condivisa in ambienti con risorse limitate. Correzioni di bug • Evita crash del sistema dopo la rimozione del dispositivo ENA in rari scenari in cui il driver non riesce a eseguire il reset.	12 agosto 2020
2.1.5	Correzioni di bug • Corregge errori di inizializzazione occasionali della scheda di rete nelle istanze Bare Metal.	23 giugno 2020

Versione driver	Dettagli	Data di rilascio
2.1.4	Correzioni di bug • Impedire problemi di connettività causati da metadati del pacchetto LSO danneggiato in arrivo dallo stack di rete. • Impedire l'arresto anomalo del sistema causato da una race condition rara che comporta l'accesso a memoria pacchetto già rilasciata.	25 novembre 2019
2.1.2	Nuove funzionalità • È stato aggiunto il supporto per il report sull'ID del fornitore per consentire al sistema operativo di generare UUID. MAC-based Correzioni di bug • Migliorate le prestazioni di configurazione di rete DHCP durante l'inizializzazione. • Checksum L4 calcolato correttamente sul traffico IPv6 in ingresso quando l'unità di trasmissione massima (MTU) supera 4K. • Miglioramenti generali alla stabilità del driver e correzioni di bug di minore entità.	4 novembre 2019

Versione driver	Dettagli	Data di rilascio
2.1.1	Correzioni di bug • Evita la perdita di pacchetti TCP LSO altamente frammentati provenienti dal sistema operativo. • Gestisce correttamente il protocollo Encapsulating Security Payload (ESP) all'interno dell'IPSec nelle reti IPv6.	16 settembre 2019

Versione driver	Dettagli	Data di rilascio

2.1.0	Il driver ENA Windows v2.1 introduce nuove capacità dei dispositivi ENA, offre ottimizzazione delle prestazioni, aggiunge nuove funzionalità e include molteplici miglioramenti alla stabilità.
	
	Nuove caratteristiche
	
	• Uso della chiave di registro Windows standardizzata per la configurazione dei frame Jumbo.
	• Consenti l'impostazione dell'ID VLAN tramite la GUI delle proprietà del driver ENA.
	• Flussi di ripristino migliorati
	  • Meccanismo di identificazione degli errori migliorato.
	  • Aggiunta del supporto per i parametri i ripristino regolabili.
	• Supporta fino a 32 I/O code per le istanze EC2 più recenti con più di 8 vCPU.
	• ~90% di riduzione del footprint di memoria dei driver.
	
	Ottimizzazione delle prestazioni
	
	• Latenza ridotta del percorso di trasmissione
	• Supporto per offload di checksum di ricezione.
	• Ottimizzazione delle prestazioni per sistemi a carico elevato (uso ottimizzato dei meccanismi di blocco).
	•
		1 luglio 2019

Versione driver	Dettagli	Data di rilascio
	Ulteriori miglioramenti per ridurre l'uso della CPU e potenziare la capacità di risposta del sistema sotto carico. Correzioni di bug • Correzione degli arresti anomali dovuti ad analisi non valida o intestazioni Tx non contigue. • Correzione degli arresti anomali del driver v1.5 durante lo scollegamento dall'interfaccia di rete elastica su istanze Bare Metal. • Correzione degli errori di calcolo di checksum delle pseudo-intestazioni LSO su IPv6. • Correzione della potenziale perdita di risorse di memoria in fase di errore di inizializzazione. • Disabilita l'offload del checksum per i frammenti IPv4. TCP/UDP • Correzione della configurazione VLAN. La rete VLAN è stata disabilitata per errore laddove avrebbe dovuto essere disabilitata solo la priorità VLAN. • Abilitazione della corretta analisi dei messaggi del driver personalizzato da parte del visualizzatore eventi. • Correzione degli errori di inizializzazione del driver per una gestione non valida del timestamp. • Correzione della race condition tra l'elaborazione dei dati e la disabilitazione dei dispositivi ENA.	

Versione driver	Dettagli	Data di rilascio
1.5.0	Aggiornamenti • Maggiore stabilità e correzioni relative alle prestazioni. • I buffer di ricezione possono ora essere configurati fino a un valore di 8192 in Proprietà avanzate del NIC ENA. • Buffer di ricezione predefinito di 1k.	4 ottobre 2018
1.2.3	Include le correzioni relative all'affidabilità e unifica il supporto per Windows Server 2008 R2 mediante Windows Server 2016.	13 febbraio 2018
1.0.8	Versione iniziale. Incluso nelle AMI per Windows Server 2008 R2, Windows Server 2012 RTM, Windows Server 2012 R2 e Windows Server 2016.	2016 luglio

Iscriviti alle notifiche di rilascio dei driver ENA Windows da Amazon SNS

Amazon SNS può avvisarti in caso di pubblicazione di nuove versioni dei driver Windows di EC2. Utilizza la procedura seguente per effettuare l'iscrizione a queste notifiche.

Iscriviti alle notifiche EC2

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. È necessario selezionare questa regione perché le notifiche SNS per le quali stai effettuando la sottoscrizione si trovano in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
4. Scegli Crea sottoscrizione.
5. Nella finestra di dialogo Create subscription (Crea sottoscrizione) segui questi passaggi:

    a. In Topic ARN (ARN argomento) copia il seguente nome della risorsa Amazon (ARN):

arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers

b. In Protocol (Protocollo), scegli `Email`.

c. Per Endpoint, inserisci un indirizzo e-mail a cui desideri che vengano inviate le notifiche.

d. Scegli Create Subscription (Crea sottoscrizione).

6. Riceverai a breve un'e-mail di conferma. Apri l'e-mail e segui le istruzioni per completare l'iscrizione.

Quando i nuovi driver Windows di EC2 vengono rilasciati, inviamo notifiche ai sottoscrittori. Se non desideri più ricevere queste notifiche, segui la procedura seguente per annullare la sottoscrizione.

Annullamento della sottoscrizione alle notifiche del driver Windows per Amazon EC2

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
3. Seleziona la casella di spunta della sottoscrizione, quindi scegli Actions (Operazioni), Delete subscriptions (Cancella sottoscrizioni). Quando viene richiesta la conferma, seleziona Elimina.

Driver paravirtuali per le istanze Windows

Le AMI Windows contengono un insieme di driver per consentire l'accesso all'hardware virtualizzato. Tali driver vengono utilizzati da Amazon EC2 per mappare instance store e volumi Amazon EBS ai rispettivi dispositivi. Nella tabella seguente vengono illustrate le differenze principali tra i diversi driver.

	Red Hat PV	Citrix PV	AWS PV
Tipo di istanza	Non supportato per tutti i tipi di istanza. Se specifichi un tipo di istanza non supportato, l'istanza sarà danneggiata.	Supportato per i tipi di istanza Xen.	Supportato per i tipi di istanza Xen.
Volumi collegati	Supporta fino a 16 volumi collegati.	Supporta più di 16 volumi collegati.	Supporta più di 16 volumi collegati.

	Red Hat PV	Citrix PV	AWS PV
Rete	Il driver presenta problemi noti durante i quali la connessione di rete si ristabilisce con carichi elevati, ad esempio in caso di trasferimenti di file FTP rapidi.		Il driver configura automaticamente i frame jumbo sulla scheda di rete quando si trova su un tipo di istanza compatibile. Quando l'istanza si trova in un gruppo di posizionamento cluster, ciò offre migliori prestazioni di rete tra le istanze che sono in tale gruppo. Per ulteriori informazioni, consulta Gruppi di collocamento per le tue istanze Amazon EC2.

La tabella seguente riporta i driver PV da eseguire su ciascuna versione di Windows Server su Amazon EC2.

Versione di Windows Server	Versione driver PV
Windows Server 2025	Non supportata
Windows Server 2022	AWS Ultima versione di PV
Windows Server 2019	AWS Ultima versione di PV
Windows Server 2016	AWS Ultima versione di PV
Windows Server 2012 R2	AWS PV versione 8.4.3
Windows Server 2012	AWS PV versione 8.4.3
Windows Server 2008 R2	AWS PV versione 8.3.5
Windows Server 2008	Citrix PV 5.9
Windows Server 2003	Citrix PV 5.9

Indice

- AWS Driver PV
- Driver Citrix PV
- Driver Red Hat PV
- Sottoscrizione alle notifiche di
- Aggiornamento dei driver PV sulle istanze Windows EC2
- Risoluzione dei problemi relativi ai driver PV sulle istanze Windows

AWS Driver PV

I driver AWS PV sono memorizzati nella directory. `%ProgramFiles%\Amazon\Xentools` Questa directory contiene anche simboli pubblici e uno strumento a riga di comando che consente di accedere alle voci in XenStore. `xenstore_client.exe` Ad esempio, il PowerShell comando seguente restituisce l'ora corrente dall'Hypervisor:

```
PS C:\> [DateTime]::FromFileTimeUTC((gwmi -n root\wmi -cl
 AWSXenStoreBase).XenTime).ToString("hh:mm:ss")
11:17:00
```

I componenti del driver AWS PV sono elencati nel registro di Windows in. `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services` Tali componenti sono i seguenti: xenbus, xeniface, xennet, xenvbd e xenvif.

AWS I driver PV hanno anche un servizio Windows denominato LiteAgent, che viene eseguito in modalità utente. Gestisce attività come gli eventi di spegnimento e riavvio dalle AWS API sulle istanze di generazione Xen. Puoi accedere ai servizi e gestirli eseguendo `Services.msc` dalla riga di comando. Quando si esegue su istanze di generazione Nitro, i driver AWS PV non vengono utilizzati e il LiteAgent servizio si interromperà automaticamente a partire dalla versione 8.2.4 del driver. L'aggiornamento al driver AWS PV più recente consente inoltre di aggiornare LiteAgent e migliorare l'affidabilità su tutte le generazioni di istanze.

Installa la versione più recente AWS Driver PV

Le AMI Windows di Amazon contengono un insieme di driver per consentire l'accesso all'hardware virtualizzato. Tali driver vengono utilizzati da Amazon EC2 per mappare instance store e volumi Amazon EBS ai rispettivi dispositivi. Ti consigliamo di installare i driver più recenti per migliorare la stabilità e le prestazioni delle istanze Windows di EC2.

Opzioni di installazione

- AWS Systems Manager Usalo per aggiornare automaticamente i driver fotovoltaici. Per ulteriori informazioni, consulta Walkthrough: Automatically Update PV Drivers on EC2 Windows Instances nella Guida per l'utente di AWS Systems Manager .
- Scarica il pacchetto driver ed esegui il programma di installazione manualmente. Per informazioni sul download e sull'installazione di driver AWS PV, o sull'aggiornamento di un controller di dominio, consulta Aggiornare le istanze di Windows Server (AWS PV (aggiornamento) manualmente.

Per i requisiti di sistema per l'installazione del pacchetto driver AWS PV, vedere. Requisiti di sistema per AWS Pacchetto driver fotovoltaici

AWS Cronologia dei pacchetti driver PV

La tabella seguente mostra le modifiche ai driver AWS PV per ciascuna versione di driver.

Versione del pacchetto	Dettagli	Data di rilascio
8.6.1 8.6.1 8.6.1	• Dipendenze di runtime aggiornate nel pacchetto di installaz ione.	21 luglio 2026
8.6.0	• Correzioni di stabilità alle interazioni. XenStore	27 maggio 2025
8.5.0	• Correzioni di stabilità per risolvere rari casi di arresto anomalo durante lo scollegamento del dispositivo di rete. • Correzioni di stabilità per risolvere rari casi di arresto anomalo durante lo scollegamento del volume EBS. • Sono stati corretti i bug nel programma di installazione del pacchetto. • È stato aggiornato il programma di installazione PV per utilizzare `Pnputil`.	31 ottobre 2024
8.4.3	Sono stati corretti i bug nel programma di installazione del pacchetto per migliorare l'esperienza di aggiornamento. Questa è l'ultima versione che può essere eseguita su Windows Server 2012 e 2012 R2. Questa versione è disponibile per il download, ma non è più supportata poiché Windows Server 2012 e 2012 R2 hanno raggiunto la fine del supporto.	24 gennaio 2023
8.4.2	Correzioni di stabilità per affrontare le race condition.	13 aprile 2022
8.4.1	Installer di pacchetti migliorato.	7 gennaio 2022
8.4.0	• Correzioni di stabilità per risolvere rari casi di I/O del disco bloccato. • Correzioni di stabilità per risolvere rari casi di arresto anomalo durante lo scollegamento del volume EBS. • Aggiunta funzionalità per distribuire il carico su più core per carichi di lavoro che sfruttano più di 20.000 IOPS e subiscono	2 marzo 2021

Versione del pacchetto	Dettagli	Data di rilascio
	una riduzione delle prestazioni dovuta a colli di bottiglia. Per abilitare questa funzionalità, consulta I carichi di lavoro che utilizzano più di 20.000 IOPS su disco subiscono una riduzione delle prestazioni dovuta ai colli di bottiglia della CPU.	
8.3.5	Installer di pacchetti migliorato. Questa è l'ultima versione che può essere eseguita su Windows Server 2008 R2. Questa versione è disponibile per il download ma non è più supportata. Windows Server 2008 R2 ha raggiunto la fine del suo ciclo di vita e non è più supportato da Microsoft.	7 gennaio 2022
8.3.4	Maggiore affidabilità del collegamento del dispositivo di rete.	4 agosto 2020
8.3.3	• Aggiornamento del XenStore-facing componente per impedire il controllo dei bug durante i percorsi di gestione degli errori. • Aggiornamento al componente di archiviazione per evitare arresti anomali quando viene inviato un SRB non valido. Per aggiornare questo driver nelle istanze di Windows Server 2008 R2, è necessario innanzitutto verificare che siano installate le patch appropriate per risolvere il seguente avviso di sicurezza Microsoft: Security Advisory 3033929.	4 febbraio 2020
8.3.2	Maggiore affidabilità dei componenti di rete.	30 luglio 2019
8.3.1	Miglioramenti delle prestazioni e della solidità ai componenti di archiviazione.	12 giugno 2019
8.2.7	Maggiore efficienza per supportare la migrazione ai tipi di istanza di generazione più recente.	20 maggio 2019

Versione del pacchetto	Dettagli	Data di rilascio
8.2.6	Maggiore efficienza di un percorso di chiusura inaspettata.	15 gennaio 2019
8.2.5	Altri miglioramenti di sicurezza PowerShell il programma di installazione è ora disponibile nel pacchetto.	12 dicembre 2018
8.2.4	Migliorie in termini di affidabilità.	2 ottobre 2018
8.2.3	Correzioni di bug e miglioramenti delle prestazioni. Segnalare un ID di volume EBS come numero di serie per i volumi EBS. Questo abilita gli scenari cluster come S2D.	29 maggio 2018
8.2.1	Miglioramenti delle prestazioni di rete e di archiviazione oltre a varie correzioni della solidità. Per verificare che la versione sia stata installata, fai riferimento al seguente valore di registro di Windows: `HKLM\Software\Amazon\PVDriver\Version 8.2.1` .	8 marzo 2018
7.4.3	Aggiunta di supporto per Windows Server 2016. Correzioni della stabilità per tutte le versioni del sistema operativo Windows supportate. *AWS La firma del driver PV versione 7.4.3 scade il 29 marzo 2019. Si consiglia di eseguire l'aggiornamento al driver PV più recente AWS .	18 novembre 2016
7.4.2	Correzioni della stabilità per il supporto del tipo di istanza X1.	2 agosto 2016

Versione del pacchetto	Dettagli	Data di rilascio
7.4.1	• Miglioramento delle prestazioni del driver AWS PV Storage. • Correzioni alla stabilità nel driver AWS PV Storage: è stato risolto un problema a causa del quale le istanze si bloccavano con il codice di controllo del bug 0x0000DEAD. • Correzioni di stabilità nel driver PV Network. AWS • Aggiunta di supporto per Windows Server 2008R2.	12 luglio 2016
7.3.2	• Miglioramento di registrazione e diagnostica. • Correzione della stabilità nel driver AWS PV Storage. In alcuni casi i dischi potrebbero non comparire in Windows dopo aver ricollegato il disco all'istanza. • Aggiunta di supporto per Windows Server 2012.	24 giugno 2015
7.3.1	Aggiornamento TRIM: correzione associata a richieste TRIM. Tale correzione stabilizza le istanze e ne migliora le prestazioni in caso di gestione di una grande quantità di richieste TRIM.	
7.3.0	Supporto TRIM: il driver AWS PV ora invia le richieste TRIM all'hypervisor. I dischi temporanei elaborano correttamente le richieste TRIM dal momento che l'archiviazione sottostante supporta TRIM (SSD). Tieni presente che EBS-based lo storage non supporta TRIM a partire da marzo 2015.	
7.2.5	• Correzione della stabilità nei driver AWS PV Storage: in alcuni casi il driver AWS PV potrebbe dereferenziare una memoria non valida e causare un errore di sistema. • Correzione della stabilità durante la generazione di un crash dump: in alcuni casi il pilota AWS PV potrebbe rimanere bloccato in condizioni di gara durante la stesura di un crash dump. Prima di questa versione, il problema poteva essere risolto esclusivamente forzando l'arresto del driver e riavviand olo al fine di perdere il dump della memoria.	

Versione del pacchetto	Dettagli	Data di rilascio
7.2.4	Persistenza dell'ID del dispositivo: questa correzione del driver maschera l'ID del dispositivo PCI della piattaforma e obbliga il sistema a mostrare sempre lo stesso ID del dispositivo, anche quando l'istanza viene spostata. Più generalmente, la correzion e influisce sul modo in cui l'hypervisor mostra i dispositivi virtuali. La correzione include anche modifiche al coinstallatore per i driver AWS fotovoltaici in modo che il sistema mantenga i dispositivi virtuali mappati.	
7.2.2	• Caricare i driver AWS PV in modalità Directory Services Restore Mode (DSRM): Directory Services Restore Mode è un'opzione di avvio in modalità sicura per i controller di dominio Windows Server. • Persistenza dell'ID del dispositivo quando la scheda di rete virtuale viene ricollegata: la correzione forza il sistema a controllare la mappatura dell'indirizzo MAC e mantenere l'ID del dispositivo. Questa correzione assicura che le schede mantengano le loro impostazioni statiche se ricollegate.	
7.2.1	• Esecuzione in modalità sicura: risoluzione di un problema che impediva il caricamento del driver in modalità sicura. In precedenza, i driver AWS PV venivano creati un'istanza solo nei normali sistemi in esecuzione. • Aggiunta di dischi ai pool di archiviazione di Microsoft Windows: in precedenza sintetizzavamo le richieste di pagina 83. Questa correzione ha disabilitato il supporto di pagina 83. Ciò non interessa i pool di archiviazione utilizzati in un ambiente di cluster perché i dischi PV non sono dischi di cluster validi.	
7.2.0	Base: la versione base AWS PV.	

Driver Citrix PV

I driver Citrix PV sono archiviati nella directory `%ProgramFiles%\Citrix\XenTools` (istanze a 32 bit) o `%ProgramFiles(x86)%\Citrix\XenTools` (istanze a 64 bit).

I componenti del driver Citrix PV sono elencati nel registro di Windows in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services`. Tali componenti sono i seguenti: xenevtchn, xeniface, xennet, Xennet6, xensvc, xenvbd e xenvif.

Citrix ha anche un componente driver denominato XenGuestAgent, che viene eseguito come servizio Windows. Gestisce attività come l'arresto e il riavvio di eventi dell'API. Puoi accedere ai servizi e gestirli eseguendo `Services.msc` dalla riga di comando.

Se riscontri errori di rete durante l'esecuzione di determinati carichi di lavoro, potresti aver bisogno di disabilitare la caratteristica di offload TCP per il driver Citrix PV. Per ulteriori informazioni, consulta Offload TCP.

Driver Red Hat PV

I driver Red Hat sono supportati per le istanze legacy, ma non sono raccomandati con istanze più recenti con più di 12 GB di RAM a causa delle loro limitazioni. Le istanze con più di 12 GB di RAM che eseguono driver Red Hat possono riscontrare problemi di avvio e diventare inaccessibili. Consigliamo di aggiornare i driver Red Hat ai driver Citrix PV, quindi di aggiornare i driver Citrix PV ai driver PV. AWS

I file di origine per i driver Red Hat sono archiviati nella directory `%ProgramFiles%\RedHat` (istanze a 32 bit) o `%ProgramFiles(x86)%\RedHat` (istanze a 64 bit). I due driver sono `rhelnet` (il driver di rete Red Hat Paravirtualized) e `rhelscsi` (i driver miniport Red Hat SCSI).

Sottoscrizione alle notifiche di

Amazon SNS può avvisarti in caso di pubblicazione di nuove versioni dei driver Windows di EC2. Puoi abbonarti per ricevere queste notifiche.

> **Note**
>
> Devi specificare la regione in cui è stato creato l'argomento SNS.

Quando i nuovi driver Windows di EC2 vengono rilasciati, inviamo notifiche ai sottoscrittori. Se non desideri più ricevere queste notifiche, puoi annullare l'abbonamento. Per ulteriori informazioni, consulta Delete an SNS topic and subscription.

Console

Per iscriversi alle notifiche di

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. È necessario selezionare questa regione perché le notifiche SNS per le quali stai effettuando la sottoscrizione si trovano in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
4. Scegli Crea sottoscrizione.
5. Nella finestra di dialogo Create subscription (Crea sottoscrizione) segui questi passaggi:
   a. In Topic ARN (ARN argomento) copia il seguente nome della risorsa Amazon (ARN):

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. In Protocol (Protocollo), scegli `Email`.
   c. In Endpoint digita l'indirizzo e-mail utilizzabile per ricevere le notifiche.
   d. Scegli Create Subscription (Crea sottoscrizione).
6. Riceverai a breve un'e-mail di conferma. Apri l'e-mail e segui le istruzioni per completare l'iscrizione.

AWS CLI

Per iscriversi alle notifiche di

Utilizza il seguente comando.

```
aws sns subscribe \
    --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers \
    --region us-east-1 \
    --protocol email \
    --notification-endpoint YourUserName@YourDomainName.ext
```

PowerShell

Per iscriversi alle notifiche di

Utilizza il seguente comando.

```
Connect-SNSNotification `
    -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers' `
    -Region us-east-1 `
    -Protocol email `
    -Endpoint "YourUserName@YourDomainName.ext"
```

Aggiornamento dei driver PV sulle istanze Windows EC2

Ti consigliamo di installare i driver PV più recenti per migliorare la stabilità e le prestazioni delle istanze Windows di EC2. Le istruzioni riportate in questa pagina consentono di scaricare il pacchetto di driver ed eseguire il programma di installazione.

Per verificare quale driver viene utilizzato dall'istanza Windows

Apri Gestore dispositivi e visualizza Adattatori di rete. Verifica che il driver PV sia uno dei seguenti:

- AWS Dispositivo di rete PV
- Scheda Ethernet Citrix PV
- Driver Red Hat PV NIC

Indice

- Requisiti di sistema per AWS Pacchetto driver fotovoltaici
- Aggiornare le istanze di Windows Server (AWS PV (aggiornamento) con Distributor
- Aggiornare le istanze di Windows Server (AWS PV (aggiornamento) manualmente
- Aggiornare un controller di dominio (AWS Aggiornamento PV)
- Aggiornamento delle istanze Windows Server 2008 e 2008 R2 (aggiornamento da Red Hat a Citrix PV)
- Aggiornamento del servizio di agente guest Citrix Xen

Requisiti di sistema per AWS Pacchetto driver fotovoltaici

I seguenti requisiti si applicano al pacchetto driver AWS PV, indipendentemente dal fatto che venga installato tramite Systems Manager o manualmente.

- Una versione di Windows Server supportata dalla versione del pacchetto. Le versioni precedenti di Windows Server richiedono una versione precedente del pacchetto. Per la versione del pacchetto da utilizzare con il sistema operativo, consultaDriver paravirtuali per le istanze Windows.
- La versione minima di .NET Framework richiesta dal programma di installazione del pacchetto, come illustrato nella tabella seguente.

AWS Versione del pacchetto driver PV	Versione minima di.NET Framework
Più recente	4.7.2
8.4.3	4.5
8.3.5	4.5

Aggiornare le istanze di Windows Server (AWS PV (aggiornamento) con Distributor

È possibile utilizzare Distributor, una funzionalità di AWS Systems Manager, per installare o aggiornare il pacchetto di driver AWS fotovoltaici. L'installazione o l'aggiornamento possono essere eseguiti una sola volta oppure è possibile installarli o aggiornarli in base a una pianificazione. L'opzione `In-place update` per Tipo di installazione non è supportata per questo pacchetto Distributor.

> **Important**
>
> Se l'istanza è un controller di dominio, consulta Aggiornare un controller di dominio (AWS Aggiornamento PV). Il processo di aggiornamento per le istanze dei controller del dominio è diverso rispetto alle edizioni standard di Windows.

1. Si consiglia di creare un backup nel caso in cui sia necessario eseguire il rollback delle modifiche.

> **Tip**
>
> Invece di creare l'AMI dalla console Amazon EC2, puoi anche utilizzare Systems Manager Automation per creare l'AMI utilizzando il runbook `AWS-CreateImage`. Per ulteriori informazioni, consulta AWS-CreateImage nella Guida per l'utente di riferimento del runbook di automazione AWS Systems Manager .

   a. Quando interrompi un'istanza, i dati presenti sui volumi dell'archivio dell'istanza vengono cancellati. Prima di arrestare un'istanza, verificare di aver copiato tutti i dati necessari dai volumi di instance store nello storage persistente, ad esempio Amazon EBS o Amazon S3.
   b. Nel riquadro di navigazione, scegliere Instances (Istanze).
   c. Selezionare l'istanza che richiede l'aggiornamento del driver e scegliere Instance state (Stato istanza), Stop instance (Arresta istanza).
   d. Dopo avere interrotto l'istanza, selezionare l'istanza, scegliere Actions (Operazioni), Image and templates (Immagine e modelli), quindi scegliere Create image (Crea immagine).
   e. Scegli Instance state (Stato istanza), Start instance (Avvia istanza).
2. Collegati all'istanza tramite un'applicazione desktop remoto. Per ulteriori informazioni, consulta the section called "Connettiti utilizzando un client RDP".
3. Prima di eseguire questo aggiornamento, consigliamo di portare offline tutti i dischi non di sistema e di annotare le mappature delle lettere di unità ai dischi secondari in Disk Management (Gestione disco). Questo passaggio non è necessario se si esegue un aggiornamento sul posto dei AWS driver fotovoltaici. Consigliamo inoltre di impostare i servizi non essenziale sull'avvio Manual (Manuale) nella console Services.
4. Per le istruzioni su come installare o aggiornare il pacchetto di driver AWS FV utilizzando Distributor, consulta le procedure in Installazione o aggiornamento dei pacchetti nella Guida per l'utente. AWS Systems Manager
5. Per Nome, scegli AWSPVDriver.
6. In Tipo di installazione, scegli Disinstalla e reinstalla.
7. Configura gli altri parametri per il pacchetto secondo necessità ed esegui l'installazione o l'aggiornamento utilizzando la procedura di riferimento in. Step 4

   Dopo aver eseguito il pacchetto Distributor, l'istanza si riavvia automaticamente e quindi aggiorna il driver. L'istanza non sarà disponibile per un massimo di 15 minuti.

8. Una volta completato l'aggiornamento e dopo che l'istanza ha superato entrambi i controlli dell'integrità nella console Amazon EC2, verifica che il nuovo driver sia stato installato connettendoti all'istanza usando Desktop remoto.
9. Una volta effettuata la connessione, eseguite il comando seguente: PowerShell

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

10. Verifica che la versione del driver sia la stessa dell'ultima versione elencata nella tabella della cronologia delle versioni dei driver. Per ulteriori informazioni, consulta AWS Cronologia dei pacchetti driver PV Apri Gestione disco per esaminare i volumi secondari offline e portarli online in base alle lettere di unità annotate nella Step 3.

Se in precedenza avete disabilitato Offload TCP l'utilizzo di Netsh per i driver PV Citrix, vi consigliamo di riattivare questa funzione dopo l'aggiornamento ai driver PV. AWS I problemi di TCP Offloading con i driver Citrix non sono presenti nei driver PV. AWS Di conseguenza, TCP Offloading offre prestazioni migliori con i driver PV. AWS

Se in precedenza avete applicato un indirizzo IP statico o una configurazione DNS all'interfaccia di rete, potrebbe essere necessario riapplicare l'indirizzo IP statico o la configurazione DNS dopo aver aggiornato i driver PV. AWS

Aggiornare le istanze di Windows Server (AWS PV (aggiornamento) manualmente

Utilizzate la seguente procedura per eseguire un aggiornamento sul posto dei driver AWS PV o per eseguire l'aggiornamento dai driver Citrix PV ai driver AWS PV su Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 o Windows Server 2022. Questo aggiornamento non è disponibile per i driver Red Hat o per altre versioni di Windows Server.

> **Important**
>
> Se l'istanza è un controller di dominio, consulta Aggiornare un controller di dominio (AWS Aggiornamento PV). Il processo di aggiornamento per le istanze dei controller del dominio è diverso rispetto alle edizioni standard di Windows.

Per eseguire l'aggiornamento AWS Driver fotovoltaici manualmente

1. Si consiglia di creare un backup nel caso in cui sia necessario eseguire il rollback delle modifiche.

   > **Tip**
   >
   > Invece di creare l'AMI dalla console Amazon EC2, puoi anche utilizzare Systems Manager Automation per creare l'AMI utilizzando il runbook `AWS-CreateImage`. Per ulteriori informazioni, consulta AWS-CreateImage nella Guida per l'utente di riferimento del runbook di automazione AWS Systems Manager .

   a. Quando interrompi un'istanza, i dati presenti sui volumi dell'archivio dell'istanza vengono cancellati. Prima di arrestare un'istanza, verificare di aver copiato tutti i dati necessari dai volumi di instance store nello storage persistente, ad esempio Amazon EBS o Amazon S3.
   b. Nel riquadro di navigazione, scegliere Instances (Istanze).
   c. Selezionare l'istanza che richiede l'aggiornamento del driver e scegliere Instance state (Stato istanza), Stop instance (Arresta istanza).
   d. Dopo avere interrotto l'istanza, selezionare l'istanza, scegliere Actions (Operazioni), Image and templates (Immagine e modelli), quindi scegliere Create image (Crea immagine).
   e. Scegli Instance state (Stato istanza), Start instance (Avvia istanza).
2. Collegati all'istanza tramite un'applicazione desktop remoto.
3. Prima di eseguire questo aggiornamento, consigliamo di portare offline tutti i dischi non di sistema e di annotare le mappature delle lettere di unità ai dischi secondari in Disk Management (Gestione disco). Questo passaggio non è necessario se si esegue un aggiornamento sul posto dei AWS driver fotovoltaici. Consigliamo inoltre di impostare i servizi non essenziale sull'avvio Manual (Manuale) nella console Services.
4. Scarica i driver sull'istanza utilizzando una delle seguenti opzioni:
   - Browser: scarica il pacchetto di driver più recente per l'istanza ed estrai l'archivio zip.
   - PowerShell— Esegui i seguenti comandi:

     ```
     Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/Latest/AWSPVDriver.zip -outfile $env:USERPROFILE\pv_driver.zip
     Expand-Archive $env:userprofile\pv_driver.zip -DestinationPath $env:userprofile\pv_drivers
     ```

Se si riceve un errore durante il download del file e si utilizza Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il PowerShell terminale. Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il comando seguente e riprovare:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

5. Esegui `AWSPVDriverSetup.msi`.

Dopo aver eseguito l'MSI, l'istanza si riavvia automaticamente e quindi aggiorna il driver. L'istanza non sarà disponibile per un massimo di 15 minuti. Una volta completato l'aggiornamento e dopo che l'istanza ha superato entrambi i controlli di integrità nella console Amazon EC2, puoi verificare che il nuovo driver sia stato installato connettendoti all'istanza tramite Remote Desktop ed eseguendo il seguente PowerShell comando:

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

Verifica che la versione del driver sia la stessa dell'ultima versione elencata nella tabella della cronologia delle versioni dei driver. Per ulteriori informazioni, consulta AWS Cronologia dei pacchetti driver PV Apri Gestione disco per esaminare i volumi secondari offline e portarli online in base alle lettere di unità annotate nella Step 3.

Se in precedenza hai disabilitato Offload TCP l'utilizzo dei driver Netsh for Citrix PV, ti consigliamo di riattivare questa funzionalità dopo l'aggiornamento ai driver PV. AWS I problemi di TCP Offloading con i driver Citrix non sono presenti nei driver PV. AWS Di conseguenza, TCP Offloading offre prestazioni migliori con i driver PV. AWS

Se in precedenza avete applicato un indirizzo IP statico o una configurazione DNS all'interfaccia di rete, potrebbe essere necessario riapplicare l'indirizzo IP statico o la configurazione DNS dopo aver aggiornato i driver PV. AWS

Aggiornare un controller di dominio (AWS Aggiornamento PV)

Utilizzate la seguente procedura su un controller di dominio per eseguire un aggiornamento sul posto dei driver AWS PV o per eseguire l'aggiornamento dai driver Citrix PV ai driver PV. AWS Per garantire che i ruoli FSMO restino operativi durante l'aggiornamento, consigliamo di trasferirli ad altri controller di dominio prima di iniziare l'aggiornamento. Per ulteriori informazioni, consulta Come visualizzare e trasferire i ruoli FSMO sul sito Web Microsoft Learn.

Per aggiornare un controller di dominio

1. Si consiglia di creare un backup del controller di dominio nel caso in cui sia necessario eseguire il rollback delle modifiche. L'utilizzo di un'AMI come backup non è supportato. Per ulteriori informazioni, consulta Backup and restore considerations nella documentazione di Microsoft.
2. Esegui il comando seguente per configurare Windows per l'avvio in Directory Services Restore Mode (DSRM).

   > **Warning**
   >
   > Prima di eseguire questo comando, confermare di conoscere la password DSRM. Tale informazione è richiesta per accedere all'istanza quando l'aggiornamento è completo e l'istanza si riavvia automaticamente.

   ```
   bcdedit /set {default} safeboot dsrepair
   ```

   PowerShell:

   ```
   PS C:\> bcdedit /set "{default}" safeboot dsrepair
   ```

   Il sistema deve essere avviato in DSRM perché l'utilità di aggiornamento rimuove i driver di storage Citrix PV in modo da poter installare i driver PV. AWS Pertanto, consigliamo di annotare le mappature delle lettere di unità e delle cartelle ai dischi secondari in Disk Management (Gestione disco). Quando i driver di archiviazione Citrix PV non sono presenti, le unità secondarie non vengono rilevate. I controller di dominio che utilizzano una cartella NTDS su unità secondarie non si avviano perché il disco secondario non sarà rilevato.

   > **Warning**
   >
   > Una volta eseguito il comando, non riavviare manualmente il sistema. Il sistema risulterà irraggiungibile perché i driver Citrix PV non supportano DSRM.

3. Eseguire il seguente comando per aggiungere **`DisableDCCheck`** al registro:

   ```
   reg add HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck /t
    REG_SZ /d true
   ```

4. Scarica il pacchetto di driver più recente per l'istanza ed estrai l'archivio zip.
5. Esegui `AWSPVDriverSetup.msi`.

   Dopo aver eseguito l'MSI, l'istanza si riavvia automaticamente e quindi aggiorna il driver. L'istanza non sarà disponibile per un massimo di 15 minuti.
6. Una volta completato l'aggiornamento e dopo che l'istanza ha superato entrambi i controlli dello stato nella console Amazon EC2, connettersi all'istanza utilizzando Desktop remoto. Apri Disk Management (Gestione disco) per esaminare i volumi secondari offline e portarli online in base alle mappature delle lettere di unità e delle cartelle annotate in precedenza.

   È necessario connettersi all'istanza specificando il nome utente nel seguente formato hostname\administrator. Ad esempio,\ administrator. Win2k12TestBox
7. Eseguire il comando riportato di seguito per rimuovere la configurazione di avvio DSRM:

   ```
   bcdedit /deletevalue safeboot
   ```
8. Riavviare l'istanza.
9. Per completare il processo di aggiornamento, verificare che il nuovo driver sia istallato. In Gestione dispositivi, in Storage Controllers (Controller di archiviazione), individuare PV Storage Host Adapter (Adattatore host archiviazione PV)AWS Verifica che la versione del driver sia la stessa dell'ultima versione elencata nella tabella della cronologia delle versioni dei driver. Per ulteriori informazioni, consulta AWS Cronologia dei pacchetti driver PV.
10. Eseguire il seguente comando per eliminare **`DisableDCCheck`** dal registro:

    ```
    reg delete HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck
    ```

> **Note**
>
> Se in precedenza avete disabilitato Offload TCP l'utilizzo di Netsh for Citrix PV drivers, vi consigliamo di riattivare questa funzione dopo l'aggiornamento a PV Drivers. AWS I problemi di TCP Offloading con i driver Citrix non sono presenti nei driver PV. AWS Di conseguenza, TCP Offloading offre prestazioni migliori con i driver PV. AWS

Aggiornamento delle istanze Windows Server 2008 e 2008 R2 (aggiornamento da Red Hat a Citrix PV)

Prima di iniziare ad aggiornare i driver Red Hat in driver Citrix PV, assicurati di completare quanto segue:

- Installare la versione più recente del servizio EC2Config. Per ulteriori informazioni, consulta Installazione della versione più recente di EC2Config.
- Verifica di avere installato Windows PowerShell 3.0. Per verificare la versione installata, esegui il comando seguente in una PowerShell finestra:

  ```
  PS C:\> $PSVersionTable.PSVersion
  ```

  Windows PowerShell 3.0 è incluso nel pacchetto di installazione di Windows Management Framework (WMF) versione 3.0. Se è necessario installare Windows PowerShell 3.0, vedere Windows Management Framework 3.0 nel Microsoft Download Center.
- Esegui il backup delle informazioni importanti dell'istanza o crea un'AMI dall'istanza. Per ulteriori informazioni sulla creazione di un'AMI, consulta Crea un' EBS-backed AMI Amazon.

  > **Tip**
  >
  > Invece di creare l'AMI dalla console Amazon EC2, puoi anche utilizzare Systems Manager Automation per creare l'AMI utilizzando il runbook `AWS-CreateImage`. Per ulteriori informazioni, consulta AWS-CreateImage nella Guida per l'utente di riferimento del runbook di automazione AWS Systems Manager .

  Se crei un'AMI, assicurati di completare quanto segue:

  - Prendi nota della tua password.
  - Non eseguire lo strumento Sysprep o utilizzare il servizio EC2Config.
  - Imposta la scheda Ethernet in modo da ottenere automaticamente un indirizzo IP utilizzando DHCP.

Per aggiornare i driver Red Hat

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale. Per ulteriori informazioni sulla connessione all'istanza, consulta Connessione all'istanza Windows con il protocollo RDP.
2. Nell'istanza, scaricare il pacchetto di aggiornamento Citrix PV.
3. Estrarre il contenuto del pacchetto di aggiornamento in una ubicazione a scelta.
4. Apri il file Upgrade.bat. In caso di avviso di sicurezza, scegliere Run (Esegui).
5. Nella finestra di dialogo Upgrade Drivers (Aggiorna driver), rivedere le informazioni e scegliere Yes (Sì) se si è pronti ad avviare l'aggiornamento.
6. Nella finestra di dialogo Driver Xen Red Hat paravirtualizzati per il programma di disinstallazione di Windows, scegli Sì per rimuovere il software Red Hat. L'istanza sarà riavviata.

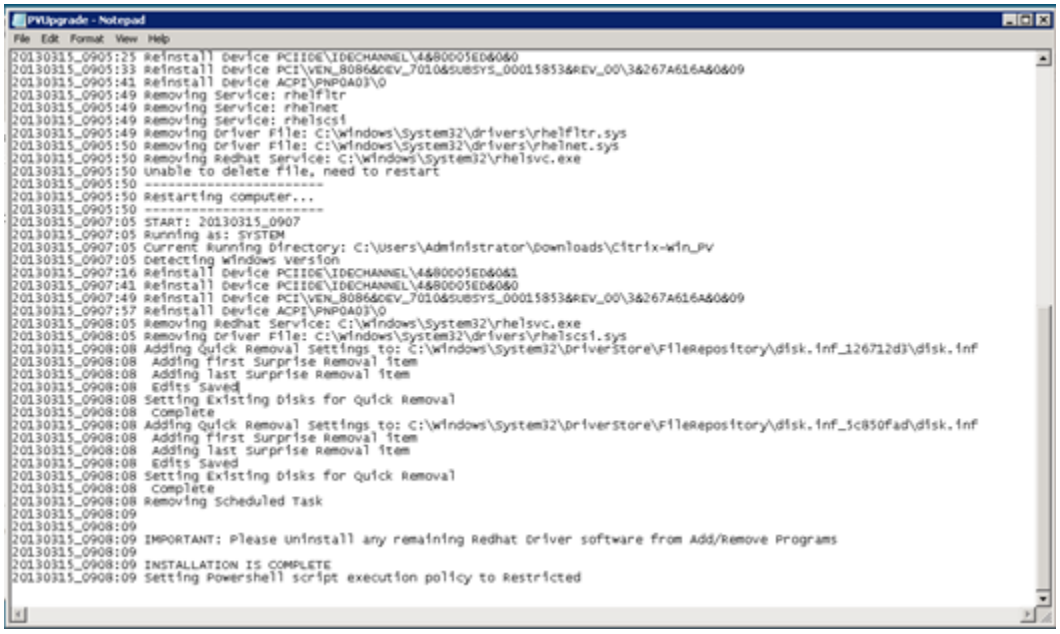
> **Note**
>
> Se non si visualizza la finestra di dialogo del programma di disinstallazione, scegliere Red Hat Paravirtualize nella barra delle applicazioni di Windows.



7. Controllare che l'istanza si sia riavviata che sia pronta all'uso.
   a. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
   b. Nella pagina Instances (Istanze) selezionare Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), quindi scegliere Get system log (Ottieni registro di sistema).
   c. Le operazioni di aggiornamento dovrebbero aver riavviato il server 3 o 4 volte. È possibile verificarlo nel file di log in base al numero di volte in cui viene visualizzato `Windows is Ready to use`.

```
    Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
 Ec2Config service v2.1.9.0
  RedHat PV NIC Driver v1.3.10.0
2013/03/15 17:11:01Z: Waiting for meta-data accessibility...
2013/03/15 17:11:02Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BFD64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
<Username>Administrator</Username>
<Password>
L79ThJPF8LyIL38IZht0FBrjet3vnT2csTiU/XGVMRCH7kQtBnznAnXrKd1sirXlxl9BwVMsd9b38jFJqv0lIUpgNNJRZoCDc7IbUw
</Password>
2013/03/15 17:11:30Z: Product activation was successful.
2013/03/15 17:11:32Z: Message: Windows is Ready to use
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
 Ec2Config service v2.1.9.0
2013/03/15 21:04:24Z: There was an exception writing driver information to console: System.Exception:
   at Ec2Config.Service1.Go()
2013/03/15 21:04:35Z: Waiting for meta-data accessibility...
2013/03/15 21:04:40Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BFD64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
2013/03/15 21:05:08Z: Product activation was successful.
2013/03/15 21:05:09Z: Message: Windows is Ready to use
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
 Ec2Config service v2.1.9.0
  Citrix PV Ethernet Adapter v5.9.960.49119
2013/03/15 21:07:20Z: Waiting for meta-data accessibility...
2013/03/15 21:07:21Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BFD64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
2013/03/15 21:07:27Z: Message: Windows is Ready to use
```

8. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
9. Chiudere la finestra di dialogo Red Hat Paravirtualized Xen Drivers for Windows uninstaller (Driver Xen Red Hat paravirtualizzati per il programma di disinstallazione di Windows).
10. Confermare che l'installazione è completa. Andare alla cartella `Citrix-WIN_PV` estratta in precedenza, aprire il file `PVUpgrade.log` e cercare il testo `INSTALLATION IS COMPLETE`.



Aggiornamento del servizio di agente guest Citrix Xen

Se utilizzi driver PV Citrix Xen su Windows Server, puoi aggiornare il servizio d'agente guest Citrix Xen. Questo servizio di Windows gestisce attività come l'arresto e il riavvio di eventi dell'API. Puoi eseguire questo pacchetto di aggiornamento su qualsiasi versione di Windows Server, purché l'istanza esegua driver Citrix PV.

> **Important**
>
> Per Windows Server 2008 R2 e versioni successive, si consiglia di eseguire l'aggiornamento ai driver AWS PV che includono l'aggiornamento Guest Agent.

Prima di avviare l'aggiornamento dei driver, esegui il backup delle informazioni importanti dell'istanza oppure crea un'AMI per tale istanza. Per ulteriori informazioni sulla creazione di un'AMI, consulta Crea un' EBS-backed AMI Amazon.

> **Tip**
>
> Invece di creare l'AMI dalla console Amazon EC2, puoi anche utilizzare Systems Manager Automation per creare l'AMI utilizzando il runbook `AWS-CreateImage`. Per ulteriori informazioni, consulta AWS-CreateImage nella Guida per l'utente di riferimento del runbook di automazione AWS Systems Manager .

Se crei un'AMI, assicurati di completare quanto segue:

- Non abilitare lo strumento Sysprep nel servizio EC2Config.
- Prendi nota della tua password.
- Imposta la scheda Ethernet su DHCP.

Per aggiornare il servizio d'agente guest Citrix Xen

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale. Per ulteriori informazioni sulla connessione all'istanza, consulta Connessione all'istanza Windows con il protocollo RDP.
2. Nell'istanza, scaricare il pacchetto di aggiornamento Citrix.
3. Estrarre il contenuto del pacchetto di aggiornamento in una ubicazione a scelta.

4. Apri il file Upgrade.bat. In caso di avviso di sicurezza, scegliere Run (Esegui).
5. Nella finestra di dialogo Upgrade Drivers (Aggiorna driver), rivedere le informazioni e scegliere Yes (Sì) se si è pronti ad avviare l'aggiornamento.
6. Quando l'aggiornamento è completo, si aprirà il file `PVUpgrade.log` con il testo `UPGRADE IS COMPLETE`.
7. Riavviare l'istanza.

Risoluzione dei problemi relativi ai driver PV sulle istanze Windows

Le seguenti solo soluzioni a problemi che si potrebbero verificare con vecchie immagini Amazon EC2 e driver PV.

Indice

- Windows Server 2012 R2 perde la connettività di rete e archiviazione dopo un riavvio dell'istanza
- Offload TCP
- Sincronizzazione oraria
- I carichi di lavoro che utilizzano più di 20.000 IOPS su disco subiscono una riduzione delle prestazioni dovuta ai colli di bottiglia della CPU

Windows Server 2012 R2 perde la connettività di rete e archiviazione dopo un riavvio dell'istanza

> **Important**
>
> Questo problema si verifica solo con AMI disponibili prima del settembre 2014.

Le Amazon Machine Image (AMI) per Windows Server 2012 R2 rese disponibili prima del 10 settembre 2014 possono perdere connettività di rete e archiviazione dopo un riavvio dell'istanza. L'errore nel registro di Console di gestione AWS sistema indica: «Difficoltà nel rilevamento dei dettagli del driver fotovoltaico per l'uscita della console». La perdita di connettività è causata dalla funzione di pulizia Plug and Play. Questa caratteristica ricerca e disabilita i dispositivi inattivi del sistema ogni 30 giorni. La funzione identifica erroneamente il dispositivo di rete EC2 come inattivo e lo rimuove dal sistema. Quando ciò accade, l'istanza perde la connettività di rete dopo un riavvio.

Per i sistemi ritenuti potenzialmente soggetti a tale problema, puoi scaricare ed eseguire un aggiornamento in sede del driver. Se non riesci a completare tale aggiornamento, puoi eseguire uno

script helper. Questo stabilisce se l'istanza è interessata. Se lo è, e se il dispositivo di rete Amazon EC2 non è stato rimosso, lo script disabilita la scansione di pulizia Plug and Play. Se il dispositivo di rete è stato rimosso, lo script ripara il dispositivo, disabilita la scansione di pulizia Plug and Play e abilita il riavvio dell'istanza con la connessione di rete abilitata.

Indice

- Scegliere come risolvere i problemi
- Metodo 1 – Connettività di rete migliorata
- Metodo 2 – Configurazione del registro
- Esecuzione dello script di correzione

Scegliere come risolvere i problemi

Sono disponibili due metodi per ripristinare la connettività di rete e archiviazione di un'istanza interessata dal problema. Seleziona uno dei seguenti metodi:

Metodo	Prerequisiti	Panoramica della procedura
Metodo 1 – Connettività di rete migliorata	La connettività di rete migliorata è disponibile solo in un cloud privato virtuale (VPC) che richiede un tipo di istanza C3. Se il server non utilizza al momento il tipo di istanza C3, è necessario cambiarlo temporaneamente.	Cambia il tipo di istanza del server in istanza C3. La connettività di rete migliorata ti permette quindi di connetterti all'istanza interessata e di correggere il problema. Dopo aver risolto il problema, modifica l'istanza riportandola al tipo originale. Questo metodo è in genere più rapido del Metodo 2 e meno soggetto a errori da parte dell'utente. Saranno applicati costi aggiuntivi finché l'istanza C3 resta in esecuzione.
Metodo 2 – Configurazione del registro	Capacità di creare o accedere a un secondo server. Capacità	Distacca il volume root dall'istanza interessata, collegalo a un'istanza differente, connettit

Metodo	Prerequisiti	Panoramica della procedura
	di modificare le impostazioni del registro.	i e apporta le modifiche nel registro. Saranno applicati costi aggiuntivi finché il server aggiuntivo resta in esecuzion e. Questo metodo è più lento del Metodo 1, ma si è dimostrato efficace in situazion i in cui il Metodo 1 non ha consentito la risoluzione del problema.

Metodo 1 – Connettività di rete migliorata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Individua l'istanza interessata. Selezionare l'istanza e scegliere Instance state (Stato istanza), quindi Stop (Arresta).

   > **Warning**
   >
   > Quando si arresta un'istanza, i dati sui volumi dell'archivio dell'istanza vengono persi. Per preservare questi dati, esegui il backup su uno storage persistente.

4. Dopo l'arresto dell'istanza, creare un backup. Selezionare l'istanza e scegliere Actions (Operazioni), Image and templates (Immagine e modelli), quindi scegliere Create image (Crea immagine).
5. Cambiare il tipo di istanza con qualsiasi tipo di istanza C3.
6. Avviare l'istanza.
7. Connettiti all'istanza utilizzando Remote Desktop e quindi scarica il pacchetto AWS PV Drivers Upgrade sull'istanza.
8. Estrai i contenuti della cartella ed esegui `AWSPVDriverSetup.msi`.

   Dopo aver eseguito l'MSI, l'istanza si riavvia automaticamente e quindi aggiorna i driver. L'istanza non sarà disponibile per un massimo di 15 minuti.

9. Una volta completato l'aggiornamento e dopo che l'istanza ha superato entrambi i controlli dello stato nella console Amazon EC2, connettersi all'istanza utilizzando Desktop remoto e verificare che i nuovi driver siano istallati. In Gestione dispositivi, in Controller di storage, individua AWS Scheda host storage PV. Verifica che la versione del driver sia la stessa dell'ultima versione elencata nella tabella della cronologia delle versioni dei driver. Per ulteriori informazioni, consulta AWS Cronologia dei pacchetti driver PV.
10. Arrestare l'istanza e modificarla riportandola al suo tipo originale.
11. Avviare l'istanza e ripristinare un utilizzo normale.

Metodo 2 – Configurazione del registro

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Individua l'istanza interessata. Seleziona l'istanza e scegli Instance state (Stato istanza), quindi Stop instance (Arresta istanza).

> **Warning**
>
> Quando si arresta un'istanza, i dati sui volumi dell'archivio dell'istanza vengono persi. Per preservare questi dati, esegui il backup su uno storage persistente.

4. Scegli Launch Instance (Avvia istanza) e crea un'istanza temporanea di Windows Server 2008 o Windows Server 2012 nella stessa zona di disponibilità dell'istanza interessata. Non creare un'istanza Windows Server 2012 R2.

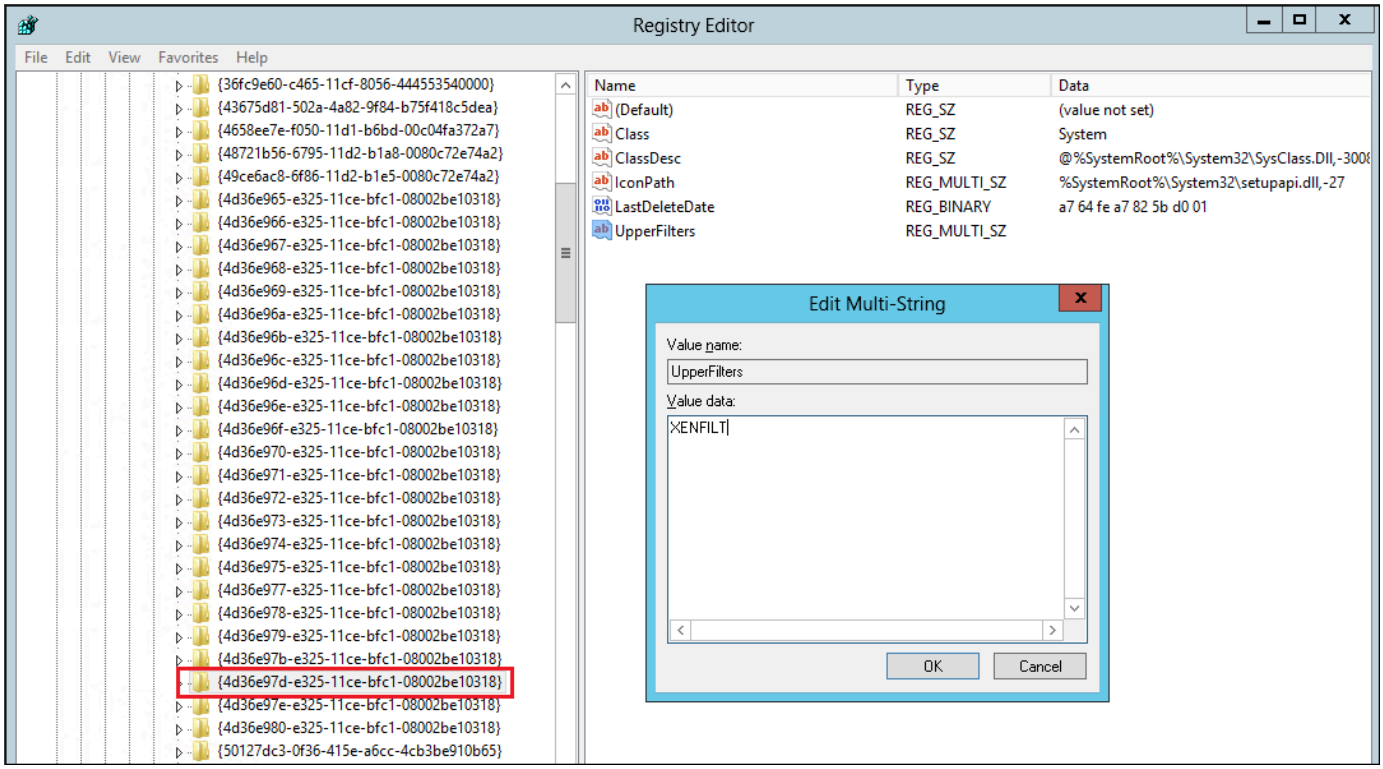
> **Important**
>
> Se non crei l'istanza nella stessa Zona di disponibilità dell'istanza interessata, non potrai collegare il volume root dell'istanza interessata sulla nuova istanza.

5. Nel riquadro di navigazione, selezionare Volumes (Volumi).
6. Individua il volume root dell'istanza interessata. Scollega il volume e collega il volume all'istanza temporanea creata in precedenza. Collegala con il nome del dispositivo predefinito (xvdf).
7. Utilizzare Desktop remoto per collegarsi all'istanza temporanea, quindi usare l'utilità Disk Management (Gestione disco) per rendere il volume disponibile per l'uso.

8. Nell'istanza temporanea, aprire la finestra di dialogo Run (Esegui), digitare **`regedit`** e premere Invio.
9. Nel pannello di navigazione dell'Editor del Registro di sistema, scegli HKEY_ Local_Machine, quindi dal menu File scegli Load Hive.
10. Nella finestra di dialogo Load Hive (Carica Hive), andare a Volume interessato\Windows \System32\config\System e digitare un nome temporaneo nella finestra di dialogo Key Name (Nome chiave). Ad esempio, specifica OldSys.
11. Nel riquadro di navigazione dell'editor del Registro, individuare le chiavi seguenti:

    HKEY_LOCAL_MACHINE\\ 001\ Control\ Class\ ***`your_temporary_key_name`*** 4d36e97d-e325-11ce-bfc1-08002be10318 ControlSet

    HKEY_LOCAL_MACHINE\\ ControlSet 001\ Control***`your_temporary_key_name`***\ Class\ 4d36e96a-e325-11ce-bfc1-08002be10318
12. Per ogni chiave, apri, UpperFilters inserisci un valore di XENFILT, quindi scegli OK.



13. Individuare la chiave seguente:

    HKEY_LOCAL_MACHINE\\ 001\ Services\ XENBUS\ Parameters ***`your_temporary_key_name`*** ControlSet
14. Creare una nuova stringa (REG_SZ) con il nome e il valore seguente: ActiveDevice

PCI\VEN_5853&DEV_0001&SUBSYS_00015853&REV_01

15. Individuare la chiave seguente:

    HKEY_LOCAL_MACHINE\\ 001\ Services\ XENBUS ***your_temporary_key_name*** ControlSet

16. Cambiare il valore Count (Conteggio) da 0 a 1.
17. Individuare ed eliminare le chiavi seguenti:

    HKEY_LOCAL_MACHINE\\ 001\ Servizi\ xenvbd\ ***your_temporary_key_name*** ControlSet StartOverride

    HKEY_LOCAL_MACHINE\\ 001\ Servizi\ xenfilt\ ***your_temporary_key_name*** ControlSet StartOverride

18. Nel riquadro di navigazione dell'editor del Registro, scegliere la chiave temporanea creata contestualmente alla prima apertura dell'editor del Registro.
19. Dal menu File, scegliere Unload Hive (Scarica Hive).
20. Nell'utilità Disk Management (Gestione disco), scegliere l'unità collegata in precedenza, aprire il menu contestuale (pulsante destro del mouse) e scegliere Offline.
21. Nella console Amazon EC2, scollega il volume interessato dall'istanza temporanea e ricollegalo all'istanza di Windows Server 2012 R2 con il nome del dispositivo/. dev/sda1 Devi specificare questo nome del dispositivo per indicare il volume come volume root.
22. Avviare l'istanza.
23. Connettiti all'istanza utilizzando Remote Desktop e quindi scarica il pacchetto AWS PV Drivers Upgrade sull'istanza.
24. Estrai i contenuti della cartella ed esegui `AWSPVDriverSetup.msi`.

    Dopo aver eseguito l'MSI, l'istanza si riavvia automaticamente e quindi aggiorna i driver. L'istanza non sarà disponibile per un massimo di 15 minuti.

25. Una volta completato l'aggiornamento e dopo che l'istanza ha superato entrambi i controlli dello stato nella console Amazon EC2, connettersi all'istanza utilizzando Desktop remoto e verificare che i nuovi driver siano istallati. In Gestione dispositivi, in Controller di storage, individua AWS Scheda host storage PV. Verifica che la versione del driver sia la stessa dell'ultima versione elencata nella tabella della cronologia delle versioni dei driver. Per ulteriori informazioni, consulta AWS Cronologia dei pacchetti driver PV.
26. Cancella o interrompi l'istanza temporanea creata durante questa procedura.

Esecuzione dello script di correzione

Se non riesci a eseguire un aggiornamento in sede del driver o a migrare a un'istanza più recente, puoi eseguire lo script di correzione per risolvere i problemi causati dall'attività di pulizia Plug and Play.

Per eseguire lo script di correzione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Scegliere l'istanza per la quale si intende eseguire lo script di correzione. Selezionare Instance state (Stato istanza), quindi Stop instance (Arresta istanza).

   > **Warning**
   >
   > Quando si arresta un'istanza, i dati sui volumi dell'archivio dell'istanza vengono persi. Per preservare questi dati, esegui il backup su uno storage persistente.

4. Dopo l'arresto dell'istanza, creare un backup. Selezionare l'istanza e scegliere Actions (Operazioni), Image and templates (Immagine e modelli), quindi scegliere Create image (Crea immagine).
5. Selezionare Instance state (Stato istanza), quindi Start instance (Avvia istanza).
6. Connettiti all'istanza utilizzando Remote Desktop e quindi scarica la RemediateDriverIssue.zip cartella nell'istanza.
7. Estrarre i contenuti della cartella.
8. Esegui lo script di riparazione in base alle istruzioni contenute nel Readme.txt file. Il file si trova nella cartella in cui è stato estratto RemediateDriverIssue.zip.

Offload TCP

> **Important**
>
> Questo problema non si applica alle istanze che eseguono driver di AWS rete PV o Intel.

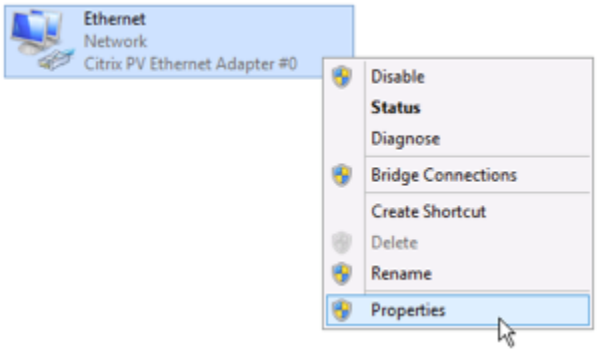
Per impostazione predefinita, l'offload TCP viene abilitato per i driver Citrix PV nelle AMI Windows. Se riscontri errori a livello di trasporto o anomalie nella trasmissione dei pacchetti (come indicato su

Windows Performance Monitor), ad esempio quando stai eseguendo determinati carichi di lavoro SQL, potrebbe essere necessario disabilitare questa caratteristica.

> **Warning**
>
> La disabilitazione dell'offload TCP potrebbe ridurre le prestazioni di rete dell'istanza.

Per disabilitare l'offload TCP per Windows Server 2012 e 2008

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. Se si utilizza Windows Server 2012, premere Ctrl+Esc per accedere alla schermata Start (Avvia), quindi scegliere Control Panel (Pannello di controllo). Se si utilizza Windows Server 2008, scegliere Start (Avvia) e selezionare Control Panel (Pannello di controllo).
3. Scegliere Network and Internet (Rete e Internet), quindi Network and Sharing Center (Centro connessioni di rete e condivisione).
4. Scegliere Change adapter settings (Modifica le impostazioni della scheda).
5. Aprire il menu contestuale (clic con il pulsante destro del mouse) per Citrix PV Ethernet Adapter #0 e selezionare Proprietà.



6. Nella finestra di dialogo Local Area Connection Properties (Proprietà connessione alla rete locale), scegliere Configure (Configura) per aprire la finestra di dialogo Citrix PV Ethernet Adapter #0 Properties (Proprietà scheda Ethernet Citrix PV #0).
7. Nella scheda Avanzate, disabilitate ciascuna proprietà, ad eccezione di Correct TCP/UDP Checksum Value. Per disabilitare una proprietà, selezionarla da Property (Proprietà) e scegliere Disabled (Disattivato) in Value (Valore).
8. Seleziona OK.
9. Nella finestra del prompt dei comandi, eseguire i comandi seguenti.

```
netsh int ip set global taskoffload=disabled
netsh int tcp set global chimney=disabled
netsh int tcp set global rss=disabled
netsh int tcp set global netdma=disabled
```

10. Riavviare l'istanza.

Sincronizzazione oraria

Prima del rilascio del 13/02/2013 dell'AMI Windows, l'agente guest Citrix Xen poteva definire l'ora in modo errato. Ciò può determinare la scadenza della locazione DHCP. In caso di problemi di connessione all'istanza, potresti dover aggiornare l'agente.

Per stabilire se disponi dell'agente guest Citrix Xen aggiornato, controlla se il file `C:\Program Files\Citrix\XenGuestAgent.exe` è datato marzo 2013. Se la data è precedente, aggiorna il servizio d'agente guest Citrix Xen. Per ulteriori informazioni, consulta Aggiornamento del servizio di agente guest Citrix Xen.

I carichi di lavoro che utilizzano più di 20.000 IOPS su disco subiscono una riduzione delle prestazioni dovuta ai colli di bottiglia della CPU

È possibile che si verifichi questo problema se si utilizzano istanze di Windows che eseguono driver AWS PV che sfruttano più di 20.000 IOPS e si verifica un codice di controllo dei bug `0x9E: USER_MODE_HEALTH_MONITOR`.

Le letture e le scritture su disco (IO) nei driver AWS PV avvengono in due fasi: preparazione dell'IO e completamento dell'IO. Per impostazione predefinita, la fase di preparazione viene eseguita su un singolo core arbitrario. La fase di completamento viene invece eseguita sul core `0`. La quantità di elaborazione necessaria per elaborare un IO varia in base alle dimensioni e ad altre proprietà. Alcuni I/O eseguono un'elaborazione maggiore nella fase di preparazione mentre altri nella fase di completamento. Quando un'istanza gestisce più di 20.000 IOPS, la fase di preparazione o di completamento può comportare un collo di bottiglia in cui la CPU su cui viene eseguita è al 100% di capacità. Il fatto che la fase di preparazione o completamento diventi un collo di bottiglia dipende dalle proprietà dell'iOS utilizzato dall'applicazione.

A partire dai driver AWS fotovoltaici 8.4.0, il carico della fase di preparazione e della fase di completamento può essere distribuito su più core, eliminando i colli di bottiglia. Ogni applicazione utilizza proprietà IO diverse. Pertanto, l'applicazione di una delle seguenti configurazioni potrebbe

aumentare, ridurre o non influire affatto sulle prestazioni dell'applicazione. Dopo aver applicato una di queste configurazioni, monitorare l'applicazione per verificare di raggiungere le prestazioni desiderate.

1. Prerequisiti

   Prima di iniziare questa procedura di risoluzione dei problemi, verificare i seguenti prerequisiti:

   - La tua istanza utilizza i driver AWS PV versione 8.4.0 o successiva. Per eseguire l'aggiornamento, consulta Aggiornamento dei driver PV sulle istanze Windows EC2.
   - Hai accesso RDP all'istanza. Per la procedura di connessione all'istanza Windows tramite RDP, consulta Connettiti alla tua istanza Windows utilizzando un client RDP.
   - Disponi dell'accesso amministratore sull'istanza.

2. Osservazione del carico della CPU sull'istanza

   Puoi utilizzare Gestione attività di Windows per visualizzare il carico su ogni CPU in modo da determinare potenziali colli di bottiglia per l'IO del disco.

   1. Verifica che l'applicazione sia in esecuzione e gestisca il traffico come il carico di lavoro di produzione.
   2. Connettiti all'istanza tramite RDP.
   3. Seleziona il menu Avvia sull'istanza.
   4. Specifica `Task Manager` nel menu Avvia per aprire Gestione attività.
   5. Se Gestione attività visualizza la visualizzazione di riepilogo, seleziona Maggiori dettagli per espandere la vista dettagliata.
   6. Scegliere la scheda Performance (Prestazioni).
   7. Seleziona CPU nel riquadro sinistro.
   8. Apri il menu contestuale (clic con il pulsante destro del mouse) per il grafico nel riquadro principale e seleziona Cambia grafico in > Processori logici per visualizzare ogni singolo core.
   9. A seconda del numero di core presenti nella tua istanza, potresti vedere le righe che visualizzano il carico della CPU nel tempo oppure potresti semplicemente vedere un numero.
      - Se vedi grafici che mostrano il carico nel tempo, cerca le CPU in cui il riquadro è quasi completamente ombreggiato.
      - Se visualizzi un numero su ciascun core, cerca i core che riportano costantemente il 95% o un valore maggiore.

10. Prendi nota se per il core `0` o un altro core si sta verificando un carico pesante.

3. Scelta della configurazione da applicare

Nome configurazione	Quando applicare questa configurazione	Note
Default configuration	Il carico di lavoro è inferiore a 20.000 IOPS o altre configurazioni non hanno migliorato le prestazioni o la stabilità.	Per questa configurazione, l'IO si verifica su pochi core che possono beneficia re di carichi di lavoro più piccoli aumentando la localizzazione della cache e riducendo la commutazione di contesto.
Allow driver to choose whether to distribute completion	Il carico di lavoro sta conducendo oltre 20.000 IOPS e si osserva un carico moderato o elevato sul core `0` .	Questa configurazione è consigliata per tutte le istanze Xen che utilizzano PV 8.4.0 o versioni successiv e e che sfruttano più di 20.000 IOPS, indipende ntemente dal fatto che si verifichino problemi.
Distribute both preparation and completion	Il carico di lavoro sta utilizzan do oltre 20.000 IOPS e consente al driver di scegliere la distribuzione che non ha migliorato le prestazioni o per un core diverso da `0` si sta verifican do un carico elevato.	Questa configurazione consente la distribuzione sia della fase di preparazione IO che della fase di completam ento.

> **Note**
>
> Si consiglia di non distribuire la preparazione IO senza distribuire anche il completamento (impostazione `DpcRedirection` senza impostazione `NotifierDistributed`) perché la fase di completamento è sensibile al sovraccarico dovuto alla fase di preparazione quando la fase di preparazione è in esecuzione in parallelo.

Valori chiave del registro

- NotifierDistributed

  Valore `0` o non presente — La fase di completamento verrà eseguita sul core `0` .

  Valore `1` — Il driver sceglie di eseguire la fase di completamento sul core `0` o un core aggiuntivo per disco collegato.

  Valore `2` — Il driver esegue la fase di completamento su un core aggiuntivo per ogni disco collegato.
- DpcRedirection

  Valore `0` o non presente — La fase di preparazione verrà eseguita su un unico core arbitrario.

  Valore `1` — La fase di preparazione è distribuita su più core.

Configurazione di default

Applica la configurazione predefinita con versioni dei driver AWS PV precedenti alla 8.4.0 o se si osserva un peggioramento delle prestazioni o della stabilità dopo aver applicato una delle altre configurazioni in questa sezione.

1. Connettiti all'istanza tramite RDP.
2. Aprire un nuovo prompt dei PowerShell comandi come amministratore.

3. Emettere i seguenti comandi per rimuovere le chiavi di registro `NotifierDistributed` e `DpcRedirection`.

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name NotifierDistributed
```

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name DpcRedirection
```

4. Riavviare l'istanza.

Consenti al driver di scegliere se distribuire il completamento

Imposta la chiave di `NotiferDistributed` registro per consentire al driver di archiviazione PV di scegliere se distribuire il completamento dell'IO.

1. Connettiti all'istanza tramite RDP.
2. Aprire un nuovo PowerShell prompt dei comandi come amministratore.
3. Emettere il seguente comando per impostare la chiave di registro `NotiferDistributed`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name NotifierDistributed
```

4. Riavviare l'istanza.

Distribuisci sia la preparazione che il completamento

Impostare le chiavi di registro `NotifierDistributed` e `DpcRedirection` per distribuire sempre sia la fase di preparazione che quella di completamento.

1. Connettiti all'istanza tramite RDP.
2. Aprire un nuovo PowerShell prompt dei comandi come amministratore.
3. Emettere i seguenti comandi per impostare le chiavi di registro `NotifierDistributed` e `DpcRedirection`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000002 -Name NotifierDistributed
```

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name DpcRedirection
```

4. Riavviare l'istanza.

Driver NVMe

I volumi Amazon EBS e i volumi degli store di istanze sono esposti come dispositivi a blocchi NVMe sulle istanze. Nitro-based Per utilizzare appieno le prestazioni e le funzionalità delle funzionalità di Amazon EBS per i volumi esposti come dispositivi a blocchi NVMe, sull'istanza deve essere installato il driver NVMe. AWS Tutte le AMI AWS Windows di ultima generazione vengono fornite con il driver NVMe installato per impostazione predefinita AWS .

Per ulteriori informazioni su EBS e NVMe, consulta Amazon EBS e NVMe nella Guida per l'utente di Amazon EBS. Per ulteriori informazioni sulle instance store SSD e NVMe, consulta Volumi di archivio dell'istanza SSD per istanze EC2.

Istanze Linux

Le AMI seguenti includono i driver NVMe necessari:

- Amazon Linux 2
- AMI Amazon Linux 2018.03
- Ubuntu 14.04 o versioni successive con kernel `linux-aws`

> **Note**
>
> AWS Graviton-based i tipi di istanza richiedono Ubuntu 18.04 o versioni successive con kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 o versioni successive
- SUSE Linux Enterprise Server 12 SP2 o versioni successive
- CentOS 7.4.1708 o versioni successive

- FreeBSD 11.1 o versioni successive
- Debian 9 o versioni successive GNU/Linux

Per confermare che l'istanza disponga del driver NVMe

È possibile verificare che l'istanza disponga del driver NVMe utilizzando il comando seguente.

- Amazon Linux, RHEL, CentOS e SUSE Linux Enterprise Server

```
$ modinfo nvme
```

  Se l'istanza ha il driver NVMe, il comando restituisce informazioni sul driver.
- Amazon Linux 2 e Ubuntu

```
$ ls /sys/module/ | grep nvme
```

  Se l'istanza ha il driver NVMe, il comando restituisce i driver installati.

Per aggiornare il driver NVMe

Se l'istanza ha il driver NVMe, è possibile aggiornare il driver alla versione più recente utilizzando la procedura seguente.

1. Connettiti alla tua istanza.
2. Aggiornare la cache dei pacchetti per ottenere gli aggiornamenti dei pacchetti necessari come riportato di seguito.
   - Per Amazon Linux 2, Amazon Linux, CentOS e Red Hat Enterprise Linux:

     ```
     [ec2-user ~]$ sudo yum update -y
     ```
   - Per Ubuntu e Debian:

     ```
     [ec2-user ~]$ sudo apt-get update -y
     ```
3. Ubuntu 16.04 e versioni successive includono il `linux-aws` pacchetto, che contiene i driver NVMe ed ENA richiesti dalle istanze. Nitro-based Aggiornare il pacchetto `linux-aws` per ricevere la versione più recente come riportato di seguito:

```
[ec2-user ~]$ sudo apt-get install --only-upgrade -y linux-aws
```

Per Ubuntu 14.04, è possibile installare il pacchetto `linux-aws` più recente come segue:

```
[ec2-user ~]$ sudo apt-get install linux-aws
```

4. Riavviare l'istanza per caricare la versione più recente del kernel.

```
sudo reboot
```

5. Riconnettersi all'istanza dopo averla riavviata.

Istanze Windows

PowerShell

Se non hai avviato l'istanza da una delle più recenti AMI AWS Windows fornite da Amazon, utilizza la seguente procedura per installare il driver AWS NVMe corrente sulla tua istanza. Per questa installazione è richiesto il riavvio. L'istanza verrà riavviata dallo script di installazione oppure devi riavviarla come fase finale.

Prerequisiti

- PowerShell è installata la versione 3.0 o successiva.
- I comandi mostrati in questa sezione devono essere eseguiti nella versione a 64 bit di PowerShell. Non utilizzare la `x86` versione di PowerShell. Questa è la versione a 32 bit della shell e non è supportata per questi comandi.

Per scaricare e installare la versione più recente AWS Driver NVMe

1. Si consiglia di creare un'AMI come backup come segue, nel caso in cui sia necessario eseguire il rollback delle modifiche.

   a. Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Prima di arrestare un'istanza, verificare di aver copiato tutti i dati necessari dai volumi di instance store nello storage persistente, ad esempio Amazon EBS o Amazon S3.
   b. Nel riquadro di navigazione, scegliere Instances (Istanze).

c. Selezionare l'istanza che richiede l'aggiornamento del driver e scegliere Instance state (Stato istanza), Stop instance (Arresta istanza).

d. Dopo avere interrotto l'istanza, selezionare l'istanza, scegliere Actions (Operazioni), Image and templates (Immagine e modelli), quindi scegliere Create image (Crea immagine).

e. Scegli Instance state (Stato istanza), Start instance (Avvia istanza).

2. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.

3. Scarica i driver sull'istanza utilizzando una delle seguenti opzioni:

   - Browser: scarica il pacchetto di driver più recente per l'istanza ed estrai l'archivio zip.
   - PowerShell— Esegui i seguenti comandi:

```
Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/
NVMe/Latest/AWSNVMe.zip -outfile $env:USERPROFILE\nvme_driver.zip
Expand-Archive $env:userprofile\nvme_driver.zip -DestinationPath
 $env:userprofile\nvme_driver
```

   Se si riceve un errore durante il download del file e si utilizza Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il PowerShell terminale. Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il comando seguente e riprovare:

```
[Net.ServicePointManager]::SecurityProtocol =
 [Net.SecurityProtocolType]::Tls12
```

4. Installa il driver sulla tua istanza eseguendo lo `install.ps1` PowerShell script dalla `nvme_driver` directory (`.\install.ps1`). Se ricevi un errore, assicurati di utilizzare PowerShell 3.0 o versioni successive.

   a. (Facoltativo) A partire dalla versione AWS NVMe`1.5.0`, le prenotazioni permanenti Small Computer System Interface (SCSI) sono supportate per Windows Server 2016 e versioni successive. Questa funzionalità aggiunge il supporto per Windows Server Failover Clustering con archiviazione Amazon EBS condivisa. Per impostazione predefinita, questa funzionalità non è abilitata durante l'installazione.

   È possibile abilitare la funzionalità durante l'esecuzione dello script `install.ps1` per installare il driver specificando il parametro `EnableSCSIPersistentReservations` con un valore di `$true`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $true
```

È possibile disabilitare la funzionalità durante l'esecuzione dello script `install.ps1` per installare il driver specificando il parametro `EnableSCSIPersistentReservations` con un valore di `$false`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $false
```

b. A partire da AWS NVMe`1.5.0`, `install.ps1` lo script installa sempre lo strumento con il driver. `ebsnvme-id`

(Facoltativo) Per le versioni `1.4.0`, `1.4.1` e `1.4.2`, lo script `install.ps1` consente di specificare se lo strumento `ebsnvme-id` deve essere installato con il driver.

i. Per installare lo strumento `ebsnvme-id`, specificare `InstallEBSNVMeIdTool 'Yes'`.

ii. Se non si desidera installare lo strumento, specificare `InstallEBSNVMeIdTool 'No'`.

Se non si specifica `InstallEBSNVMeIdTool` e lo strumento è già presente su `C:\ProgramData\Amazon\Tools`, il pacchetto aggiornerà lo strumento per impostazione predefinita. Se lo strumento non è presente, `install.ps1` non aggiornerà lo strumento per impostazione predefinita.

Se non desideri installare lo strumento come parte del pacchetto ma desideri installarlo in un secondo momento, puoi trovare la versione più recente o lo strumento nel pacchetto driver. In alternativa, puoi scaricare la versione `1.0.0` da Amazon S3:

Scarica lo strumento `ebsnvme-id`.

5. Se il programma di installazione non riavvia l'istanza, riavviala manualmente.

Distributor

È possibile utilizzare Distributor, una funzionalità di AWS Systems Manager, per installare il pacchetto driver NVMe una volta o con aggiornamenti pianificati.

Per installare la versione più recente AWS Driver NVMe

1. Per istruzioni su come installare il pacchetto di driver NVMe utilizzando Distributor, consulta le procedure descritte in Installazione o aggiornamento dei pacchetti nella Guida per l'utente di Amazon EC2 Systems Manager.
2. In Tipo di installazione, scegli Disinstalla e reinstalla.
3. Per Nome, scegliere AWSNVMe.
4. (Facoltativo) Per Argomenti aggiuntivi, puoi personalizzare l'installazione specificando i valori. I valori devono essere formattati utilizzando una sintassi JSON valida. Per esempi su come passare argomenti aggiuntivi per il pacchetto `aws configure`, consulta la Documentazione di riferimento sul plugin per il documento di comando.

   a. A partire da AWS NVMe`1.5.0`, il driver supporta le prenotazioni permanenti SCSI per Windows Server 2016 e versioni successive. Per impostazione predefinita, questa funzionalità non è abilitata durante l'installazione.

      - Per abilitare questa funzionalità, specifica `{"SSM_EnableSCSIPersistentReservations": "true"}`.
      - Se non desideri abilitare questa funzionalità, specifica `{"SSM_EnableSCSIPersistentReservations": "false"}`.

   b. A partire da AWS NVMe`1.5.0`, `install.ps1` lo script installerà sempre lo strumento. `ebsnvme-id`

      (Facoltativo) Per le versioni `1.4.0`, `1.4.1` e `1.4.2`, lo script `install.ps1` consente di specificare se lo strumento ebsnvme-id deve essere installato con il driver.

      - Per installare lo strumento ebsnvme-id, specifica `{"SSM_InstallEBSNVMeIdTool": "Yes"}`.
      - Se non si desidera installare lo strumento, specificare `{"SSM_InstallEBSNVMeIdTool": "No"}`.

      Se `SSM_InstallEBSNVMeIdTool` non è specificato per Argomenti aggiuntivi e lo strumento è già presente in `C:\ProgramData\Amazon\Tools`, il pacchetto aggiornerà lo strumento per impostazione predefinita. Se lo strumento non è presente, il pacchetto non aggiornerà lo strumento per impostazione predefinita.

Se non desideri installare lo strumento come parte del pacchetto ma desideri installarlo in un secondo momento, puoi trovare la versione più recente dello strumento nel pacchetto driver. In alternativa, puoi scaricare la versione `1.0.0` da Amazon S3:

Scarica lo strumento `ebsnvme-id`.

5. Se il programma di installazione non riavvia l'istanza, riavviala manualmente.

Configura le prenotazioni persistenti SCSI per le istanze Windows

Dopo aver installato la versione del driver AWS NVMe `1.5.0` o successiva, è possibile abilitare o disabilitare le prenotazioni permanenti SCSI utilizzando il registro di Windows per Windows Server 2016 e versioni successive. Per applicare le modifiche al registro è necessario riavviare l'istanza.

È possibile abilitare le prenotazioni persistenti SCSI con il seguente comando che imposta il valore `EnableSCSIPersistentReservations` su `1`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 1
```

È possibile disabilitare le prenotazioni persistenti SCSI con il seguente comando che imposta il valore `EnableSCSIPersistentReservations` su `0`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 0
```

AWS Cronologia delle versioni dei driver NVMe per Windows

La tabella seguente mostra quali driver AWS NVMe vengono eseguiti su ciascuna versione di Windows Server su Amazon EC2.

Versione di Windows Server	AWS Versione del driver NVMe
Windows Server 2025	versione più recente
Windows Server 2022	versione più recente

Versione di Windows Server	AWS Versione del driver NVMe
Windows Server 2019	versione più recente
Windows Server 2016	versione più recente
Windows Server 2012 R2	versione 1.5.1 e precedente
Windows Server 2012	versione 1.5.1 e precedente
Windows Server 2008 R2	versione 1.3.2 e precedente
Windows Server 2008	versione 1.3.2 e precedente

La tabella seguente descrive le versioni rilasciate del driver AWS NVMe.

Versione del pacchetto	Versione driver	Dettagli	Data di rilascio
1.8.2 1.8.2 1.8.2	1.8.2	• È stato corretto il controllo dei bug all'avvio migliorando la gestione delle interruzioni.	15 giugno 2026
1.8.1 1.8.1	1.8.1	• È stato risolto un problema di compatibilità con le versioni precedenti con la generazione del numero di serie del disco.	24 febbraio 2026
1.8.0	1.8.0	• È stato aggiunto il supporto per gli IOCTL per funzionare con dispositivi che implementano la gestione dinamica dello spazio dei nomi. Per ulteriori informazioni, vedere IOCTL_SCSI_MINIPORT IOCTL nella documentazione Microsoft. • Correzioni di bug nel comando Get Log Page e nella generazione del numero di serie.	16 gennaio 2026

Versione del pacchetto	Versione driver	Dettagli	Data di rilascio
1.7.0	1.7.0	• Aggiunto supporto per il comando NVMe Get Log Page. • Aggiunto supporto per statistiche dettagliate sulle prestazioni per volumi di archivio dell'istanza EBS e EC2. • Correzioni dei bug per il comando Identifica namespace.	17 settembre 2025
1.6.0	1.6.0	• Aggiornato lo script di installazione per utilizzare PNPUtil. • Aggiornato ebsnvme-id.exe per utilizzare NVMe IOCTL.	25 ottobre 2024
1.5.1	1.5.0	È stato corretto lo script di installazione per creare una cartella per lo strumento `ebsnvme-id` se non è presente.	17 novembre 2023
1.5.0	1.5.0	È stato aggiunto il supporto per le prenotazioni persistenti SCSI (Small Computer System Interface) per le istanze che eseguono Windows Server 2016 e versioni successive. Lo strumento ebsnvme-id (`ebsnvme-id.exe`) è ora installato per impostazione predefinita.	31 agosto 2023
1.4.2	1.4.2	È stato corretto un bug per cui non Driver AWS NVMe supportava i volumi di archiviazione delle istanze sulle istanze D3.	16 marzo 2023

Versione del pacchetto	Versione driver	Dettagli	Data di rilascio
1.4.1	1.4.1	Riferisce su Namespace Preferred Write Granularity (NPGW) per i volumi EBS che supportano questa caratteristica NVMe opzionale. Per ulteriori informazioni, vedere la sezione 8.25, «Miglioramento delle prestazioni attraverso l'aderenza alle I/O dimensioni e all'allineamento», nella specifica di base NVMe, versione 1.4.	20 maggio 2022
1.4.0	1.4.0	• Aggiunto il supporto per gli IOCTL che consentono alle applicazioni di interagire con i dispositivi NVMe. Questo supporto consente alle applicazioni di ottenere l'elenco di `IdentifyController` , `IdentifyNamespace` e `NameSpace` dal dispositivo NVMe. Per ulteriori informazioni, consulta le Protocol-specific domande nella documentazione Microsoft. • La versione del driver 1.4.0 e lo strumento `ebsnvme-id` più recente (`ebsnvme-id.exe`) sono combinati in un unico pacchetto. Questa combinazione consente di installare sia il driver che lo strumento da un unico pacchetto. Per ulteriori dettagli, consultare Driver NVMe. • Correzioni di bug e miglioramenti dell'affidabilità.	23 novembre 2021

Versione del pacchetto	Versione driver	Dettagli	Data di rilascio
1.3.2	1.3.2	È stato risolto un problema che potrebbe causare il danneggiamento dei dati relativo alla modifica dei volumi EBS che elaborano attivamente operazioni di I/O. I clienti che non modificano i volumi EBS online (ad esempio attraverso ridimensionamento o modifica del tipo) non sono interessati. Questa è l'ultima versione che può essere eseguita su Windows Server 2008 e 2008 R2. Questa versione è disponibile per il download ma non è più supportata. Windows Server 2008 e 2008 R2 ha raggiunto la fine del suo ciclo di vita e non è più supportato da Microsoft .	10 settembre 2019
1.3.1	1.3.1	Migliorie in termini di affidabilità.	21 maggio 2019
1.3.0	1.3.0	Miglioramenti dell'ottimizzazione dei dispositivi.	31 agosto 2018
1.2.0	1.2.0	Miglioramenti delle prestazioni e dell'affidabilità per i dispositivi AWS NVMe su tutte le istanze supportate, incluse le istanze bare metal.	13 giugno 2018
>1.0.0	>1.0.0	AWS Driver NVMe per i tipi di istanze supportati che eseguono Windows Server.	12 febbraio 2018

Sottoscrizione alle notifiche di

Amazon SNS può avvisarti in caso di pubblicazione di nuove versioni dei driver Windows di EC2. Utilizza la procedura seguente per effettuare l'iscrizione a queste notifiche.

Per effettuare la sottoscrizione alle notifiche EC2 dalla console

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. È necessario selezionare questa regione perché le notifiche SNS per le quali stai effettuando la sottoscrizione si trovano in questa regione.
3. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
4. Scegli Crea sottoscrizione.
5. Nella finestra di dialogo Create subscription (Crea sottoscrizione) segui questi passaggi:
   a. In Topic ARN (ARN argomento) copia il seguente nome della risorsa Amazon (ARN):

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. In Protocol (Protocollo), scegli `Email`.
   c. In Endpoint digita l'indirizzo e-mail utilizzabile per ricevere le notifiche.
   d. Scegli Create Subscription (Crea sottoscrizione).
6. Riceverai a breve un'e-mail di conferma. Apri l'e-mail e segui le istruzioni per completare l'iscrizione.

Quando i nuovi driver Windows di EC2 vengono rilasciati, inviamo notifiche ai sottoscrittori. Se non desideri più ricevere queste notifiche, segui la procedura seguente per annullare la sottoscrizione.

Per annullare la sottoscrizione alle notifiche dei driver Windows per Amazon EC2

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
3. Seleziona la casella di spunta della sottoscrizione, quindi scegli Actions (Operazioni), Delete subscriptions (Cancella sottoscrizioni). Quando viene richiesta la conferma, seleziona Elimina.

Per abbonarsi alle notifiche EC2 utilizzando AWS CLI

Per iscriverti alle notifiche EC2 con il AWS CLI, usa il seguente comando.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers --
protocol email --notification-endpoint YourUserName@YourDomainName.ext
```

Per abbonarsi alle notifiche EC2 utilizzando AWS Tools for Windows PowerShell

Per iscriverti alle notifiche EC2 con AWS Tools for Windows PowerShell, usa il seguente comando.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers' -Protocol email -Region us-east-1 -Endpoint 'YourUserName@YourDomainName.ext'
```

Altri driver di dispositivo Windows

Il dispositivo AWS VMClock è un dispositivo di orologio virtuale presente sulle istanze. Nitro-based Il dispositivo viene visualizzato in Gestione dispositivi nella sezione Dispositivi di sistema come. `AWS VMClock Device` AWS fornisce un pacchetto driver nullo (senza funzione) per Windows che consente al sistema operativo di riconoscere il dispositivo.

Istanze supportate

Il dispositivo AWS VMClock è disponibile per i tipi di istanza. Nitro-based Per un elenco dei tipi di Nitro-based istanze, vedi Nitro-based istanze.

Sistemi operativi supportati

Il pacchetto driver supporta le seguenti versioni di Windows Server:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Installazione del driver

Se il dispositivo AWS VMClock mostra un'icona di avviso in Device Manager, che indica che non è installato alcun driver, è possibile installare manualmente il pacchetto null driver.

Per installare AWS Il driver VMClock

1. Scarica ed estrai il pacchetto driver da Amazon S3.

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSVMClock/Latest/AWSVMClock.zip -OutFile $env:USERPROFILE\AWSVMClock.zip
   ```

```
Expand-Archive $env:USERPROFILE\AWSVMClock.zip -DestinationPath $env:USERPROFILE
\AWSVMClock
```

2. Installa il driver utilizzando`pnputil`.

```
pnputil /add-driver $env:USERPROFILE\AWSVMClock\aws_vmclock.inf /install
```

3. Verifica lo stato del dispositivo in Gestione dispositivi. Non è necessario riavviare l'istanza.

Configurazione dell'istanza Amazon EC2 Windows

Dopo aver avviato un'istanza di Windows, puoi accedere come amministratore per eseguire configurazioni aggiuntive per le funzionalità e le impostazioni di sistema di Windows. Utilità per la risoluzione dei problemi di Windows EC2 può essere utile per risolvere i problemi sull'istanza.

È possibile configurare gli agenti di avvio di Windows e altre funzionalità nel modo seguente. Windows-specific

Agenti di avvio Windows

Ogni AWS Windows AMI (e molte altre AMI disponibili su Marketplace AWS) include un Windows Launch Agent preconfigurato con impostazioni predefinite. Gli agenti di avvio svolgono attività durante lo startup dell'istanza e vengono eseguiti se un'istanza viene arrestata e successivamente avviata o se viene riavviata.

EC2 Fast Launch per Windows

Ogni istanza Windows Amazon EC2 deve superare i passaggi di avvio standard del sistema operativo Windows (OS), che includono diversi riavvii e spesso richiedono 15 minuti o più per essere completati. Le AMI Windows Server Amazon EC2 su cui è abilitata la funzionalità EC2 Fast Launch completano alcuni di questi passaggi e si riavviano in anticipo per ridurre il tempo necessario all'avvio di un'istanza.

Windows-specific impostazioni di sistema

L'elenco seguente include alcune impostazioni di sistema che si applicano solo ai sistemi operativi Windows:

Modifica della password dell'amministratore Windows

Quando ti connetti a un'istanza Windows, è necessario specificare un account utente e una password che disponga dell'autorizzazione per accedere all'istanza. La prima volta che ti connetti a un'istanza, devi utilizzare l'account dell'amministratore e fornire la password predefinita. Quando ti connetti a un'istanza per la prima volta, ti consigliamo di modificare il valore predefinito della password dell'amministratore.

Aggiunta di componenti di sistema Windows

I sistemi operativi Windows Server includono molti componenti opzionali. L'inclusione di tutti i componenti opzionali in ciascuna AMI di AWS Windows Server non è pratico. Al contrario, noi forniamo snapshot EBS dei supporti di installazione contenenti i file necessari per configurare o installare i componenti sulle istanze Windows.

Installazione di WSL su Windows

Windows Subsystem per Linux (WSL) è disponibile come download gratuito da installare sull'istanza di Windows. Installando WSL, puoi eseguire strumenti nativi della riga di comando di Linux direttamente sull'istanza di Windows e utilizzare gli strumenti di Linux per lo scripting, accanto al tradizionale desktop di Windows. Puoi passare facilmente da Linux a Windows su una singola istanza di Windows, utile per esempio in un ambiente di sviluppo.

AWS driver di dispositivo per istanze Windows

Puoi aggiornare i driver di AWS dispositivo per le tue istanze Windows. Per ulteriori informazioni, consulta the section called “Gestione dei driver di dispositivo”.

La tabella seguente riassume i driver supportati per le Nitro-based istanze in base alla versione di Windows.

Versione	Driver di archiviazione	Driver di rete avanzata
Windows Server 2025	AWS Ultima versione di NVMe	Versione più recente di ENA
Windows Server 2022	AWS Ultima versione di NVMe	Versione più recente di ENA
Windows Server 2019	AWS Ultima versione di NVMe	Versione più recente di ENA
Windows Server 2016	AWS Ultima versione di NVMe	Versione più recente di ENA

Versione	Driver di archiviazione	Driver di rete avanzata
Windows Server 2012 R2	AWS NVMe versione 1.5.1	ENA versione 2.6.0
Windows Server 2008 R2	AWS NVMe versione 1.3.2	ENA versione 2.2.3

La tabella seguente riassume i driver supportati per le Xen-based istanze in base alla versione di Windows.

Versione	Driver di archiviazione	Driver di rete avanzata
Windows Server 2022	AWS Versione più recente di PV	• Versione più recente di ENA [1] • Intel VF [2] • AWS Ultima versione 3 di PV
Windows Server 2019	AWS Ultima versione di PV	• Versione più recente di ENA [1] • Intel VF [2] • AWS Ultima versione 3 di PV
Windows Server 2016	AWS Ultima versione di PV	• Versione più recente di ENA [1] • Intel VF [2] • AWS Ultima versione 3 di PV
Windows Server 2012 R2	AWS PV versione 8.4.3	• ENA versione 2.6.0 [1] • Intel VF [2] • AWS PV versione 8.4.3 3

Versione	Driver di archiviazione	Driver di rete avanzata
Windows Server 2008 R2	AWS PV versione 8.3.5	• ENA versione 2.2.3 [1] • Intel VF [2] • AWS PV versione 8.3.5 3

[1] Ad esempio i tipi G3, H1, I3, P3`m4.16xlarge`, P3dn e R4.

[2] Per tipi di istanza C3, C4, D2, I2, M4 (esclusa `m4.16xlarge`) e R3.

[3] Per tipi di istanza C1, M1, M2, M3, T1, T2, X1 e X1e.

Agenti di avvio Windows su istanze Amazon EC2 Windows

Ogni AWS Windows AMI include un Windows Launch Agent preconfigurato con impostazioni predefinite. Gli agenti di avvio svolgono attività durante lo startup dell'istanza e vengono eseguiti se un'istanza viene arrestata e successivamente avviata o se viene riavviata. Per informazioni su un agente specifico, consulta le pagine di dettaglio nell'elenco seguente.

Per ulteriori informazioni sulle AMI AWS Windows, consulta la guida di riferimento per AWS Windows AMI.

- Utilizza l'agente EC2Launch v2 per eseguire attività durante l'avvio dell'istanza EC2 Windows
- Utilizza l'agente EC2Launch v1 per eseguire attività durante l'avvio dell'istanza EC2 Windows
- Utilizza il servizio EC2Config per eseguire attività durante l'avvio dell'istanza del sistema operativo Windows legacy EC2

Contenuti

- Confronto degli agenti di avvio Amazon EC2
- Configura il suffisso DNS per gli agenti di avvio EC2 Windows
- Sottoscrizione alle notifiche dell'agente di avvio EC2 Windows
- Amministrazione dei servizi Windows per gli agenti EC2Launch v2 ed EC2Config

Confronto degli agenti di avvio Amazon EC2

Nella tabella seguente vengono illustrate le principali differenze funzionali tra EC2Config, EC2Launch v1 e EC2Launch v2.

Caratteristica	EC2Config	EC2Launch v1	EC2Launch v2
Run as (Esegui come)	Servizio Windows	PowerShell Script	Servizio Windows
Supporta	Solo sistemi operativi legacy	Versioni di Windows Server: • 2016 • 2019 (LTSC e SAC)	Versioni di Windows Server: • 2016 • 2019 (LTSC e SAC) • 2022 • 2025
File di configurazione	XML	JSON	JSON/YAML
Imposta nome utente amministratore	No	No	Sì
Dati utente compressi	No	No	Sì
Dati utente locali inseriti in AMI	No	No	Sì, configurabile
Configurazione delle attività nei dati utente	No	No	Sì
Sfondo configurabile	No	No	Sì
Personalizza l'ordine di esecuzione delle attività	No	No	Sì
Attività configurabili	15	9	20 all'avvio

Caratteristica	EC2Config	EC2Launch v1	EC2Launch v2
Supporta il Visualizzatore eventi di Windows	Sì	No	Sì
Numero di tipi di evento del Visualizzatore eventi	2	0	30

> **Note**
>
> La documentazione di EC2Config viene fornita solo per riferimenti storici. Le versioni del sistema operativo su cui viene eseguito non sono più supportate da Microsoft. Consigliamo fortemente di eseguire l'aggiornamento al servizio di avvio più recente.

Configura il suffisso DNS per gli agenti di avvio EC2 Windows

Con gli agenti di avvio di Amazon EC2, puoi configurare un elenco di suffissi DNS utilizzati dalle istanze Windows per la risoluzione dei nomi di dominio. Gli agenti di avvio sostituiscono le impostazioni standard di Windows nella chiave di registro `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` aggiungendo i seguenti valori all'elenco di ricerca dei suffissi DNS:

- Il dominio dell'istanza
- I suffissi risultanti dalla devoluzione del dominio dell'istanza
- Dominio NV
- I domini specificati da ciascuna scheda di interfaccia di rete

Tutti gli agenti di avvio supportano la configurazione dei suffissi DNS. Per ulteriori informazioni, consulta la versione specifica dell'agente di avvio:

- Per informazioni sull'attività `setDnsSuffix` e su come configurare i suffissi DNS in EC2Launch v2, consulta set DnsSuffix.

- Per informazioni sulla configurazione dell'elenco dei suffissi DNS e su come abilitare o disabilitare la devoluzione per EC2Launch v1, consulta Configurazione dell'agente EC2Launch v1 sulla istanza di Windows.
- Per informazioni sulla configurazione dell'elenco dei suffissi DNS e su come abilitare o disabilitare la devoluzione per EC2Config, consulta File delle impostazioni di EC2Config.

Devoluzione dei nomi di dominio

La devoluzione dei nomi di dominio è un comportamento di Active Directory che consente ai computer di un dominio figlio di accedere alle risorse nel dominio padre senza utilizzare un nome di dominio completo. Per impostazione predefinita, la devoluzione del nome di dominio continua fino a quando rimangono solo due nodi nella progressione del nome di dominio.

Gli agenti di avvio svolgono la devoluzione sul nome di dominio se l'istanza è connessa a un dominio e aggiungono i risultati all'elenco di ricerca dei suffissi DNS mantenuto nella chiave di registro **`System\CurrentControlSet\Services\Tcpip\Parameters\SearchList`**. Gli agenti utilizzano le impostazioni delle seguenti chiavi di registro, per determinare il comportamento di devoluzione.

- **`System\CurrentControlSet\Services\Tcpip\Parameters\UseDomainNameDevolution`**
  - Senza impostazione, la devoluzione è disabilitata
  - Se l'impostazione è su `1`, la devoluzione è abilitata (impostazione predefinita)
  - Se l'impostazione è su `0`, la devoluzione è disabilitata
- **`System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel`**
  - Senza impostazione, usa il livello di 2 (impostazione predefinita)
  - Se l'impostazione è su `3` o superiore, usa il valore per impostare il livello

Quando si disabilita la devoluzione o si modificano le impostazioni di devoluzione a un livello superiore, la chiave di registro `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` contiene ancora i suffissi aggiunti in precedenza. Non vengono rimossi automaticamente. Puoi aggiornare manualmente l'elenco oppure puoi cancellarlo e lasciare che l'agente si occupi della procedura per configurare il nuovo elenco.

> **Note**
>
> Per cancellare l'elenco dei suffissi DNS dal registro, puoi eseguire il seguente comando.
>
> ```
> PS C:\> Invoke-CimMethod -ClassName Win32_NetworkAdapterConfiguration -
> MethodName "SetDNSSuffixSearchOrder" -Arguments @{ DNSDomainSuffixSearchOrder =
>  $null } | Out-Null
> ```

Esempi di devoluzione

Gli esempi seguenti mostrano la progressione dei nomi di dominio attraverso il processo di devoluzione.

`corp.example.com`

- Passa a `example.com`

`locale.region.corp.example.com`

1. Passa a `region.corp.example.com`
2. Passa a `corp.example.com`
3. Passa a `example.com`

`locale.region.corp.example.com` con un'impostazione di `DomainNameDevolutionLevel=3`

1. Passa a `region.corp.example.com`
2. Passa a `corp.example.com`. La progressione si interrompe qui, a causa dell'impostazione del livello.

Sottoscrizione alle notifiche dell'agente di avvio EC2 Windows

Amazon SNS può avvisarti in caso di pubblicazione di nuove versioni degli agenti di avvio EC2. Utilizza la procedura seguente per effettuare l'iscrizione a queste notifiche.

Effettua la sottoscrizione alle notifiche EC2Config

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.

2. Nella barra di navigazione modifica la regione in Stati Uniti orientali (Virginia settentrionale), se necessario. Devi selezionare questa regione perché le notifiche SNS per le quali hai effettuato l'iscrizione sono state create in questa regione.
3. Nel riquadro di navigazione, seleziona Sottoscrizioni.
4. Scegli Crea sottoscrizione.
5. Nella finestra di dialogo Crea sottoscrizione segui questi passaggi:
   a. Per ARN argomento, usa il seguente nome della risorsa Amazon (ARN) che corrisponde all'agente per il quale desideri ricevere le notifiche:
      - EC2Launch v2:

        ```
        arn:aws:sns:us-east-1:309726204594:amazon-ec2launch-v2
        ```

      - EC2Launch o EC2Config:

        ```
        arn:aws:sns:us-east-1:801119661308:ec2-windows-ec2config
        ```

   b. In Protocol (Protocollo), seleziona `Email`.
   c. Per Endpoint, inserisci l'indirizzo e-mail in cui vuoi ricevere le notifiche.
   d. Scegli Create Subscription (Crea sottoscrizione).
6. Riceverai un'e-mail in cui ti verrà chiesto di confermare l'iscrizione. Apri l'e-mail e segui le istruzioni per completare l'iscrizione.

Quando esce una nuova versione dell'agente di avvio, inviamo notifiche agli iscritti. Se non desideri più ricevere queste notifiche, segui la procedura seguente per annullare la sottoscrizione.

Annulla la sottoscrizione alle notifiche dell'agente di avvio

1. Aprire la console Amazon SNS.
2. Nel riquadro di navigazione scegli Subscriptions (Sottoscrizioni).
3. Selezionare la sottoscrizione e quindi scegliere Actions (Operazioni), Delete subscriptions (Cancella sottoscrizioni). Quando viene richiesta la conferma, seleziona Elimina.

Amministrazione dei servizi Windows per gli agenti EC2Launch v2 ed EC2Config

Se hai effettuato l'accesso alla tua istanza come utente con diritti amministrativi, puoi gestire gli agenti di avvio EC2Launch v2 ed EC2Config esattamente come faresti con qualsiasi altro servizio Windows. EC2Launch v1 è un set di PowerShell script gestito tramite un'attività pianificata per impostazione predefinita. Questa sezione tratta l'amministrazione dei servizi per EC2Launch v2 ed EC2Config.

Per applicare le impostazioni aggiornate all'istanza, puoi arrestare e riavviare l'agente EC2Launch v2 o l'agente di avvio del servizio EC2Config dall'interfaccia Microsoft Management Console (MMC) per i servizi. Analogamente, quando si installa una nuova versione dell'agente di avvio, devi prima arrestare l'agente, quindi riavviarlo al termine dell'installazione.

> **Note**
>
> Devi aprire l'interfaccia di MMC Services come amministratore per selezionare queste operazioni. A tale scopo, puoi selezionare Esegui come amministratore dal menu contestuale. In alternativa, per aprire l'interfaccia utilizzando la tastiera, procedi come indicato di seguito:
>
> 1. Utilizzando i tasti `Tab` o i tasti freccia, seleziona la voce di menu Servizi dal menu Strumenti di amministrazione.
> 2. Utilizza la seguente combinazione da tastiera per aprirla come amministratore: `Ctrl` + `Shift` +`Enter`.

Le seguenti procedure elencano i passaggi per arrestare e avviare l'agente di avvio sull'istanza.

Arresta l'agente di avvio

1. Avviare l'istanza Windows e connettersi a essa.
2. Seleziona Strumenti di amministrazione dal menu Start di Windows.
3. Apri la console Servizi come amministratore, come descritto all'inizio di questa sezione.
4. Nell'elenco dei servizi, seleziona l'agente in esecuzione sull'istanza (EC2Launch o EC2Config), poi scegli Interrompi dal menu Operazioni. In alternativa, puoi utilizzare il menu contestuale per arrestare l'agente.

Riavvia l'agente di avvio

1. Avviare l'istanza Windows e connettersi a essa.
2. Seleziona Strumenti di amministrazione dal menu Start di Windows.
3. Apri la console Servizi come amministratore, come descritto all'inizio di questa sezione.
4. Nell'elenco dei servizi, seleziona l'agente in esecuzione sull'istanza (EC2Launch o EC2Config), poi scegli Avvia o Riavvia dal menu Operazioni. In alternativa, puoi utilizzare il menu contestuale per riavviare l'agente.

Se non devi aggiornare le impostazioni di configurazione, creare le tue AMI o utilizzare AWS Systems Manager, puoi eliminare e disinstallare l'agente di avvio.

Elimina

L'eliminazione di un servizio rimuove le sottochiavi del registro.

Disinstallazione

La disinstallazione di un servizio rimuove i file, le sottochiavi del registro e tutti i tasti di scelta rapida del servizio.

Elimina l'agente di avvio

1. Avviare l'istanza Windows e connettersi a essa.
2. Avvia una finestra del Prompt dei comandi di Windows.
3. Esegui uno dei seguenti comandi per eliminare l'agente di avvio.
   - Esegui il seguente comando per eliminare EC2Launch o EC2Launch v2:

     ```
     sc delete ec2launch
     ```
   - Esegui il seguente comando per eliminare il servizio EC2Config:

     ```
     sc delete ec2config
     ```

Disinstalla l'agente di avvio

1. Avviare l'istanza Windows e connettersi a essa.

2. Scegli Sistema Windows, poi Pannello di controllo dal menu Start di Windows.
3. Scegli Programmi e funzionalità per aprire l'elenco dei programmi installati sull'istanza.
4. Seleziona il tuo agente di lancio dall'elenco (Amazon EC2Launch o EC2ConfigService), quindi scegli Disinstalla dal menu File. In alternativa, puoi utilizzare il menu contestuale.

> **Note**
>
> Puoi vedere quale versione dell'agente di avvio è installata nella colonna Versione.

Utilizza l'agente EC2Launch v2 per eseguire attività durante l'avvio dell'istanza EC2 Windows

Tutte le istanze supportate di Amazon EC2 avviate dalle AMI AWS Windows Server 2022 e Windows Server 2025 includono l'agente di avvio EC2Launch v2 () per impostazione predefinita. `EC2Launch.exe` Forniamo inoltre le AMI di Windows Server 2016 e 2019 con EC2Launch v2 installato come agente di avvio di default. Queste AMI sono fornite in aggiunta alle AMI di Windows Server 2016 e 2019 che includono EC2Launch v1. È possibile cercare le AMI di Windows che includono EC2Launch v2 di default inserendo il seguente prefisso nella ricerca dalla pagina AMI nella console Amazon EC2: `EC2LaunchV2-Windows_Server-*`.

Per confrontare le funzionalità della versione dell'agente di avvio, consulta. Confronto degli agenti di avvio Amazon EC2

EC2Launch v2 esegue attività durante il startup dell'istanza e viene eseguito se un'istanza viene arrestata e successivamente avviata o se viene riavviata. EC2Launch v2 può anche eseguire attività on demand. Alcune di queste attività sono abilitate automaticamente, mentre altre devono essere abilitate manualmente. Il servizio EC2Launch v2 supporta tutte le caratteristiche di EC2Config ed EC2Launch.

Questo servizio utilizza un file di configurazione per controllarne il funzionamento. Puoi aggiornare il file di configurazione utilizzando uno strumento grafico o modificandolo direttamente come un singolo file .yml (`agent-config.yml`). Per ulteriori informazioni sulle posizioni dei file, consulta Struttura della directory di EC2Launch v2.

EC2Launch v2 pubblica i log di eventi di Windows per facilitare la risoluzione degli errori e l'impostazione dei trigger. Per ulteriori informazioni, consulta Log di eventi di Windows.

Versioni supportate del sistema operativo

L'agente EC2Launch v2 supporta le seguenti versioni del sistema operativo (OS) Windows Server:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019 (canale e canale di manutenzione) Long-Term Semi-Annual
- Windows Server 2016

Attività che vengono eseguite per impostazione predefinita

L'agente EC2Launch v2 esegue le seguenti attività una sola volta per impostazione predefinita durante l'avvio dell'istanza iniziale. Le attività vengono organizzate in base all'ordine in cui vengono eseguite nella fase di avvio.

Fase di `Boot`

- estendere RootPartition

Fase di `PreReady`

- activateWindows
- impostare DnsSuffix
- set AdminAccount
- setWallpaper

Fase di `PostReady`

- startSsm

Concetti di EC2Launch v2

I seguenti concetti sono utili per capire quando utilizzare EC2Launch v2.

agent-config

`agent-config` è un file che si trova nella cartella di configurazione per EC2Launch v2. Include la configurazione per l'avvio, la rete e le fasi. PreReady PostReady Questo file viene utilizzato per

specificare la configurazione di un'istanza per le attività che devono essere eseguite quando l'AMI viene avviata per la prima volta o per le volte successive.

Di default, l'installazione di EC2Launch v2 installa un file `agent-config` che include le configurazioni consigliate utilizzate nelle AMI standard di Amazon Windows. Puoi aggiornare il file di configurazione per modificare l'esperienza di avvio predefinita per l'AMI specificata da EC2Launch v2. Per ulteriori informazioni sulle posizioni dei file, consulta Struttura della directory di EC2Launch v2.

Frequency (Frequenza)

La frequenza delle attività stabilisce quando le attività devono essere eseguite a seconda del contesto di avvio. La maggior parte delle attività ha una sola frequenza consentita. È possibile specificare una frequenza per le attività `executeScript`.

Vedrai le seguenti frequenze nella Configurazione dell'attività di EC2Launch v2.

- Una volta: l'attività viene eseguita una volta, quando l'AMI viene avviata per la prima volta (Sysprep terminato).
- Sempre: l'attività viene eseguita ogni volta che viene attivato l'agente di avvio. L'agente di avvio viene eseguito quando:
  - un'istanza viene avviata o riavviata
  - viene eseguito il servizio EC2Launch
  - viene richiamato `EC2Launch.exe run`

Fase

Una fase è un raggruppamento logico di attività eseguito dall'agente EC2Launch v2. Alcune attività possono essere eseguite solo in una fase specifica. Altre possono essere eseguite in più fasi. Quando utilizzi `agent-config.yml`, è necessario specificare un elenco di fasi e un elenco di attività da eseguire all'interno di ciascuna fase.

Il servizio esegue le fasi nel seguente ordine:

Fase 1: Avvio

Fase 2: Rete

Fase 3: PreReady

Windows è pronto

Al termine della PreReady fase, il servizio invia il `Windows is ready` messaggio alla console Amazon EC2.

Fase 4: PostReady

I dati dell'utente vengono eseguiti durante la PostReady fase. Alcune versioni dello script vengono eseguite prima della PostReady fase del `agent-config.yml` file e altre dopo, come segue:

Prima di `agent-config.yml`

- Versione 1.1 dei dati utente in YAML
- Dati utente XML

Dopo di `agent-config.yml`

- Dati utente YAML versione 1.0 (versione legacy per compatibilità con le versioni precedenti)

Per le fasi e attività di esempio, consulta Esempio: `agent-config.yml`.

Quando utilizzi i dati utente, devi specificare un elenco di attività per l'esecuzione dell'agente di avvio. La fase è implicita. Per le attività di esempio, consulta Esempio: dati utente.

EC2Launch v2 esegue l'elenco delle attività nell'ordine specificato in `agent-config.yml` e nei dati utente. Le fasi vengono eseguite in sequenza. La fase successiva inizia dopo il completamento della fase precedente. Anche le attività vengono eseguite in sequenza.

Attività

Puoi richiamare un'attività per eseguire un'operazione su un'istanza. Puoi configurare le attività nel file `agent-config.yml` o tramite i dati utente. Per un elenco delle attività disponibili per EC2Launch v2, consulta Attività EC2Launch v2. Per lo schema di configurazione delle attività e informazioni dettagliate, consulta Configurazione dell'attività di EC2Launch v2.

Dati utente

I dati utente sono dati configurabili quando si avvia un'istanza. Puoi aggiornare i dati utente per modificare dinamicamente la modalità di configurazione delle AMI personalizzate o delle AMI di avvio rapido. EC2Launch v2 supporta una lunghezza di input dei dati utente di 60 kB. I dati utente includono solo la UserData fase e quindi vengono eseguiti dopo il `agent-config` file. È possibile immettere i dati utente quando si avvia un'istanza utilizzando la procedura guidata di

avvio dell'istanza, oppure è possibile modificare i dati utente dalla console EC2. Per informazioni sull'utilizzo dei dati utente, consulta In che modo Amazon EC2 gestisce i dati utente per le istanze Windows.

Panoramica delle attività di EC2Launch v2

EC2Launch v2 può eseguire ad ogni avvio le seguenti attività:

- Impostare un nuovo sfondo personalizzato e facoltativo che esegue il rendering delle informazioni riguardanti l'istanza.
- Impostare gli attributi per l'account amministratore creato nel computer locale.
- Aggiungere i suffissi DNS all'elenco dei suffissi di ricerca. All'elenco vengono aggiunti solo i suffissi che non esistono già.
- Impostare le lettere di unità per eventuali volumi aggiuntivi ed estenderli per utilizzare lo spazio disponibile.
- Scrivi i file dalla configurazione sul disco.
- Esegui gli script specificati nel file di configurazione EC2Launch v2 o da `user-data`. Gli script da `user-data` possono essere in testo semplice o compressi e forniti in formato base64.
- Eseguire un programma con argomenti specificati.
- Impostare il nome del computer.
- Inviare le informazioni sull'istanza alla console Amazon EC2.
- Inviare l'impronta del certificato RDP alla console Amazon EC2.
- Estendere in modo dinamico la partizione del sistema operativo per includere qualsiasi spazio non partizionato.
- Eseguire i dati utente. Per ulteriori informazioni sulla specifica dei dati utente, consulta Configurazione dell'attività di EC2Launch v2.
- Imposta istradamenti statici non persistenti per raggiungere il servizio metadati e i server AWS KMS .
- Impostare le partizioni non di avvio su `mbr` o `gpt`.
- Avviare il servizio Systems Manager dopo Sysprep.
- Ottimizzare le impostazioni ENA.
- Abilitare OpenSSH per le versioni successive di Windows.
- Abilitare i frame jumbo.

- Impostare Sysprep per l'esecuzione con EC2Launch v2.
- Pubblicare i log di eventi di Windows.

Struttura della directory di EC2Launch v2

EC2Launch v2 deve essere installato nelle seguenti directory:

- Binari del servizio: `%ProgramFiles%\Amazon\EC2Launch`
- Dati del servizio (impostazioni, file di log e file di stato): `%ProgramData%\Amazon\EC2Launch`

> **Note**
>
> Per impostazione predefinita, Windows nasconde i file e le cartelle in `C:\ProgramData`. Per visualizzare le directory e i file di EC2Launch v2 devi digitare il percorso in Esplora risorse di Windows o modificare le proprietà della cartella per visualizzare i file e le cartelle nascosti.

La directory `%ProgramFiles%\Amazon\EC2Launch` contiene binari e librerie di supporto. Include le seguenti sottodirectory:

- `settings`
  - `EC2LaunchSettingsUI.exe`: interfaccia utente per la modifica del file `agent-config.yml`
  - `YamlDotNet.dll`: DLL per supportare alcune operazioni nell'interfaccia utente
- `tools`
  - `ebsnvme-id.exe`: strumento per esaminare i metadati dei volumi EBS nell'istanza
  - `AWSAcpiSpcrReader.exe`: strumento per determinare la porta COM corretta da utilizzare
  - `EC2LaunchEventMessage.dll`: DLL per supportare il log di eventi di Windows per EC2Launch
- `service`
  - `EC2LaunchService.exe`: eseguibile del servizio Windows che viene avviato quando l'agente di avvio viene attivato come servizio
- `EC2AgentTelemetry.dll`: DLL per il supporto della telemetria degli agenti EC2
- `EC2Launch.exe`: eseguibile principale EC2launch
- `EC2LaunchAgentAttribution.txt`: attribuzione per il codice utilizzato in EC2 Launch

La directory `%ProgramData%\Amazon\EC2Launch` contiene le sottodirectory seguenti. Tutti i dati prodotti dal servizio, inclusi i log, la configurazione e lo stato, vengono memorizzati in questa directory.

- `config` – Configurazione

  Il file di configurazione del servizio è memorizzato in questa directory come `agent-config.yml`. Questo file può essere aggiornato per modificare, aggiungere o rimuovere le attività predefinite eseguite dal servizio. L'autorizzazione per creare file in questa directory è limitata all'account di amministratore per evitare l'escalation dei privilegi.

- `log` – Log delle istanze

  I log per il servizio (`agent.log`) e la telemetria (`telemetry.log`) sono memorizzati in questa directory. Quando `agent.log` raggiunge una dimensione di 1 MB, viene ruotato automaticamente e viene creato un file di backup con un formato di timestamp (ad esempio,). `agent-2026-03-02T18-56-39.188.log` Viene mantenuto un solo file di registro di backup alla volta.

- `state` – Dati sullo stato del servizio

  Qui viene memorizzato lo stato utilizzato dal servizio per determinare quali attività devono essere eseguite. Esiste un file `.run-once` che indica se il servizio è già stato eseguito dopo Sysprep (quindi le attività con la frequenza di una volta vengono ignorate all'esecuzione successiva). Questa sottodirectory include `state.json` e `previous-state.json` per tenere traccia dello stato di ogni attività.

- `sysprep` – Sysprep

  Questa directory contiene i file utilizzati per determinare le operazioni eseguite da Sysprep quando crea un'AMI di Windows personalizzata che può essere riutilizzata.

- `wallpaper` – Sfondo

  Queste immagini di sfondo sono memorizzate in questa directory.

Telemetria

La telemetria è un'informazione aggiuntiva che aiuta AWS a comprendere meglio i requisiti, diagnosticare i problemi e fornire funzionalità per migliorare l'esperienza. Servizi AWS

EC2Launch v2 versione `2.1.592` e successive raccolgono dati di telemetria, ad esempio parametri ed errori di utilizzo. Questi dati vengono raccolti dall'istanza Amazon EC2 in cui viene eseguito EC2Launch v2. Sono incluse tutte le AMI Windows di proprietà di. AWS

I seguenti tipi di telemetria vengono raccolti da EC2Launch v2:

- Informazioni di utilizzo: comandi dell'agente, metodo di installazione e frequenza di esecuzione pianificata.
- Errori e informazioni diagnostiche – Codici di errore di installazione dell'agente, esecuzione dei codici di errore e stack di chiamate di errore.

Esempi di dati raccolti dalla versione 2.0.592 alla versione 2.1.1:

```
2025/07/18 22:38:52Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2025/07/18 22:38:52Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AgentCommandErrorCode=0
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AdminPasswordTypeCode=0
2025/07/18 22:38:52Z: EC2LaunchTelemetry: IpConflictDetectionCode=0
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AgentErrorLocation=addroutes.go:49
```

A partire dalla versione 2.2.63, i dati telemetrici dell'agente EC2 sono formattati come oggetto JSON:

```
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2" ... }
```

La telemetria è abilitata per impostazione predefinita. Puoi disabilitare la raccolta dati di telemetria in qualsiasi momento.

Disabilitare la telemetria su un'istanza

Per disattivare la telemetria per una singola istanza, puoi impostare una variabile di ambiente di sistema oppure utilizzare MSI per modificare l'installazione.

Per disattivare la telemetria impostando una variabile di ambiente di sistema, esegui il comando seguente come amministratore.

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Per disabilitare la telemetria utilizzando MSI, esegui il comando seguente dopo il download dell'MSI.

```
msiexec /i ".\AmazonEC2Launch.msi" Remove="Telemetry" /q
```

Altri argomenti per EC2Launch v2

- Installare la versione più recente di EC2Launch v2
- Configurare le impostazioni di EC2Launch v2 per le istanze Windows
- Definizioni delle attività di avvio di EC2Launch v2
- Risoluzione dei problemi relativi all'agente EC2Launch v2
- Cronologie delle versioni EC2Launch v2

Installare la versione più recente di EC2Launch v2

Puoi utilizzare uno dei seguenti metodi per installare l'agente EC2Launch v2 sulla tua istanza EC2:

- Scarica l'agente da Amazon S3 e installalo con Windows PowerShell. Per gli URL dei download, consulta Download di EC2Launch v2 su Amazon S3.
- Installazione con SSM Distributor
- Installazione a partire da un componente di EC2 Image Builder quando si crea un'immagine personalizzata.
- Avvia la tua istanza da un'AMI su cui è preinstallato EC2Launch v2.

> **Warning**
>
> AmazonEC2Launch.msi disinstalla le versioni precedenti dei servizi di avvio EC2, come EC2Launch (v1) ed EC2Config.

Per l'installazione, seleziona la scheda corrispondente al tuo metodo preferito.

PowerShell

Per installare la versione più recente dell'agente EC2Launch v2 con Windows, segui questi passaggi. PowerShell

1. Crea la tua directory locale.

```
New-Item -Path "$env:USERPROFILE\Desktop\EC2Launchv2" -ItemType Directory
```

2. Imposta l'URL per la posizione di download. Esegui il comando seguente con l'URL Amazon S3 che utilizzerai. Per gli URL dei download, consulta Download di EC2Launch v2 su Amazon S3.

```
$Url = "Amazon S3 URL/AmazonEC2Launch.msi"
```

3. Utilizza il seguente comando composito per scaricare l'agente e avviare l'installazione

```
$DownloadFile = "$env:USERPROFILE\Desktop\EC2Launchv2\" + $(Split-Path -Path
 $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadFile
msiexec /i "$DownloadFile"
```

> **Note**
>
> Se ricevi un errore durante il download del file e stai utilizzando Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il tuo terminale. PowerShell Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il comando seguente e riprovare:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. Il comando msiexec installa EC2Launch v2 nella seguente posizione nelle istanze Windows Server `%ProgramFiles%\Amazon\EC2Launch`. Per verificare che l'installazione sia stata eseguita, è possibile verificare il file system locale dell'istanza.

AWS Systems Manager Distributor

Per configurare gli aggiornamenti automatici per EC2Launch v2 con AWS Systems Manager Quick Setup, vedere. Installazione e aggiornamento automatici con Configurazione rapida di Distributor

È anche possibile eseguire un'installazione una tantum del pacchetto `AWSEC2Launch-Agent` da AWS Systems Manager Distributor. Per istruzioni su come installare un pacchetto da System Manager Distributor, consulta Installazione o pacchetti di aggiornamento nella AWS Systems Manager Guida per l'utente.

EC2 Image Builder component

Quando si costruisce un'immagine personalizzata con EC2 Image Builder, è possibile installare il componente `ec2launch-v2-windows`. Per istruzioni su come creare un'immagine personalizzata con EC2 Image Builder, vedi Creazione di una pipeline di immagini utilizzando la procedura guidata della console EC2 Image Builder nellaGuida per l'utente di EC2 Image Builder.

AMI

Per impostazione predefinita, EC2Launch v2 è preinstallato sulle AMI per i sistemi operativi Windows Server 2022 e successivi:

- Windows_Server-*version*-English-Full-Base
- Windows_Server-*version*-English-Core-Base
- Windows_Server- - _Ottimizzato *version* English-Core-EKS
- *version*AMI Windows Server con tutte le altre lingue
- *version*AMI Windows Server con SQL installato

EC2Launch è inoltre preinstallato sulle seguenti AMI Windows Server. Puoi trovare queste AMI dalla console Amazon EC2 oppure utilizzando il seguente prefisso di ricerca `EC2LaunchV2-` nel AWS CLI.

- EC2LaunchV2-Windows_Server-2019-English-Core-Base
- EC2LaunchV2-Windows_Server-2019-English-Full-Base
- EC2LaunchV2-Windows_Server-2016-English-Core-Base
- EC2LaunchV2-Windows_Server-2016-English-Full-Base

Installa e aggiorna automaticamente EC2Launch v2 con AWS Systems Manager Configurazione rapida del distributore

Con AWS Systems Manager Distributor Quick Setup, puoi configurare aggiornamenti automatici per EC2Launch v2. La seguente procedura configura Systems Manager Association sull'istanza affinché aggiorni automaticamente l'agente EC2Launch v2 alla frequenza specificata. L'associazione creata dal Distributor Quick Setup può includere istanze all'interno di una regione Account AWS and o istanze all'interno di un'organizzazione. AWS Per ulteriori informazioni sulla configurazione di un'organizzazione, consultare Tutorial: creazione e configurazione di un'organizzazione nella Guida per l'utente di AWS Organizations .

Prima di iniziare, è necessario assicurarsi che le istanze soddisfino tutti i prerequisiti.

Prerequisiti

Per configurare aggiornamenti automatici con Configurazione rapida di Distributor, le istanze devono soddisfare i seguenti prerequisiti.

- Deve essere presente almeno una istanza in esecuzione che supporta EC2Launch v2. Visualizzare i sistemi operativi supportati per EC2Launch v2.
- Sono state eseguite tutte le attività di configurazione di Systems Manager sulle istanze. Per ulteriori informazioni, consulta Configurazione di Systems Manager nella Guida per l'utente di AWS Systems Manager .
- EC2Launch v2 deve essere l'unico agente di avvio installato sull'istanza. Se è stato installato più di un agente di avvio, la configurazione di Configurazione rapida di Distributor non andrà a buon fine. Prima di configurare EC2Launch v2 con Configurazione rapida Distributor, disinstallare gli agenti di lancio EC2Config o EC2Launch v1, se presenti.

Impostare Configurazione rapida di Distributor per EC2Launch v2

Per creare una configurazione per EC2Launch v2 con Configurazione rapida di Distributor, utilizzare le seguenti impostazioni quando si completa la procedura per l'implementazione del pacchetto Distributor:

- Pacchetti software: agente Amazon EC2Launch v2.
- Frequenza di aggiornamento: selezionare una frequenza dall'elenco.
- Destinazioni: scegliere tra le opzioni di implementazione disponibili.

Per verificare lo stato della configurazione, accedere alla scheda Configurazioni di Configurazione rapida di Systems Manager nella Console di gestione AWS.

1. Apri la console all' AWS Systems Manager indirizzo. https://console.aws.amazon.com/systems-manager/
2. Nel pannello di navigazione, scegli Configurazione rapida.
3. Nella scheda Configurazioni, selezionare la riga associata alla configurazione creata. Nella scheda Configurazioni è presente un elenco delle configurazioni con un riepilogo dei dettagli principali, come Regione, Stato dell'implementazione e Stato associazione.

> **Note**
>
> Il nome dell'associazione per ogni configurazione EC2Launch v2 di Distributor inizia con il seguente prefisso: `AWS-QuickSetup-Distributor-EC2Launch-Agent-`.

4. Per visualizzare i dettagli, selezionare la configurazione e scegliere Visualizza dettagli.

Per ulteriori informazioni e procedure di risoluzione dei problemi, consultare Risoluzione dei problemi dei risultati di Configurazione rapida nella Guida per l'utente di AWS Systems Manager .

Download di EC2Launch v2 su Amazon S3

Per installare la versione più recente di EC2Launch v2, scarica il programma di installazione dai seguenti percorsi:

- https://s3.amazonaws.com/amazon-ec2launch-v2/windows/amd64/latest/AmazonEC2Launch.msi

Configurazione delle opzioni di installazione

Durante l'installazione o l'aggiornamento di EC2Launch v2, puoi configurare le opzioni di installazione con la finestra di installazione di EC2Launch v2 o con il msiexeccomando in una shell a riga di comando.

Alla prima esecuzione su un'istanza di EC2Launch v2, inizializza le impostazioni dell'agente di avvio sull'istanza come segue:

- Crea il percorso locale e vi scrive il file dell'agente di avvio. Questo a volte viene definito come installazione pulita.
- Crea la variabile d'ambiente `EC2LAUNCH_TELEMETRY` se non esiste già e la imposta in base alla tua configurazione.

Per i dettagli della configurazione, seleziona la scheda che corrisponde al metodo di configurazione che utilizzerai.

Amazon EC2Launch Setup dialog

Quando installi o aggiorni EC2Launch v2, puoi configurare le seguenti opzioni di installazione tramite la finestra di dialogo di installazione di EC2Launch v2.

Installazione di base options

Invia telemetria

Se includi questa funzionalità nella finestra di configurazione, l'installatore imposta la `EC2LAUNCH_TELEMETRY` variabile di ambiente con un valore di`1`. Se disabiliti Invia telemetria, l'installatore imposta la variabile di ambiente su un valore di `0`.

Quando l'agente EC2Launch v2 è in esecuzione, legge la`EC2LAUNCH_TELEMETRY` variabile di ambiente per determinare se caricare dati di telemetria. Se il valore è `1`, carica i dati. Altrimenti, non li carica.

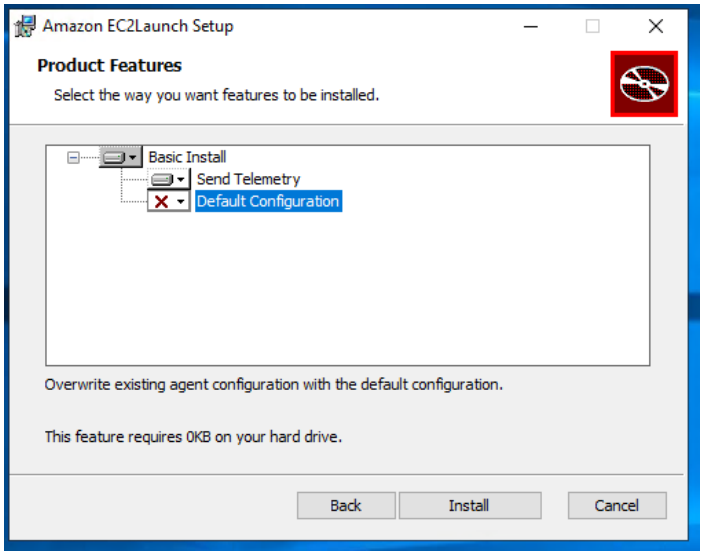
Configurazione di default

La configurazione predefinita per EC2Launch v2 consiste nel sovrascrivere l'agente di avvio locale se già esistente. La prima volta che esegui un'installazione su un'istanza, la configurazione predefinita esegue un'installazione pulita. Se disattivi la configurazione predefinita nell'installazione iniziale, l'installazione non riesce.

Se esegui nuovamente l'installazione sull'istanza, puoi disabilitare la configurazione predefinita per eseguire un aggiornamento che non sostituisca il file `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`.

Esempio: installazione di EC2Launch v2 con telemetria

L'esempio seguente mostra la finestra di configurazione di EC2Launch v2 configurata per aggiornare l'installazione corrente e abilitare la telemetria. Questa configurazione esegue un'installazione senza sostituire il file di configurazione dell'agente e imposta la `EC2LAUNCH_TELEMETRY` variabile di ambiente al valore `1`.



Command line

Quando installi o aggiorni EC2Launch v2, puoi configurare le seguenti opzioni di installazione con il comando msiexec in una shell a riga di comando.

`Valori dei` parametri ADDLOCAL

Base (richiesto)

Installa l'agente di avvio. Se questo valore non è presente nel parametro `ADDLOCAL` l'installazione termina.

Elimina

Quando includi il valore `Clean` nel parametro `ADDLOCAL`, l'installatore scrive il file di configurazione dell'agente nella seguente posizione:`%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`. Se il file di configurazione dell'agente esiste già, lo sovrascrive.

Se lasci il valore `Clean` al di fuori del parametro `ADDLOCAL`, l'installatore esegue un aggiornamento che non sostituisce il file di configurazione dell'agente.

Telemetria

Se includi il valore `Telemetry` nel parametro `ADDLOCAL`, l'installatore imposta la variabile di ambiente `EC2LAUNCH_TELEMETRY` a un valore di `1`.

Se lasci il valore `Telemetry` al di fuori del parametro `ADDLOCAL`, l'installatore imposta la variabile di ambiente a valore di `0`.

Quando l'agente EC2Launch v2 è in esecuzione, legge la`EC2LAUNCH_TELEMETRY` variabile di ambiente per determinare se caricare dati di telemetria. Se il valore è 1, carica i dati. Altrimenti, non li carica.

Esempio: installazione di EC2Launch v2 con telemetria

```
& msiexec /i "C:\Users\Administrator\Desktop\EC2Launchv2\AmazonEC2Launch.msi"
 ADDLOCAL="Basic,Clean,Telemetry" /q
```

Verifica la versione EC2Launch v2

Utilizzare la procedura seguente per verificare la versione di EC2Launch v2 installata sulle istanze.

PowerShell

Verifica la versione installata di EC2Launch v2 con Windows PowerShell, come segue.

1. Lancia un'istanza dall'AMI e connettila.
2. Esegui il seguente comando PowerShell per verificare la versione installata di EC2Launch v2:

```
& "C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" version
```

Windows Control Panel

Verifica la versione installata di EC2Launch v2 nel Pannello di Controllo di Windows come segue:

1. Lancia un'istanza dall'AMI e connettila.
2. Apri il Pannello di Controllo e scegli Programmi e funzionalità.
3. Nella lista dei programmi installati, cerca `Amazon EC2Launch`. Il numero della versione viene mostrato nella colonna Version (Versione).

Per visualizzare gli ultimi aggiornamenti per le AMI AWS Windows, consulta la cronologia delle versioni di Windows AMI nel Windows AMI Reference. AWS

Per la versione più recente di EC2Launch v2, consulta Cronologia delle versioni di EC2Launch v2.

Puoi ricevere notifiche quando vengono rilasciate nuove versioni del servizio EC2Launch v2. Per ulteriori informazioni, consulta Sottoscrizione alle notifiche dell'agente di avvio EC2 Windows.

Configurare le impostazioni di EC2Launch v2 per le istanze Windows

Questa sezione contiene informazioni su come configurare le impostazioni per EC2Launch v2.

Gli argomenti includono:

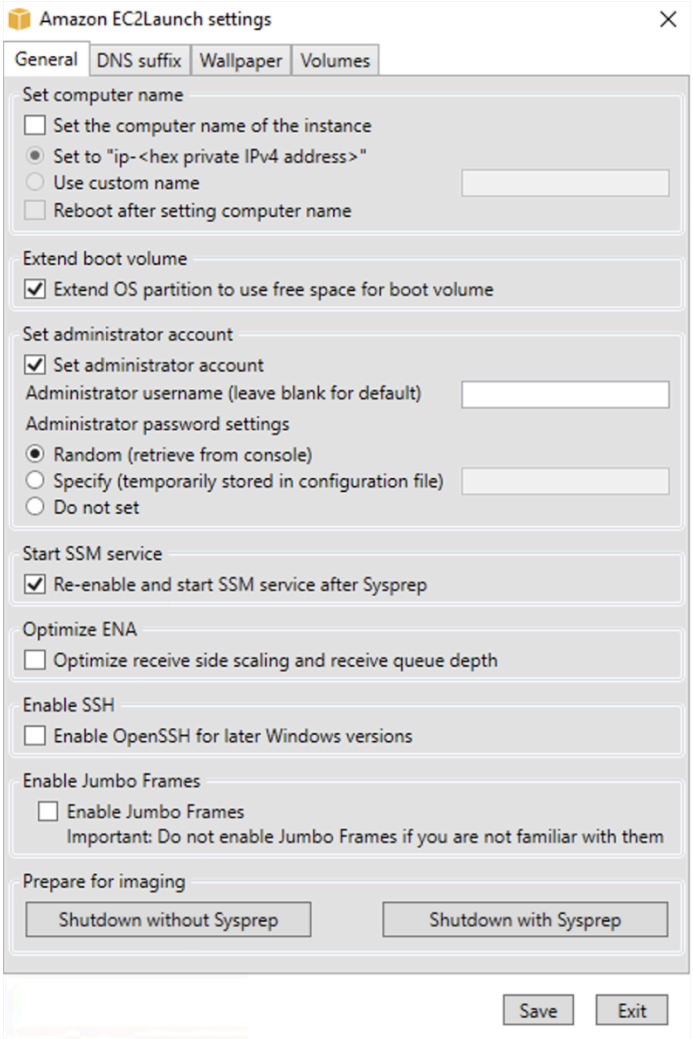
- Modifica delle impostazioni utilizzando la finestra di dialogo delle impostazioni di EC2Launch v2
- Configurare EC2Launch v2 tramite la CLI
- Configurazione dell'attività di EC2Launch v2
- Codici di uscita e riavvii EC2Launch v2
- EC2Launch v2 e Sysprep

Modifica delle impostazioni utilizzando la finestra di dialogo delle impostazioni di EC2Launch v2

La procedura seguente descrive come utilizzare la finestra di dialogo di EC2Launch v2 per abilitare o disabilitare le impostazioni.

> **Note**
>
> Se hai configurato erroneamente delle attività personalizzate nel file agent-config.yml e tenti di aprire la finestra di dialogo delle impostazioni di Amazon EC2Launch, verrà visualizzato un errore. Per un esempio di schema, consulta la sezione Esempio: `agent-config.yml`.

1. Avviare l'istanza Windows e connettersi a essa.
2. Dal menu Start, scegli Tutti i programmi, quindi passa alle impostazioni di EC2Launch. Prima di scegliere Arresta con Sysprep o Arresta senza Sysprep, assicurati di salvare tutte le modifiche che vuoi applicare quando esegui l'arresto.



3. Nella scheda Generale della finestra di dialogo Impostazioni EC2Launch puoi abilitare o disabilitare le seguenti impostazioni.

   a. Set Computer Name (Imposta il nome del computer)

      Se questa impostazione viene abilitata (per impostazione predefinita è disabilitata), il nome host attuale viene confrontato con il nome host desiderato ad ogni avvio. Se i nomi host non corrispondono, il nome host viene reimpostato e il sistema si riavvia facoltativamente per acquisire il nuovo nome host. Se non viene specificato un nome host personalizzato, viene generato utilizzando, ad esempio, l'indirizzo IPv4 privato formattato esadecimale `ip-AC1F4E6`. Per evitare che il nome host esistente venga modificato, non abilitare questa impostazione.

   b. Estendi volume di avvio

Questa impostazione estende in modo dinamico `Disk 0/Volume 0` per includere qualsiasi spazio non partizionato. Ciò può essere utile quando l'istanza viene avviata da un volume root di dimensioni personalizzate.

c. Imposta account amministratore

Se abilitata, puoi impostare gli attributi di nome utente e password per l'account amministratore creato nel computer locale. Se questa caratteristica non è abilitata, non viene creato un account amministratore nel sistema dopo Sysprep. Fornire una password in `adminPassword` solo se `adminPasswordtype` è `Specify`.

I tipi di password sono definiti come segue:

i. `Random`

EC2Launch genera una password e la crittografa utilizzando la chiave dell'utente. Il sistema disattiva questa impostazione dopo l'avvio dell'istanza in modo che questa password rimanga se l'istanza viene riavviata o arrestata e avviata.

ii. `Specify`

EC2Launch utilizza la password specificata in `adminPassword`. Se la password non soddisfa i requisiti di sistema, EC2Launch genera invece una password casuale. La password viene memorizzata in `agent-config.yml` come testo non crittografato e viene cancellata dopo che Sysprep ha impostato la password amministratore. EC2Launch crittografa la password utilizzando la chiave dell'utente.

iii. `Do not set`

EC2launch utilizza la password specificata nel file unattend.xml. Se non specifichi una password in unattend.xml, l'account amministratore viene disabilitato.

d. Avvia servizio SSM

Se questa opzione è selezionata, il servizio Systems Manager è abilitato per iniziare dopo Sysprep. EC2Config v2 esegue tutte le attività descritte precedentemente, mentre SSM Agent elabora le richieste per le funzionalità di Systems Manager come Run Command e Gestione stato.

Puoi utilizzare Run Command per aggiornare le istanze esistenti al fine di utilizzare la versione più recente del servizio EC2Launch v2 e di SSM Agent. Per ulteriori informazioni,

consulta Update SSM Agent using Run Command nella Guida per l'utente di AWS Systems Manager.

e. Ottimizza ENA

Se selezionate, le impostazioni ENA sono configurate per garantire che le impostazioni ENA Receive Side Scaling e Receive Queue Depth siano ottimizzate per. AWS Per ulteriori informazioni, consulta Configura l'affinità della CPU con Receive Side Scaling.

f. Abilita SSH

Questa impostazione abilita OpenSSH per consentire l'amministrazione remota del sistema per le versioni successive di Windows.

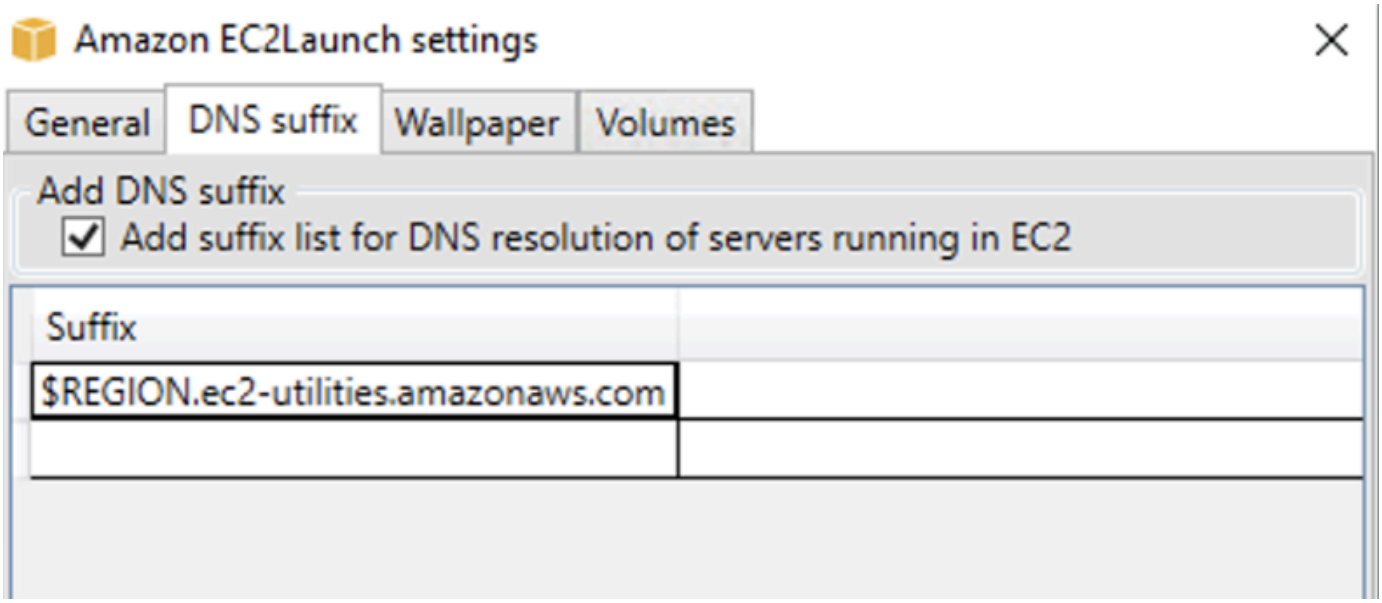
g. Abilita frame jumbo

Seleziona questa opzione per abilitare i frame jumbo. I frame jumbo possono avere effetti indesiderati sulle comunicazioni di rete, quindi assicurati di capire in che modo i frame jumbo influiscono sul tuo sistema prima di attivarli. Per ulteriori informazioni sui frame jumbo, consulta Frame jumbo (9001 MTU).

h. Preparazione per l'imaging

Seleziona questa impostazione se vuoi che l'istanza EC2 venga arrestate con o senza Sysprep. Quando vuoi eseguire Sysprep con EC2Launch v2, scegli Arresto con Sysprep.

4. Nella scheda Suffisso DNS puoi selezionare se aggiungere un elenco di suffissi DNS per la risoluzione DNS dei server in esecuzione in EC2, senza specificare il nome di dominio completo. I suffissi DNS possono contenere le variabili `$REGION` e `$AZ`. All'elenco vengono aggiunti solo i suffissi che non sono già presenti.

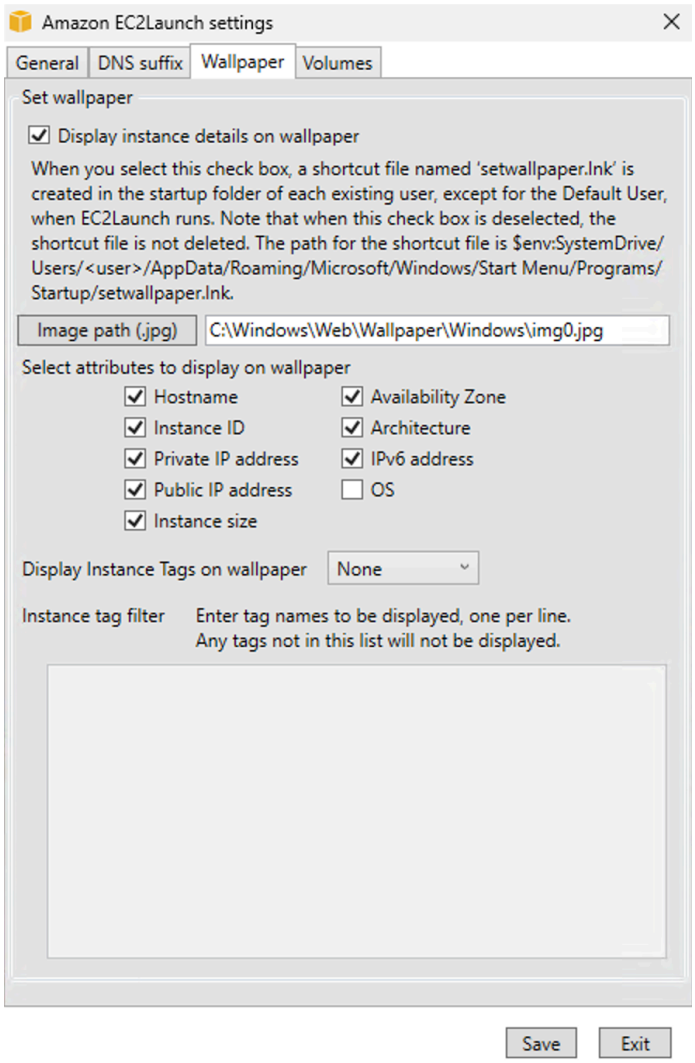


5. Nella scheda Sfondo, puoi configurare lo sfondo dell'istanza con un'immagine di sfondo e specificare i dettagli dell'istanza per lo sfondo da visualizzare. Amazon EC2 genera i dettagli ogni volta che effettui l'accesso.

   È possibile configurare lo sfondo con i seguenti comandi.

   - Mostra i dettagli dell'istanza sullo sfondo: questa casella di controllo attiva o disattiva la visualizzazione dei dettagli dell'istanza sullo sfondo.
   - Percorso dell'immagine (.jpg): specifica il percorso dell'immagine da utilizzare come sfondo.
   - Seleziona gli attributi da visualizzare sullo sfondo: seleziona le caselle di controllo relative ai dettagli dell'istanza che desideri visualizzare sullo sfondo. Deseleziona le caselle di controllo dei dettagli dell'istanza selezionati in precedenza che desideri rimuovere dallo sfondo.
   - Visualizza i tag delle istanze sullo sfondo: seleziona una delle seguenti impostazioni per visualizzare i tag delle istanze sullo sfondo:
     - Nessuno: non visualizzare alcun tag delle istanze sullo sfondo.
     - Mostra tutti: visualizza tutti i tag delle istanze sullo sfondo.
     - Mostra filtrati: visualizza i tag delle istanze specificati sullo sfondo. Quando selezioni questa impostazione, puoi aggiungere i tag delle istanze che desideri visualizzare sullo sfondo nella casella del Filtro dei tag delle istanze.

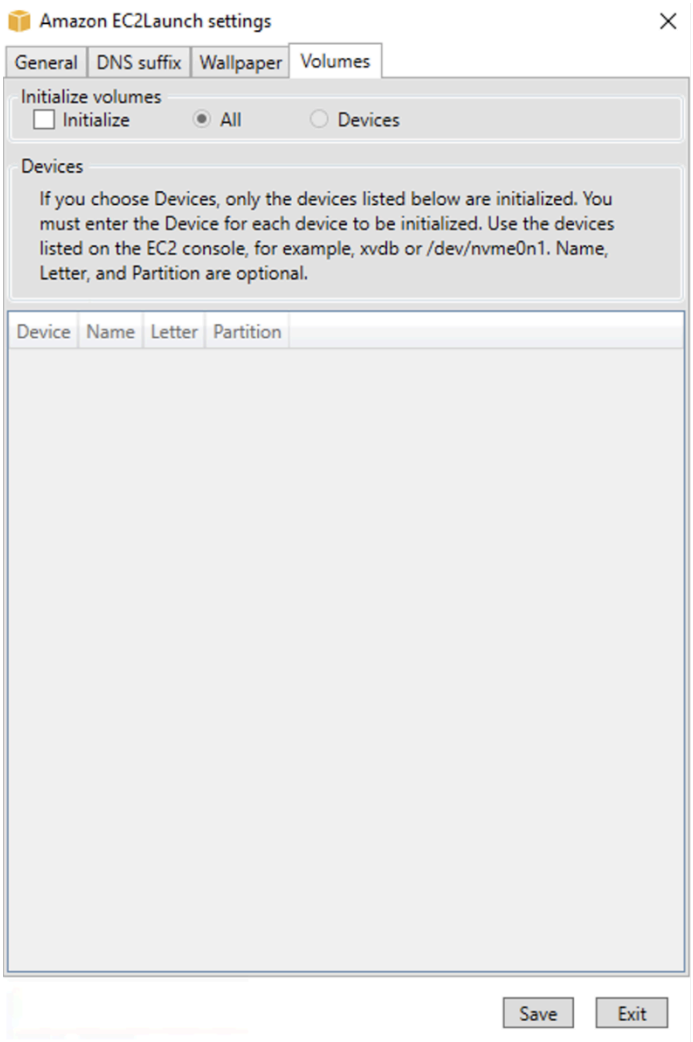
> **Note**
>
> È necessario abilitare i tag nei metadati per mostrare i tag sullo sfondo. Per ulteriori informazioni sui tag e metadati delle istanze, consulta Visualizza i tag per le istanze EC2 utilizzando i metadati dell'istanza.



6. Nella scheda Volumi seleziona se vuoi inizializzare i volumi collegati all'istanza. L'abilitazione imposta le lettere di unità per eventuali volumi aggiuntivi e li estende per utilizzare lo spazio disponibile. Se si seleziona All (Tutto) vengono inizializzati tutti i volumi di archiviazione. Se selezioni Dispositivi vengono inizializzati solo i dispositivi specificati nell'elenco. Devi specificare immettere il dispositivo per ogni dispositivo da inizializzare. Utilizza i dispositivi elencati sulla console EC2, ad esempio, `xvdb` o `/dev/nvme0n1`. Nell'elenco a discesa vengono visualizzati i

volumi di archiviazione collegati all'istanza. Per immettere un dispositivo non collegato all'istanza, immetterlo nel campo di testo.

Nome, Lettera e Partizione sono campi facoltativi. Se per Partizione non viene specificato alcun valore, i volumi di archiviazione superiori a 2 TB vengono inizializzati con il tipo di partizione `gpt` e quelli inferiori a 2 TB vengono inizializzati con il tipo di partizione `mbr`. Se i dispositivi sono configurati e un dispositivo non NTFS contiene una tabella di partizione o i primi 4 KB del disco contengono dati, il disco viene ignorato e l'operazione viene registrata.



Configurare EC2Launch v2 tramite la CLI

Puoi utilizzare l'interfaccia a riga di comando (CLI) per configurare le impostazioni di EC2Launch e gestire il servizio. La sezione seguente contiene le descrizioni e le informazioni sull'utilizzo dei comandi CLI che puoi usare per gestire EC2Launch v2.

> **Note**
>
> L'eseguibile CLI EC2Launch v2,, risiede in. `EC2Launch.exe` `C:\Program Files\Amazon\EC2Launch\` Per impostazione predefinita, questa directory non si trova nel PATH di Windows. La `ec2launch` *`command`* forma mostrata negli esempi di questa sezione è un'abbreviazione che una shell non riconosce direttamente. Per eseguire un comando, utilizzate il percorso completo dell'eseguibile o modificate prima la directory di installazione. L' PowerShell esempio seguente utilizza il percorso completo con l'operatore di chiamata:
>
> ```
> & "C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" status
> ```

Comandi

- collect-logs
- get-agent-config
- list-volumes
- reset
- run
- status
- sysprep
- validate
- version
- wallpaper

collect-logs

Raccoglie i file di log per EC2launch, comprime i file e li inserisce in una directory specificata.

Esempio

```
ec2launch collect-logs -o C:\Mylogs.zip
```

Utilizzo

```
ec2launch collect-logs [flags]
```

Flag

`-h, --help`

aiuto per `collect-logs`

`-o, --output string`

percorso dei file di log di output compressi

get-agent-config

Stampa `agent-config.yml` nel formato specificato (JSON o YAML). Se non viene specificato alcun formato, `agent-config.yml` viene stampato nel formato specificato in precedenza.

Esempio

```
ec2launch get-agent-config -f json
```

Utilizzo

`ec2launch get-agent-config [flags]`

Flag

`-h, --help`

aiuto per `get-agent-config`

`-f, --format string`

formato di output del file `agent-config`: `json`, `yaml`

list-volumes

Elenca tutti i volumi di archiviazione collegati all'istanza, inclusi i volumi temporanei ed EBS.

Esempio

```
ec2launch list-volumes
```

Utilizzo

`ec2launch list-volumes`

Flag

`-h, --help`

aiuto per `list-volumes`

reset

L'obiettivo principale di questa attività è reimpostare l'agente per la prossima esecuzione. A tale scopo, il comando reset elimina tutti i dati sullo stato dell'agente per EC2Launch v2 dalla directory `EC2Launch` locale (consultare Struttura della directory di EC2Launch v2). Il ripristino elimina facoltativamente i log di servizio e Sysprep.

Il comportamento degli script dipende dalla modalità in cui l'agente esegue gli script: in linea o distaccati.

In linea (impostazione predefinita)

L'agente EC2Launch v2 esegue gli script uno alla volta (`detach: false`). Questa è l'impostazione predefinita.

> **Note**
>
> Quando lo script in linea emette un comando reset o sysprep, viene eseguito immediatamente e reimposta l'agente. L'attività corrente termina, quindi l'agente si spegne senza eseguire altre attività.
> Ad esempio, se l'attività che emette il comando fosse stata seguita da un'attività `startSsm` (inclusa per impostazione predefinita dopo l'esecuzione dei dati utente), l'attività non viene eseguita e il servizio Systems Manager non viene mai avviato.

Distaccato

L'agente EC2Launch v2 esegue gli script contemporaneamente ad altre attività (`detach: true`).

> **Note**
>
> Quando lo script distaccato emette un comando reset o sysprep, tali comandi attendono che l'agente finisca prima di procedere all'esecuzione. Le attività successive all'ExecuteScript continueranno a essere eseguite.

Esempio

```
ec2launch reset -c
```

Utilizzo

`ec2launch reset [flags]`

Flag

`-c`, `--clean`

pulisce i log delle istanze prima di `reset`

`-h`, `--help`

aiuto per `reset`

run

Esecuzioni di EC2Launch v2

Esempio

```
ec2launch run
```

Utilizzo

`ec2launch run [flags]`

Flag

`-h`, `--help`

aiuto per `run`

status

Ottiene lo stato dell'agente EC2Launch v2. Blocca facoltativamente il processo fino al completamento dell'agente. Il codice di uscita del processo determina lo stato dell'agente:

- `0` — l'agente è stato eseguito e ha avuto successo.
- `1` — l'agente è stato eseguito e non è andato a buon fine.

- 2 — l'agente è ancora in esecuzione.
- 3 — l'agente si trova in uno stato sconosciuto. Lo stato dell'agente non è in esecuzione o è stato interrotto.
- 4 — si è verificato un errore nel tentativo di recuperare lo stato dell'agente.
- 5 — l'agente non è in esecuzione e lo stato dell'ultima esecuzione nota è sconosciuto. Ciò può significare che:
  - sia `state.json` che `previous-state.json` sono stati eliminati.
  - `previous-state.json` è danneggiato.

  Questo è lo stato dell'agente dopo l'esecuzione del comando `reset`.

Esempio:

```
ec2launch status -b
```

> **Note**
>
> Il `status` comando scrive un breve messaggio nella console (ad esempio,`agent ran successfully`). Tuttavia, i valori del codice di uscita del processo elencati in precedenza determinano lo stato dell'agente, non quel messaggio. Per visualizzare il codice di uscita in PowerShell, leggete la variabile `$LASTEXITCODE` automatica dopo aver eseguito il comando, ad esempio:
>
> ```
> & "C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" status; "ExitCode=
> $LASTEXITCODE"
> ```
>
> L'output di `ExitCode=0` indica che l'agente è stato eseguito correttamente.

Utilizzo

`ec2launch status [flags]`

Flag

`-b,--block`

blocca il processo fino al termine dell'esecuzione del'aggente

`-h,--help`

aiuto per `status`

sysprep

L'obiettivo principale di questa attività è reimpostare l'agente per la prossima esecuzione. A tale scopo, il comando sysprep reimposta lo stato dell'agente, aggiorna il file `unattend.xml`, disabilita RDP ed esegue Sysprep.

Il comportamento degli script dipende dalla modalità in cui l'agente esegue gli script: in linea o distaccati.

In linea (impostazione predefinita)

L'agente EC2Launch v2 esegue gli script uno alla volta (`detach: false`). Questa è l'impostazione predefinita.

> **Note**
>
> Quando lo script in linea emette un comando reset o sysprep, viene eseguito immediatamente e reimposta l'agente. L'attività corrente termina, quindi l'agente si spegne senza eseguire altre attività.
> Ad esempio, se l'attività che emette il comando fosse stata seguita da un'attività `startSsm` (inclusa per impostazione predefinita dopo l'esecuzione dei dati utente), l'attività non viene eseguita e il servizio Systems Manager non viene mai avviato.

Distaccato

L'agente EC2Launch v2 esegue gli script contemporaneamente ad altre attività (`detach: true`).

> **Note**
>
> Quando lo script distaccato emette un comando reset o sysprep, tali comandi attendono che l'agente finisca prima di procedere all'esecuzione. Le attività successive all'ExecuteScript continueranno a essere eseguite.

Esempio:

```
ec2launch sysprep
```

Utilizzo

`ec2launch sysprep [flags]`

Flag

`-c,--clean`

pulisce i log delle istanze prima di `sysprep`

`-h,--help`

aiuto per Sysprep

`-s,--shutdown`

arresta l'istanza dopo `sysprep`

validate

Convalida il file `agent-config` `C:\ProgramData\Amazon\EC2Launch\config\agent-config.yml`.

Esempio

```
ec2launch validate
```

Utilizzo

`ec2launch validate [flags]`

Flag

-h , `--help`

aiuto per `validate`

version

Ottiene la versione eseguibile.

Esempio

```
ec2launch version
```

Utilizzo

`ec2launch version [flags]`

Flag

`-h, --help`

aiuto per `version`

wallpaper

Imposta il nuovo sfondo sul percorso dello sfondo fornito (file .jpg) e visualizza i dettagli dell'istanza selezionata.

Sintassi

```
ec2launch wallpaper ^
--path="C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg" ^
--all-tags ^
--
attributes=hostName,instanceId,privateIpAddress,publicIpAddress,ipv6Address,instanceSize,availa
```

Input

Parameters

--allowed-tags [,] ***`tag-name-1 tag-name-n`***

(Facoltativo) Array JSON codificato in Base64 di nomi di tag delle istanze da visualizzare sullo sfondo. Puoi usare questo tag o `--all-tags`, ma non entrambi.

`attribute-string-1`--attributi, ***`attribute-string-n`***

(Facoltativo) Un elenco separato da virgole di stringhe di attributi `wallpaper` per applicare le impostazioni allo sfondo.

[--percorso | -p] ***`path-string`***

(Obbligatorio) Specifica il percorso del file dell'immagine di sfondo `wallpaper`.

Flag

--all-tags

(Facoltativo) Visualizza tutti i tag delle istanze sullo sfondo. Puoi usare questo tag o `--allowed-tags`, ma non entrambi.

[--help | -h]

Visualizza l'assistenza per il comando wallpaper.

Configurazione dell'attività di EC2Launch v2

In questa sezione sono riportati lo schema, le attività, i dettagli e gli esempi di configurazione per `agent-config.yml` e i dati utente.

Attività ed esempi

- Schema: agent-config.yml
- Configurare gli script dei dati utente di EC2Launch v2 che vengono eseguiti durante l'avvio o il riavvio

Schema: agent-config.yml

La struttura del file `agent-config.yml` è riportata di seguito. Nota che un'attività non può essere ripetuta nella stessa fase. Per le proprietà delle attività, consulta le descrizioni delle attività che seguono.

Struttura del documento: agent-config.yml

JSON

```
{
 "version": "1.1",
 "config": [
  {
   "stage": "string",
   "tasks": [
    {
     "task": "string",
     "inputs": {
```

```
      ...
     }
    },
    ...
   ]
  },
  ...
 ]
}
```

YAML

```
version: 1.1
config:
- stage: string
  tasks:
  - task: string
 inputs:
   ...
  ...
...
```

Esempio: **`agent-config.yml`**

Nell'esempio seguente vengono illustrate le impostazioni per il file di configurazione `agent-config.yml`.

```
version: 1.1
config:
- stage: boot
  tasks:
  - task: extendRootPartition
- stage: preReady
  tasks:
  - task: activateWindows
    inputs:
      activation:
        type: amazon
  - task: setDnsSuffix
    inputs:
      suffixes:
      - $REGION.ec2-utilities.amazonaws.com
  - task: setAdminAccount
```

```
    inputs:
      password:
        type: random
  - task: setWallpaper
    inputs:
      path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
      attributes:
      - hostName
      - instanceId
      - privateIpAddress
      - publicIpAddress
      - instanceSize
      - availabilityZone
      - architecture
- stage: postReady
  tasks:
  - task: startSsm
```

Configurare gli script dei dati utente di EC2Launch v2 che vengono eseguiti durante l'avvio o il riavvio

Gli esempi JSON e YAML seguenti mostrano la struttura del documento per i dati utente. Amazon EC2 analizza ogni attività rinominata nell'array `tasks` specificato nel documento. Ogni attività ha il proprio set di proprietà e requisiti. Per informazioni dettagliate, consulta la Definizioni delle attività di avvio di EC2Launch v2.

> **Note**
>
> Un'attività deve essere visualizzata una sola volta nell'array di attività per i dati utente.

Struttura del documento: dati utente

JSON

```
{
 "version": "1.1",
 "tasks": [
  {
   "task": "string",
   "inputs": {
    ...
   },
```

```
  },
  ...
 ]
}
```

YAML

```
version: 1.1
tasks:
- task: string
  inputs:
    ...
...
```

Esempio: dati utente

Per ulteriori informazioni su questi dati utente, vedere In che modo Amazon EC2 gestisce i dati utente per le istanze Windows.

Il seguente esempio di documento YAML mostra PowerShell uno script che EC2Launch v2 esegue come dati utente per creare un file.

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
```

È possibile utilizzare un formato XML per i dati utente compatibile con le versioni precedenti dell'agente di avvio. EC2Launch v2 esegue lo script come attività `executeScript` nella fase `UserData`. Per conformarsi al comportamento di EC2Launch v1 e EC2Config, lo script dei dati utente viene eseguito come processo per impostazione predefinita. attached/inline

Puoi aggiungere tag opzionali per personalizzare la modalità di esecuzione dello script. Ad esempio, per eseguire lo script dei dati utente al riavvio dell'istanza e una volta all'avvio dell'istanza, puoi utilizzare il seguente tag:

`<persist>true</persist>`

Esempio:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

È possibile specificare uno o più argomenti con il tag. PowerShell `<powershellArguments>` Se non viene passato alcun argomento, EC2Launch v2 aggiunge il seguente argomento per impostazione predefinita: `-ExecutionPolicy Unrestricted`.

Esempio:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Per eseguire uno script di dati utente XML come processo distaccato, aggiungi il seguente tag ai dati utente.

`<detach>true</detach>`

Esempio:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

> **Note**
>
> Il tag di distacco non è supportato nei precedenti agenti di avvio.

Log delle modifiche: dati utente

La tabella seguente elenca le modifiche apportate ai dati utente e le confronta con la versione dell'agente EC2Launch v2 applicabile.

Versione dei dati utente	Informazioni	Introdotta in
1.1	• Le attività relative ai dati utente vengono eseguite prima della fase `PostReady` nel file di configurazione dell'agente. • Esegue i dati utente prima di avviare l'agente Systems Manager (stesso comportamento di EC2Launch v1 ed EC2Config).*	EC2Launch v2 versione 2.0.1245
1.0	• Diventerà obsoleta. • Le attività relative ai dati utente vengono eseguite dopo la fase `PostReady` nel file di configurazione dell'agente. Non è compatibile con EC2Launch v1 e versioni precedenti. • Influenzata da una race condition tra l'avvio dell'agente Systems Manager e le attività relative ai dati utente.	EC2Launch v2 versione 2.0.0

* Se utilizzato con il file `agent-config.yml` predefinito.

Codici di uscita e riavvii EC2Launch v2

È possibile utilizzare EC2Launch v2 per definire come i codici di uscita vengono gestiti dagli script. Per impostazione predefinita, il codice di uscita dell'ultimo comando eseguito in uno script viene segnalato come codice di uscita per l'intero script. Ad esempio, se uno script include tre comandi e il primo comando ha esito negativo ma quelli seguenti hanno esito positivo, lo stato di esecuzione viene segnalato come `success` perché il comando finale ha avuto esito positivo.

Se si desidera che uno script riavvii un'istanza, è necessario specificare `exit 3010` nello script, anche quando il riavvio è l'ultimo passo dello script. `exit 3010` indica a EC2Launch v2 di riavviare l'istanza e richiamare nuovamente lo script fino a quando non restituisce un codice di uscita che non

è `3010` o fino a quando non viene raggiunto il numero massimo di riavvii. EC2Launch v2 consente un massimo di 5 riavvii per attività. Se si tenta di riavviare un'istanza da uno script utilizzando un meccanismo diverso, ad esempio `Restart-Computer`, lo stato di esecuzione dello script non sarà coerente. Ad esempio, potrebbe rimanere bloccato in un ciclo di riavvio o non eseguire il riavvio.

Se utilizzi un formato di dati utente XML compatibile con agenti meno recenti, i dati utente potrebbero essere eseguiti più volte di quanto desideri. Per ulteriori informazioni, consulta Il servizio esegue i dati utente più di una volta nella sezione di risoluzione dei problemi.

EC2Launch v2 e Sysprep

Il servizio EC2Launch v2 esegue Sysprep, uno strumento Microsoft che ti permette di creare un'AMI di Windows personalizzata che può essere riutilizzata. Quando EC2Launch v2 chiama Sysprep, utilizza i file contenuti in `%ProgramData%\Amazon\EC2Launch` per determinare quali operazioni eseguire. Puoi modificare questi file indirettamente utilizzando la finestra di dialogo Impostazioni EC2Launch direttamente utilizzando un editor YAML o un editor di testo. Tuttavia esistono alcune impostazioni avanzate che non sono disponibili nella finestra di dialogoImpostazioni EC2Launch, quindi è necessario modificarle direttamente.

Se crei un'AMI da un'istanza dopo l'aggiornamento delle sue impostazioni, le nuove impostazioni vengono applicate a ogni istanza lanciata dalla nuova AMI. Per informazioni sulla creazione di un'AMI, consulta Crea un' EBS-backed AMI Amazon.

Definizioni delle attività di avvio di EC2Launch v2

Ogni attività eseguita da EC2Launch v2 durante il lancio o l'avvio ha il proprio insieme di proprietà e requisiti. I dettagli delle attività includono le impostazioni per l'esecuzione di un'attività (sempre o una sola volta), a quale fase del processo di avvio dell'agente viene eseguito, la sintassi ed esempi di documento YAML. Per ulteriori informazioni, consulta i dettagli delle attività illustrati in questo riferimento.

Attività di EC2Launch v2

- activateWindows
- abilitare JumboFrames
- abilitare OpenSsh
- executeProgram
- executeScript
- estendere RootPartition

- initializeVolume
- optimizeEna
- impostato AdminAccount
- set DnsSuffix
- set HostName
- setWallpaper
- startSsm
- sysprep
- writeFile

activateWindows

Attiva Windows su un set di AWS KMS server. L'attivazione viene ignorata se l'istanza viene rilevata come Bring-Your-Own-License (BYOL).

Frequency - una volta

AllowedStages — `[PreReady]`

Inputs —

`activation`: (mappa)

`type`: (stringa) tipo di attivazione da utilizzare, impostato su `amazon`

Esempio

```
task: activateWindows
  inputs:
    activation:
    type: amazon
```

abilitare JumboFrames

Abilita i frame jumbo che aumentano l'unità di trasmissione massima (MTU) della scheda di rete. Per ulteriori informazioni, consulta Frame jumbo (9001 MTU).

Frequency - sempre

AllowedStages — `[PostReady, UserData]`

Inputs - nessuno

Esempio

```
task: enableJumboFrames
```

abilitare OpenSsh

Abilita Windows OpenSSH e aggiunge la chiave pubblica per l'istanza alla cartella delle chiavi autorizzate.

Frequency - una volta

AllowedStages — `[PreReady, UserData]`

Inputs - nessuno

Esempio

Nell'esempio seguente viene illustrato come abilitare OpenSSH su un'istanza e come aggiungere la chiave pubblica per l'istanza alla cartella delle chiavi autorizzate. Questa configurazione funziona solo su istanze che eseguono Windows Server 2019 e versioni successive.

```
task: enableOpenSsh
```

executeProgram

Esegue uno script con argomenti opzionali e una frequenza specificata.

Fasi: è possibile eseguire l'attività `executeProgram` durante le fasi`PreReady`, `PostReady` e `UserData`.

Frequenza: configurabile, vedere Input.

Input

Questa sezione contiene uno o più programmi per l'esecuzione dell'attività executeProgram (input). Ogni input può includere le seguenti impostazioni configurabili:

frequenza (stringa)

(Obbligatorio) Specifica esattamente uno dei seguenti valori:

- `once`
- `always`

path (stringa)

(Obbligatorio) Il percorso del file per l'eseguibile da eseguire.

argomenti (elenco di stringhe)

(Facoltativo) Un elenco di argomenti separati da virgole da fornire al programma come input.

runAs (stringa)

(Obbligatorio) Deve essere impostato su `localSystem`

Output

Tutte le attività scrivono le voci del file di registro nel file `agent.log`. L'output aggiuntivo dell'attività `executeProgram` viene archiviato separatamente in una cartella denominata dinamicamente, come segue:

`%LocalAppData%\Temp\`*`EC2Launch#########`*`\`*`outputfilename.tmp`*

Il percorso esatto dei file di output è incluso nel file `agent.log`, ad esempio:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\ExecuteProgramInputs.tmp
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

File di output per l'operazione **`ExecuteProgram`**

`ExecuteProgramInputs.tmp`

Contiene il percorso dell'eseguibile e tutti i parametri di input che l'attività `executeProgram` passa durante l'esecuzione.

`Output.tmp`

Contiene l'output di runtime del programma eseguito dall'attività `executeProgram`.

`Err.tmp`

Contiene messaggi di errore di runtime provenienti dal programma eseguito dall'attività `executeProgram`.

Esempi

Gli esempi seguenti mostrano come eseguire un file eseguibile da una directory locale su un'istanza con l'attività `executeProgram`.

Esempio 1: Configurazione dell'eseguibile con un argomento

Questo esempio mostra un'attività `executeProgram` che esegue un eseguibile di installazione in modalità silenziosa.

```
task: executeProgram
  inputs:
    - frequency: always
      path: C:\Users\Administrator\Desktop\setup.exe
      arguments: ['-quiet']
```

Esempio 2: eseguibile VLC con due argomenti

Questo esempio mostra un'attività `executeProgram` che esegue un file eseguibile VLC con due argomenti passati come parametri di input.

```
task: executeProgram
  inputs:
    - frequency: always
      path: C:\vlc-3.0.11-win64.exe
      arguments: ['/L=1033','/S']
      runAs: localSystem
```

executeScript

Esegue uno script con argomenti opzionali e una frequenza specificata. Il comportamento degli script dipende dalla modalità in cui l'agente esegue gli script: in linea o distaccati.

In linea (impostazione predefinita)

L'agente EC2Launch v2 esegue gli script uno alla volta (`detach: false`). Questa è l'impostazione predefinita.

> **Note**
>
> Quando lo script in linea emette un comando reset o sysprep, viene eseguito immediatamente e reimposta l'agente. L'attività corrente termina, quindi l'agente si spegne senza eseguire altre attività.
> Ad esempio, se l'attività che emette il comando fosse stata seguita da un'attività `startSsm` (inclusa per impostazione predefinita dopo l'esecuzione dei dati utente), l'attività non viene eseguita e il servizio Systems Manager non viene mai avviato.

Distaccato

L'agente EC2Launch v2 esegue gli script contemporaneamente ad altre attività (`detach: true`).

> **Note**
>
> Quando lo script distaccato emette un comando reset o sysprep, tali comandi attendono che l'agente finisca prima di procedere all'esecuzione. Le attività successive all'ExecuteScript continueranno a essere eseguite.

Fasi: è possibile eseguire l'attività `executeScript` durante le fasi`PreReady`, `PostReady` e `UserData`.

Frequenza: configurabile, vedere Input.

Input

Questa sezione contiene uno o più script per l'esecuzione dell'attività executeScript (input). Ogni input può includere le seguenti impostazioni configurabili:

frequenza (stringa)

(Obbligatorio) Specifica esattamente uno dei seguenti valori:

- `once`
- `always`

Tipo: stringa

(Obbligatorio) Specifica esattamente uno dei seguenti valori:

- `batch`
- `powershell`

argomenti (elenco di stringhe)

(Facoltativo) Un elenco di argomenti di tipo stringa da passare alla shell (non allo PowerShell script). Questo parametro non è supportato per le attività eseguite su `type: batch`. Se non viene passato alcun argomento, EC2Launch v2 aggiunge il seguente argomento per impostazione predefinita: `-ExecutionPolicy Unrestricted`.

contenuto (stringa)

(Obbligatorio) Contenuto dello script.

runAs (stringa)

(Obbligatorio) Specificare esattamente uno dei seguenti valori:

- `admin`
- `localSystem`

staccare (booleano)

(Facoltativo) L'agente EC2Launch v2 esegue di default gli script uno alla volta (`detach: false`). Per eseguire lo script in concomitanza con altre attività, impostate il valore su`true` (`detach: true`).

> **Note**
>
> I codici di uscita dello script (tra cui `3010`) non hanno effetto quando `detach` è impostato su `true`.

Output

Tutte le attività scrivono le voci del file di registro nel file `agent.log`. L'output aggiuntivo dello script eseguito dall'attività `executeScript` viene archiviato separatamente in una cartella denominata dinamicamente, come segue:

`%LocalAppData%\Temp\`*`EC2Launch#########\outputfilename.ext`*

Il percorso esatto dei file di output è incluso nel file `agent.log`, ad esempio:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\UserScript.ps1
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

File di output per il task **`ExecuteScript`**

`UserScript.`*`ext`*

Contiene lo script eseguito dall'attività `executeScript`. L'estensione del file dipende dal tipo di script specificato nel parametro `type` per l'attività `executeScript`, come segue:

- Se il tipo è`batch`, l'estensione del file è `.bat`.
- Se il tipo è`powershell`, l'estensione del file è `.ps1`.

`Output.tmp`

Contiene l'output di runtime dello script eseguito dall'attività `executeScript`.

`Err.tmp`

Contiene messaggi di errore di runtime provenienti dallo script eseguito dall'attività `executeScript`.

Esempi

Gli esempi seguenti mostrano come eseguire uno script in linea con l'attività `executeScript`.

Esempio 1: file di testo di output Ciao

Questo esempio mostra un'`executeScript`operazione che esegue PowerShell uno script per creare un file di testo «Hello world» sull'`C:`unità.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
      runAs: admin
      content: |-
        New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
```

```
        Set-Content 'C:\PowerShellTest.txt' "Hello world"
```

Esempio 2: eseguire due script

Questo esempio mostra che l'attività `executeScript` può eseguire più di uno script e il tipo di script non deve necessariamente corrispondere.

Il primo script (`type: powershell`) scrive un riepilogo dei processi attualmente in esecuzione sull'istanza in un file di testo che si trova sull'unità `C:`.

Il secondo script (`batch`) scrive le informazioni di sistema nel file `Output.tmp`.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
      runAs: localSystem
      content: |
        Get-Process | Out-File -FilePath C:\Process.txt
    - frequency: always
      type: batch
      runAs: localSystem
      content: |
        systeminfo
```

Esempio 3: configurazione di sistema idempotente con riavvii

Questo esempio mostra un'attività `executeScript` che esegue uno script idempotente per eseguire la seguente configurazione di sistema con un riavvio tra ogni fase:

- Impostare il nome del computer.
- Aggiungere il computer al dominio
- Abilitare Telnet.

Lo script garantisce che ogni operazione venga eseguita una sola volta. Ciò impedisce un ciclo di riavvio e rende lo script idempotente.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
      runAs: localSystem
```

```
      content: |-
        $name = $env:ComputerName
        if ($name -ne $desiredName) {
          Rename-Computer -NewName $desiredName
          exit 3010
        }
        $domain = Get-ADDomain
        if ($domain -ne $desiredDomain)
        {
          Add-Computer -DomainName $desiredDomain
          exit 3010
        }
        $telnet = Get-WindowsFeature -Name Telnet-Client
        if (-not $telnet.Installed)
        {
          Install-WindowsFeature -Name "Telnet-Client"
          exit 3010
        }
```

estendere RootPartition

Estende il volume root per utilizzare tutto lo spazio disponibile sul disco.

Frequency - una volta

AllowedStages — `[Boot]`

Inputs - nessuno

Esempio

```
task: extendRootPartition
```

initializeVolume

Inizializza i volumi vuoti che sono collegati all'istanza in modo che vengano attivati e partizionati. L'agente di avvio salta l'inizializzazione se rileva che il volume non è vuoto. Un volume è considerato vuoto se i primi 4 KiB del volume sono vuoti o se il volume non ha un layout di Windows-recognizable unità.

Il parametro di input `letter` viene sempre applicato quando viene eseguita questa attività, indipendentemente dal fatto che l'unità sia già inizializzata.

L'attività `initializeVolume` effettua le seguenti operazioni.

- Imposta gli attributi del disco `offline` e `readonly` su false.
- Creare una partizione. Se non è specificato alcun tipo di partizione nel parametro di input `partition`, si applicano le seguenti impostazioni predefinite:
  - Se la dimensione del disco è inferiore a 2 TB, imposta il tipo di partizione su `mbr`.
  - Se la dimensione del disco è pari o superiore a 2 TB, imposta il tipo di partizione su `.gpt`.
- Formatta il volume come NTFS.
- Imposta l'etichetta del volume, come indicato di seguito:
  - Utilizza il valore del parametro di input `name`, se specificato.
  - Se il volume è temporaneo e non è stato specificato alcun nome, imposta l'etichetta del volume su `Temporary Storage Z`.
- Se il volume è temporaneo (SSD o HDD, non Amazon EBS), crea un file `Important.txt` nel root del volume con il seguente contenuto:

```
This is an 'Instance Store' disk and is provided at no additional charge.

*This disk offers increased performance since it is local to the host
*The number of Instance Store disks available to an instance vary by instance type
*DATA ON THIS DRIVE WILL BE LOST IN CASES OF IMPAIRMENT OR STOPPING THE INSTANCE.
 PLEASE ENSURE THAT ANY IMPORTANT DATA IS BACKED UP FREQUENTLY

For more information, please refer to: Archivio dell'istanza archiviazione a blocchi
 temporanea per le istanze EC2.
```

- Imposta la lettera dell'unità sul valore specificato nel parametro di input `letter`.

Fasi: è possibile eseguire l'attività `initializeVolume` durante le fasi `PostReady` e `UserData`.

Frequenza: sempre.

Input

È possibile configurare i parametri di runtime come segue:

dispositivi (elenco di mappe)

(Condizionale) Configurazione per ogni dispositivo inizializzato dall'agente di avvio. Questo parametro è obbligatorio quando il parametro di input `initialize` è impostato su `devices`.

- dispositivo (stringa, obbligatorio): identifica il dispositivo durante la creazione dell'istanza. Ad esempio, `xvdb`, `xvdf` o `\dev\nvme0n1`.
- lettera (stringa, facoltativo): un carattere. La lettera dell'unità da assegnare.
- nome (stringa, facoltativo): il nome del volume da assegnare.
- partizione (stringa, facoltativo): specifica uno dei seguenti valori per il tipo di partizione da creare o consenti all'agente di avvio di utilizzare le impostazioni predefinite in base alla dimensione del volume:
  - mbr
  - gpt

inizializza (stringa)

(Obbligatorio) Specificare esattamente uno dei seguenti valori:

- `all`
- `devices`

Esempi

Gli esempi seguenti mostrano esempi di configurazioni di input per l'attività `initializeVolume`.

Esempio 1: inizializzazione di due volumi su un'istanza

Questo esempio mostra un'attività `initializeVolume` che inizializza due volumi secondari su un'istanza. Il dispositivo denominato `DataVolume2` nell'esempio è effimero.

```
task: initializeVolume
inputs:
  initialize: devices
  devices:
  - device: xvdb
    name: DataVolume1
    letter: D
    partition: mbr
  - device: /dev/nvme0n1
    name: DataVolume2
    letter: E
    partition: gpt
```

Esempio 2: inizializzazione dei volumi EBS collegati a un'istanza

Questo esempio mostra un'attività `initializeVolume` che inizializza tutti i volumi EBS vuoti collegati all'istanza.

```
task: initializeVolume
inputs:
  initialize: all
```

optimizeEna

Ottimizza le impostazioni ENA in base al tipo di istanza corrente; l'istanza potrebbe essere riavviata.

Frequency - sempre

AllowedStages — `[PostReady, UserData]`

Inputs - nessuno

Esempio

```
task: optimizeEna
```

impostato AdminAccount

Imposta gli attributi per l'account amministratore predefinito creato nel computer locale.

Frequency - una volta

AllowedStages — `[PreReady]`

Inputs —

`name`: (stringa) nome dell'account amministratore

`password`: (mappa)

`type`: (stringa) strategia per impostare la password come `static`, `random` o `doNothing`

`data`: (stringa) archivia i dati se il campo `type` è statico

Esempio

```
task: setAdminAccount
inputs:
  name: Administrator
  password:
```

```
  type: random
```

set DnsSuffix

Aggiunge suffissi DNS all'elenco dei suffissi di ricerca. All'elenco vengono aggiunti solo i suffissi che non esistono già. Per ulteriori informazioni sul modo in cui gli agenti di lancio impostano i suffissi DNS, consultare Configura il suffisso DNS per gli agenti di avvio EC2 Windows.

Frequency - sempre

AllowedStages — `[PreReady]`

Inputs —

`suffixes`: (elenco di stringhe) elenco di uno o più suffissi DNS validi, le variabili di sostituzione valide sono `$REGION` e `$AZ`

Esempio

```
task: setDnsSuffix
inputs:
  suffixes:
  - $REGION.ec2-utilities.amazonaws.com
```

set HostName

Imposta il nome host del computer su una stringa personalizzata o, se `hostName` non è specificato, sull'indirizzo IPv4 privato.

Frequency - sempre

AllowedStages — `[PostReady, UserData]`

Inputs —

`hostName`: (stringa) nome host facoltativo, che deve essere formattato come segue.

- Deve essere uguale o inferiore a 15 caratteri
- Deve contenere solo caratteri alfanumerici (a-z A-Z, 0-9) e trattini (-).
- Non deve essere costituito interamente da caratteri numerici.

`reboot`: (booleano) indica se è consentito un riavvio quando viene modificato il nome host

Esempio

```
task: setHostName
inputs:
  reboot: true
```

setWallpaper

Crea il file di scorciatoia `setwallpaper.lnk` nella cartella di startup di ciascun utente esistente, eccetto `Default User`. Questo file di scorciatoia viene eseguito quando l'utente accede per la prima volta dopo l'avvio dell'istanza. Imposta l'istanza con uno sfondo personalizzato che visualizzi gli attributi dell'istanza.

Il percorso del file di scorciatoia è:

```
$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/
Startup/setwallpaper.lnk
```

> **Note**
>
> La rimozione dell'attività `setWallpaper` non elimina questo file di scorciatoia. Per ulteriori informazioni, consulta L ' attività SetWallpaper non è abilitata ma lo sfondo viene ripristinato al riavvio.

Fasi: puoi configurare lo sfondo durante le fasi `PreReady` e `UserData`.

Frequenza: `always`

Configurazione dello sfondo

È possibile configurare lo sfondo con le seguenti impostazioni.

Input

Parametri di input che fornisci e attributi che puoi impostare per configurare lo sfondo:

path (stringa)

(Obbligatorio) Il percorso del nome del file immagine in formato.jpg locale da utilizzare per l'immagine di sfondo.

attributi (elenco di stringhe)

(Facoltativo) Puoi aggiungere uno o più dei seguenti attributi allo sfondo:

- `architecture`
- `availabilityZone`
- `hostName`
- `instanceId`
- `instanceSize`
- `privateIpAddress`
- `publicIpAddress`
- `ipv6Address`

instanceTags

(Facoltativo) Per questa impostazione puoi utilizzare esattamente una delle seguenti opzioni.

- AllTags(stringa): aggiunge tutti i tag di istanza allo sfondo.

```
instanceTags: AllTags
```

- instanceTags (elenco di stringhe): specifica un elenco di nomi di tag delle istanze da aggiungere allo sfondo. Ad esempio:

```
instanceTags:
  - Tag 1
  - Tag 2
```

Esempio

L'esempio seguente mostra gli input di configurazione dello sfondo che impostano il percorso del file per l'immagine di sfondo dello sfondo, insieme ai tag delle istanze denominati `Tag 1` e `Tag 2` e agli attributi che includono il nome dell'host, l'ID dell'istanza e gli indirizzi IP privati e pubblici dell'istanza.

```
task: setWallpaper
inputs:
  path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
  attributes:
  - hostName
  - instanceId
```

```
  - privateIpAddress
  - publicIpAddress
  instanceTags:
  - Tag 1
  - Tag 2
```

> **Note**
>
> È necessario abilitare i tag nei metadati per mostrare i tag sullo sfondo. Per ulteriori informazioni sui tag e metadati delle istanze, consulta Visualizza i tag per le istanze EC2 utilizzando i metadati dell'istanza.

startSsm

Avvia il servizio Systems Manager (SSM) dopo Sysprep.

Frequency - sempre

AllowedStages — `[PostReady, UserData]`

Inputs - nessuno

Esempio

```
task: startSsm
```

sysprep

Reimposta lo stato del servizio, aggiorna `unattend.xml`, disabilita RDP ed esegue Sysprep. Questa attività viene eseguita solo dopo che tutte le altre attività sono state completate.

Frequency - una volta

AllowedStages — `[UserData]`

Inputs —

`clean`: (booleano) pulisce i log delle istanze prima di eseguire Sysprep

`shutdown`: (booleano) chiude l'istanza dopo l'esecuzione di Sysprep

Esempio

```
task: sysprep
inputs:
clean: true
shutdown: true
```

writeFile

Scrive un file in una destinazione.

Frequency - vedi Inputs

AllowedStages — `[PostReady, UserData]`

Inputs —

`frequency`: (stringa) `once` o `always`

`destination`: (stringa) percorso in cui scrivere il contenuto

`content`: (stringa) testo da scrivere nella destinazione

Esempio

```
task: writeFile
inputs:
  - frequency: once
  destination: C:\Users\Administrator\Desktop\booted.txt
  content: Windows Has Booted
```

Risoluzione dei problemi relativi all'agente EC2Launch v2

In questa sezione vengono illustrati scenari di risoluzione dei problemi comuni di EC2Launch v2 e informazioni sulla visualizzazione dei log di eventi di Windows, nonché l'output e i messaggi dei log della console.

Argomenti sulla risoluzione dei problemi

- Scenari per la risoluzione dei problemi comuni
- Log di eventi di Windows
- Output del log della console EC2Launch v2

Scenari per la risoluzione dei problemi comuni

In questa sezione vengono illustrati gli scenari di risoluzione dei problemi comuni e le fasi per la risoluzione dei problemi.

Scenari

- Il servizio non riesce a impostare lo sfondo
- Il servizio non riesce a eseguire i dati utente
- Il servizio esegue un'attività una sola volta
- Il servizio non riesce a eseguire un'attività
- Il servizio esegue i dati utente più di una volta
- Le attività pianificate da EC2Launch v1 non vengono eseguite dopo la migrazione a EC2Launch v2
- Il servizio inizializza un volume EBS che non è vuoto
- L'attività SetWallpaper non è abilitata ma lo sfondo viene ripristinato al riavvio
- Servizio bloccato nello stato di esecuzione
- Agent-config.yml non valido impedisce l'apertura della finestra di dialogo delle impostazioni di EC2Launch v2
- Attività: ExecuteScript deve essere univoco e richiamato una sola volta

Il servizio non riesce a impostare lo sfondo

Risoluzione

1. Controlla che `%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\setwallpaper.lnk` esista.
2. Controlla `%ProgramData%\Amazon\EC2Launch\log\agent.log` per vedere se si sono verificati errori.

Il servizio non riesce a eseguire i dati utente

Possibile causa: il servizio potrebbe aver restituito l'esito negativo prima dell'esecuzione dei dati utente.

Risoluzione

1. Controlla `%ProgramData%\Amazon\EC2Launch\state\previous-state.json`.

2. Vedi se `boot`, `network`, `preReady` e `postReadyLocalData` sono stati tutti contrassegnati come completati.
3. Se una delle fasi non è riuscita, controlla `%ProgramData%\Amazon\EC2Launch\log\agent.log` per vedere se si sono verificati errori specifici.

Il servizio esegue un'attività una sola volta

Risoluzione

1. Controlla la frequenza dell'attività.
2. Se il servizio è già stato eseguito dopo Sysprep e la frequenza dell'attività è impostata su `once`, l'attività non verrà eseguita nuovamente.
3. Imposta la frequenza dell'attività su `always` se vuoi che venga eseguita ogni volta che viene eseguito EC2Launch v2.

Il servizio non riesce a eseguire un'attività

Risoluzione

1. Controlla le ultime voci in `%ProgramData%\Amazon\EC2Launch\log\agent.log`.
2. Se non si sono verificati errori, prova a eseguire manualmente il servizio da `"%ProgramFiles%\Amazon\EC2Launch\EC2Launch.exe" run` per verificare se le attività hanno esito positivo.

Il servizio esegue i dati utente più di una volta

Risoluzione

I dati utente vengono gestiti in modo diverso tra EC2Launch v1 e EC2Launch v2. EC2Launch v1 esegue i dati utente come attività pianificata sull'istanza quando `persist` è impostato su `true`. Se `persist` è impostato su `false`, l'attività non viene pianificata anche quando esce con un riavvio o viene interrotta durante l'esecuzione.

EC2Launch v2 esegue i dati utente come attività agente e tiene traccia del relativo stato di esecuzione. Se i dati utente emettono un riavvio del computer o sono stati interrotti durante l'esecuzione, lo stato di esecuzione persiste come `pending` e i dati utente verranno eseguiti nuovamente al successivo avvio dell'istanza. Se si desidera impedire l'esecuzione dello script dei dati utente più di una volta, rendere lo script idempotente.

Lo script idempotente di esempio seguente imposta il nome del computer e si unisce a un dominio.

```
<powershell>
  $name = $env:computername
  if ($name -ne $desiredName) {
 Rename-Computer -NewName $desiredName
  }
  $domain = Get-ADDomain
  if ($domain -ne $desiredDomain)
  {
 Add-Computer -DomainName $desiredDomain
  }
  $telnet = Get-WindowsFeature -Name Telnet-Client
  if (-not $telnet.Installed)
  {
 Install-WindowsFeature -Name "Telnet-Client"
  }
</powershell>
<persist>false</persist>
```

Le attività pianificate da EC2Launch v1 non vengono eseguite dopo la migrazione a EC2Launch v2

Risoluzione

Lo strumento di migrazione non rileva alcuna attività pianificata collegata agli script EC2Launch v1, pertanto non imposta automaticamente tali attività in EC2Launch v2. Per configurare queste attività, modificare il file `agent-config.yml` o utilizzare la finestra di dialogo Impostazioni di EC2Launch v2. Ad esempio, se un'istanza dispone di un'attività pianificata che esegue `InitializeDisks.ps1`, dopo avere eseguito lo strumento di migrazione, è necessario specificare i volumi che si desidera inizializzare nella finestra di dialogo delle impostazioni di EC2Launch v2. Vedere il passaggio 6 della procedura per Modifica delle impostazioni utilizzando la finestra di dialogo delle impostazioni di EC2Launch v2.

Il servizio inizializza un volume EBS che non è vuoto

Risoluzione

Prima di inizializzare un volume, EC2Launch v2 tenta di rilevare se è vuoto. Se un volume non è vuoto, ignora l'inizializzazione. I volumi rilevati come non vuoti non vengono inizializzati. Un volume è considerato vuoto se i primi 4 KiB di un volume sono vuoti o se un volume non ha un layout di Windows-recognizable unità. Un volume inizializzato e formattato su un sistema Linux non ha un

layout di Windows-recognizable unità, ad esempio MBR o GPT. Pertanto, sarà considerato vuoto e inizializzato. Se si desidera conservare questi dati, non fare affidamento sul rilevamento di unità EC2Launch v2 vuote. Specificare invece i volumi che si desidera inizializzare nella finestra di dialogo delle impostazioni di EC2Launch v2 (vedere il passaggio 6) o in `agent-config.yml`.

L' attività SetWallpaper non è abilitata ma lo sfondo viene ripristinato al riavvio

Il processo `setWallpaper` crea il file di scorciatoia `setwallpaper.lnk` nella cartella di startup di ciascun utente esistente. Questo file di scorciatoia viene eseguito quando l'utente accede per la prima volta dopo l'avvio dell'istanza. Imposta l'istanza con uno sfondo personalizzato che visualizzi gli attributi dell'istanza. La rimozione del processo `setWallpaper` non elimina questo file di scorciatoia. È necessario eliminare questo file manualmente o con uno script.

Il percorso del file di scorciatoia è:

`$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk`

Risoluzione

Eliminare questo file manualmente o con uno script.

PowerShell Script di esempio per eliminare un file di scelta rapida

```
foreach ($userDir in (Get-ChildItem "C:\Users" -Force -Directory).FullName)
{
 $startupPath = Join-Path $userDir -ChildPath "AppData\Roaming\Microsoft\Windows\Start
 Menu\Programs\Startup"
 if (Test-Path $startupPath)
 {
  $wallpaperSetupPath = Join-Path $startupPath -ChildPath "setwallpaper.lnk"
  if (Test-Path $wallpaperSetupPath)
  {
   Remove-Item $wallpaperSetupPath -Force -Confirm:$false
  }
 }
}
```

Servizio bloccato nello stato di esecuzione

Descrizione

EC2Launch v2 è bloccato con i messaggi di log (`agent.log`) simili ai seguenti:

```
2022-02-24 08:08:58 Info:
 ********************************************************************************
2022-02-24 08:08:58 Info: EC2Launch Service starting
2022-02-24 08:08:58 Info: Windows event custom log exists: Amazon EC2Launch
2022-02-24 08:08:58 Info: ACPI SPCR table not supported. Bailing Out
2022-02-24 08:08:58 Info: Serial port is in use. Waiting for Serial Port...
2022-02-24 08:09:00 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:02 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:04 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:06 Info: ACPI SPCR table not supported. Use default console port.
```

Possibile causa

SAC è abilitato e utilizza la porta seriale. Per ulteriori informazioni, consulta Utilizzo di SAC per risolvere i problemi relativi all'istanza di Windows.

Risoluzione

Per risolvere il problema, prova a eseguire i seguenti passaggi:

- Disabilita il servizio che utilizza la porta seriale.
- Se desideri che il servizio continui a utilizzare la porta seriale, scrivi degli script personalizzati per eseguire le attività dell'agente di avvio e richiamarle come attività pianificate.

`Agent-config.yml non valido impedisce` l'apertura della finestra di dialogo delle impostazioni di EC2Launch v2

Description

Le impostazioni di EC2Launch v2 tentano di analizzare il file `agent-config.yml` prima dell'apertura della finestra di dialogo. Se il file di configurazione YAML non segue lo schema supportato, nella finestra di dialogo viene visualizzato il seguente errore:

`Unable to parse configuration file agent-config.yml. Review configuration file. Exiting application.`

Risoluzione

1. Verifica che il file di configurazione segua lo schema supportato.

2. Se vuoi iniziare da zero, copia il file di configurazione predefinito in `agent-config.yml`. Puoi utilizzare il plugin di `agent-config.yml` di esempio fornito nella sezione Task Configuration (Configurazione attività).
3. Puoi anche ricominciare da capo eliminando `agent-config.yml`. Le impostazioni di EC2Launch v2 generano un file di configurazione vuoto.

Attività: ExecuteScript deve essere univoco e richiamato una sola volta

Description

Un'attività non può essere ripetuta nella stessa fase.

Risoluzione

Alcune attività devono essere inserite come array, ad esempio executeScript e executeProgram. Per un esempio di come scrivere lo script in forma di array, consulta l'argomento executeScript.

Log di eventi di Windows

EC2Launch v2 pubblica i log di eventi di Windows per gli eventi importanti, ad esempio per l'avvio del servizio, se Windows è pronto o sull'esito positivo o il fallimento delle attività. Gli identificatori di evento identificano in modo univoco un particolare evento. Ogni evento contiene informazioni su fasi, attività e livelli e una descrizione. Puoi impostare i trigger per eventi specifici utilizzando l'identificatore di evento.

Gli ID evento forniscono informazioni su un evento e identificano in modo univoco alcuni eventi. La cifra meno significativa di un ID evento indica la gravità di un evento.

Evento	Cifra meno significativa
`Success`	`. . .0`
`Informational`	`. . .1`
`Warning`	`. . .2`
`Error`	`. . .3`

Service-related gli eventi generati all'avvio o all'arresto del servizio includono un identificatore di evento a una cifra.

Event	Identificatore a una cifra
`Success`	`0`
`Informational`	`1`
`Warning`	`2`
`Error`	`3`

I messaggi di evento per gli eventi `EC2LaunchService.exe` iniziano con `Service:`. I messaggi di evento per gli eventi `EC2Launch.exe` non iniziano con `Service:`.

Gli ID evento a quattro cifre includono informazioni su stadio, attività e gravità di un evento.

Argomenti

- Formato ID evento
- Esempi di ID evento
- Schema dei log di eventi di Windows

Formato ID evento

Nella tabella seguente viene illustrato il formato di un identificatore di evento EC2Launch v2.

3	2 1	0
S	T	L

Le lettere e i numeri nella tabella rappresentano il tipo di evento e le definizioni seguenti.

Tipo di evento	Definizione
S (fase)	0 - messaggio Service-level 1 - Avvio

Tipo di evento	Definizione
	2 - Rete 3 - PreReady 5 - Windows è pronto 6 - PostReady 7 - Dati utente
T (attività)	Le attività rappresentate dai due valori corrispondenti sono diverse per ogni fase. Per visualizzare l'elenco completo degli eventi, consulta lo Schema dei log di eventi di Windows.
L (livello di evento)	0 - Operazione completata 1 - Messaggio informativo 2 - Avvertenza 3 - Errore

Esempi di ID evento

Di seguito sono riportati gli ID evento di esempio.

- `5000` - Windows è pronto per l'uso
- `3010`- L'operazione di attivazione di Windows in PreReady fase è avvenuta con successo
- `6013`- L'attività Imposta sfondo nella fase PostReady Local Data ha riscontrato un errore

Schema dei log di eventi di Windows

MessageId/Event Id	Messaggio di evento
. . .0	Success
. . .1	Informational
. . .2	Warning
. . .3	Error
x	EC2Launch service-level logs
0	EC2Launch service exited successfully
1	EC2Launch service informational logs
2	EC2Launch service warning logs
3	EC2Launch service error logs
10	Replace state.json with previous-state.json
100	Serial Port
200	Sysprep
300	PrimaryNic
400	Metadata
x000	Stage (1 digit), Task (2 digits), Status (1 digit)
1000	Boot
1010	Boot - extend_root_partition

MessageId/Event Id	Messaggio di evento
2000	Network
2010	Network - add_routes
3000	PreReady
3010	PreReady - activate_windows
3020	PreReady - install_egpu_manager
3030	PreReady - set_monitor_on
3040	PreReady - set_hibernation
3050	PreReady - set_admin_account
3060	PreReady - set_dns_suffix
3070	PreReady - set_wallpaper
3080	PreReady - set_update_schedule
3090	PreReady - output_log
3100	PreReady - enable_open_ssh
5000	Windows is Ready to use
6000	PostReadyLocalData
7000	PostReadyUserData
6010/7010	PostReadyLocal/UserData - set_wallpaper
6020/7020	PostReadyLocal/UserData - set_update_schedule

MessageId/Event Id	Messaggio di evento
6030/7030	PostReadyLocal/UserData - set_hostname
6040/7040	PostReadyLocal/UserData - execute_program
6050/7050	PostReadyLocal/UserData - execute_script
6060/7060	PostReadyLocal/UserData - manage_package
6070/7070	PostReadyLocal/UserData - initialize_volume
6080/7080	PostReadyLocal/UserData - write_file
6090/7090	PostReadyLocal/UserData - start_ssm
7100	PostReadyUserData - enable_open_ssh
6110/7110	PostReadyLocal/UserData - enable_jumbo_frames

Output del log della console EC2Launch v2

Questa sezione contiene un esempio di output del log della console per EC2Launch v2 ed elenca tutti i messaggi di errore del log della console EC2Launch v2 che consentono di risolvere i problemi. Per ulteriori informazioni sull'output della console di istanza e su come accedervi, consultare the section called "Output della console delle istanze".

Output

- Output del log della console EC2Launch v2

- Messaggi di log della console EC2Launch v2

Output del log della console EC2Launch v2

Di seguito è riportato un esempio di output del log della console per EC2Launch v2. Alcuni valori in questo esempio sono sostituiti con testo rappresentativo circondato da parentesi graffe.

```
2025/07/22 21:26:53Z: Windows sysprep configuration complete.
2025/07/22 21:26:53Z: Message: Waiting for access to metadata...
2025/07/22 21:26:53Z: Message: Meta-data is now available.
2025/07/22 21:26:53Z: AMI Origin Version: 2024.12.13
2025/07/22 21:26:53Z: AMI Origin Name: Windows_Server-2022-English-Full-Base
2025/07/22 21:26:53Z: OS: Microsoft Windows NT 10.0.20348
2025/07/22 21:26:53Z: OsVersion: 10.0
2025/07/22 21:26:53Z: OsProductName: Windows Server 2022 Datacenter
2025/07/22 21:26:53Z: OsBuildLabEx: 20348.1.amd64fre.fe_release.210507-1500
2025/07/22 21:26:53Z: OsCurrentBuild: 20348
2025/07/22 21:26:53Z: OsReleaseId: 2009
2025/07/22 21:26:53Z: Language: en-US
2025/07/22 21:26:53Z: TimeZone: UTC
2025/07/22 21:26:53Z: Offset: UTC +0000
2025/07/22 21:26:53Z: Launch: EC2 Launch v2.2.63
2025/07/22 21:26:53Z: AMI-ID: ami-1234567890abcdef1
2025/07/22 21:26:53Z: Instance-ID: i-1234567890abcdef0
2025/07/22 21:26:54Z: Instance Type: t3.xlarge
2025/07/22 21:26:54Z: Driver: AWS NVMe Driver v1.6.0.35
2025/07/22 21:26:54Z: SubComponent: 1.6.0.35; EnableSCSIPersistentReservations: 0
2025/07/22 21:26:54Z: Driver: AWS PV Driver Package v8.5.0
2025/07/22 21:26:55Z: Driver: Amazon Elastic Network Adapter v2.8.0.0
2025/07/22 21:26:55Z: Driver: EC2 Windows Utility Device v3.1.0.25
2025/07/22 21:26:55Z: HOSTNAME: EC2AMAZ-9FJG5CC
2025/07/22 21:26:55Z: RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
2025/07/22 21:26:55Z: RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
2025/07/22 21:26:56Z: SSM: Amazon SSM Agent v3.3.2746.0
2025/07/22 21:26:57Z: User data format: no_user_data
2025/07/22 21:26:57Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2025/07/22 21:26:57Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AgentCommandErrorCode=1
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AdminPasswordTypeCode=0
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AgentErrorLocation=execute_windows.go:410
2025/07/22 21:26:57Z: EC2LaunchTelemetry: IpConflictDetectionCode=0
2025/07/22 21:26:57Z: Message: Windows is Ready to use
```

```
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2", ...}
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2", ...}
```

Messaggi di log della console EC2Launch v2

Di seguito è riportato un elenco di tutti i messaggi di log della console EC2Launch v2.

```
Error EC2Launch service is stopping. {error message}
```

Dettagli dell'errore di un servizio arrestato:

- `Error setting up EC2Launch agent folders`
- `See instance logs for detail`
- `Error stopping service`
- `Error initializing service`

```
Windows sysprep configuration complete
```

```
Invalid administrator username: {invalid username}
```

```
Invalid administrator password
Username: {username}
Password: <Password>{encrypted password}</Password>
```

Il messaggio seguente è un blocco di informazioni che contiene i dettagli dell'AMI:

```
AMI Origin Version: {amiVersion}
AMI Origin Name: {amiName}
Microsoft Windows NT {currentVersion}.{currentBuildNumber}
OsVersion: {currentVersion}
OsProductName: {productName}
OsBuildLabEx: {buildLabEx}
OsCurrentBuild: {currentBuild}
OsReleaseId: {releaseId}
Language: {language}
TimeZone: {timeZone}
Offset: UTC {offset}
Launch agent: EC2Launch {BuildVersion}
AMI-ID: {amiId}
```

```
Instance-ID: {instanceId}
Instance Type: {instanceType}
HOSTNAME: {computer name}
RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
SqlServerBilling: {sql billing}
SqlServerInstall: {sql patch leve, edition type}
Driver: AWS NVMe Driver {version}
Driver: Inbox NVMe Driver {version}
Driver: AWS PV Driver Package {version}
Driver: EC2 Windows Utility Device {version}
SSM: Amazon SSM Agent {version}
AWS VSS Version: {version}
```

```
Windows sysprep configuration complete.
Windows is being configured. 'SysprepState is {state}'
Windows is still being configured. 'SysprepState is {state}'
Windows is Ready to use
Waiting for access to metadata...
Meta-data is now available.
Metadata is not available for this instance.
Timed out waiting for access to metadata.
User data format: {format}
```

I messaggi di telemetria di EC2Launch v2 includono i valori delle proprietà di telemetria di avvio. A partire dalla versione 2.2.63, i dati di telemetria dell'agente EC2 sono formattati come oggetto JSON.

```
EC2LaunchTelemetry: {telemetry property}
```

```
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2" ... }
```

Cronologie delle versioni EC2Launch v2

Cronologie delle versioni

- Cronologia delle versioni di EC2Launch v2

Cronologia delle versioni di EC2Launch v2

Per assicurarti di avere installato l'agente di avvio più recente, consulta Installare la versione più recente di EC2Launch v2. È possibile ricevere notifiche quando vengono rilasciate nuove versioni

dell'agente EC2Launch v2. Per ulteriori informazioni, consulta Sottoscrizione alle notifiche dell'agente di avvio EC2 Windows.

La tabella seguente descrive le versioni rilasciate di EC2Launch v2.

Versione	Dettagli	Data di rilascio
2.5.2	• È stato risolto un problema per cui la convalida dei certificati RDP non riesce per i certificati personalizzati e i certificati di gruppo Policy-deployed .	5 agosto 2026
2.5.1	• Rilevamento degli errori migliorato durante l'attivazione dell'ibernazione.	3 giugno 2026
2.5.0	• Logica della porta seriale aggiornata per continuare le attività dell'agente quando la porta seriale non è disponibile. • È stata aggiunta la versione del driver EC2 Windows Utility Device all'output della console dell'istanza. • È stato rimosso il file bench.log inutilizzato. • Ricerca ottimizzata dei driver durante la scrittura sull'output della console dell'istanza.	4 maggio 2026
2.4.0	• Registrazione semplificata degli agenti rimuovendo i file `console.log` ridondanti. `err.log` • Funzionalità di registrazione degli agenti migliorate aggiungendo la rotazione dei log, limitando la dimensione del registro a 1 MB e migliorando la precisione temporale a millisecondi. • Richiesta di Hyper-V stato rimossa e relativo output della console dell'istanza.	5 marzo 2026

Versione	Dettagli	Data di rilascio
2.3.237	• È stato risolto un problema di arresto anomalo dell'agente causato dall'incompatibilità tra alcune versioni di runtime di Visual C++ e le funzioni di telemetria dell'agente.	25 febbraio 2026
2.3.108	• È stata aggiunta la visualizzazione dell'indirizzo IPv6 allo sfondo. Per gli attributi di memoria e rete, consultare AWS la documentazione.	29 dicembre 2025
2.3.56	• È stato risolto un problema per cui le route di rete persisten ti preconfigurate non venivano gestite correttamente da EC2Launch v2.	4 novembre 2025
2.3.5	• Rilevamento dell'interfaccia di rete principale migliorato utilizzando IMDS durante l'aggiunta di percorsi.	15 settembre 2025
2.2.63	• Agente di lancio aggiornato per migliorare Telemetria.	29 luglio 2025
2.1.1	• Aggiunto il supporto completo per IPv6.	14 maggio 2025
2,02107	• Aggiunta di percorsi migliorata per gestire scenari in cui gli indirizzi IPv4 o IPv6 non sono disponibili sull'interfaccia.	27 marzo 2025

Versione	Dettagli	Data di rilascio
2,02081	• È stato risolto un problema in cui le informazioni sul certifica to RDP non venivano recuperate o convalidate correttamente. Aggiunta funzionalità per avviare automaticamente i Servizi di Desktop remoto, se necessario. • Regolate le autorizzazioni del servizio EC2Launch v2 per risolvere un problema che si verifica durante l'interrogazione dello stato del servizio.	4 febbraio 2025
2.0.2046	• È stato aggiornato il percorso dello sfondo nel file `agent-config.yml` affinché venga utilizzato il percorso predefinito dello sfondo del sistema operativo. • È stata aggiunta la telemetria per monitorare le posizioni in cui si verificano gli errori dell'agente. • È stata aggiornata la messaggistica di log dell'agente.	3 ottobre 2024
2,0,1981	• Sono stati aggiornati i messaggi di errore dell'interfaccia a riga di comando di `EC2Launch.exe` per gli utenti non amministr atori.	6 agosto 2024
2,0,1948	• È stata aggiunta la telemetria per monitorare l'utilizzo delle opzioni di password dell'amministratore. • Sono state modificate le autorizzazioni di EC2Launch.	1° luglio 2024

Versione	Dettagli	Data di rilascio
2,0,1924	• L'interfaccia utente delle impostazioni di EC2Launch è stata aggiornata. • Il comando dell'interfaccia a riga di comando per lo sfondo è stato aggiornato. • Il programma di installazione di EC2Launch è stato aggiornato.	10 giugno 2024
2,0,1914	• Sono stati aggiunti percorsi con indirizzi gateway non specificati (`0.0.0.0` per IPv4 oppure `::` per IPv6). • Aggiungere sempre entrambi i percorsi IPv4 e IPv6. • È stato risolto un problema per cui il nome utente `Administrator` veniva aggiunto al file `agent-config.yml` quando non veniva specificato. • Sono state modificate le autorizzazioni di EC2Launch v2.	5 giugno 2024

Versione	Dettagli	Data di rilascio
2,0,1881	• È stata aggiunta un'opzione con password crittografata all'attività `setAdminAccount` . • È stato aggiunto il comando dell'interfaccia a riga di comando per crittografare la password statica in agent-config.yml. • È stato risolto un problema per cui i dati utente XML non aggiungono PowerShell argomenti quando vengono eseguiti con le autorizzazioni di amministratore. Per ulteriori dettagli, consultare In che modo Amazon EC2 gestisce i dati utente per le istanze Windows. • PowerShell Argomenti modificati per gli script delle `executeScript` attività e dei dati utente quando vengono eseguiti con `LocalSystem` autorizzazioni. Quando gli argomenti sono vuoti, l'agente utilizza il seguente valore predefinito: `-ExecutionPolicy Unrestricted` . • È stata impedita la stampa di versioni duplicate dei driver nel log della console.	8 maggio 2024

Versione	Dettagli	Data di rilascio
2.0.1815	• È stata modificata la gestione degli errori affinché l'esito sia negativo per problemi critici di configurazione prima di sysprep. • È stato risolto un problema per cui le attività relative allo sfondo e ai nomi host potevano utilizzare un indirizzo IP errato nelle istanze con più indirizzi IP assegnati all'interfaccia di rete principale. • Le attività relative allo sfondo e ai nomi host sono state modificate affinché ottengano per prima cosa un IP privato da IMDS, per poi eseguire il failback su WMI se IMDS è disabilit ato. • È stato risolto un problema relativo all'attività `initializ eVolume` che causava la mancata inizializzazione dei volumi `sc1` a causa di un errore transitorio.	6 marzo 2024
2,0,1739	• È stato risolto un problema che impediva l'acquisizione dei codici di uscita da attività `executeScript` eseguite come utente amministratore di Windows.	17 gennaio 2024

Versione	Dettagli	Data di rilascio
2,0,1702	• Autorizzazioni `Telemetry.log` limitate a `read-execute` solo per gli utenti standard. • Il servizio Windows EC2Launch è stato configurato per il riavvio in caso di errore di avvio. • Gli errori `add-routes` sono stati resi risolvibili registrando l'output `route.exe stderr`. • È stato risolto un problema che si verificava quando le metriche del percorso non rientravano nell'intervallo [1, 9999]. • È stato aggiunto il supporto per gli sfondi per numerosi nuovi tipi di istanze. • È stato risolto un problema causato dagli script di dati utente che venivano eseguiti come utente amministratore di Windows e inviavano l'output a `stderr`.	4 gennaio 2024

Versione	Dettagli	Data di rilascio
2,0,1643	• Lo strumento `ebsnvme-id.exe` è stato aggiornato alla versione 1.1.0.7. • È stato risolto un problema relativo alle impostazioni di dimensionamento lato ricezione (RSS) e della profondità della coda di ricezione sui tipi di istanze metal che iniziano con "metal-*", come metal-48x1. • È stato rimosso l'evento di telemetria che riporta i comandi userdata XML che bloccano l'agente. • È stata aggiornata l'attività `setDnsSuffix` per limitare la devoluzione del nome di dominio in base alla voce del registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • È stata aggiunta un'attività pubblica e una CLI che aggiunge percorsi di rete. • Nota: questa è l'ultima versione che supporta ufficialmente Windows Server 2012. • Nota: questa è l'ultima versione che supporta ufficialmente i sistemi operativi a 32 bit.	4 ottobre 2023
2,0,1580	• È stato modificato il modo in cui l'agente di avvio gestisce gli errori quando si modificano le autorizzazioni dei file di log. • È stato aggiunto un timeout per la connessione alla porta seriale. Il timeout consente all'agente di avvio di continuare a funzionare se la porta seriale è in uso.	05 settembre 2023

Versione	Dettagli	Data di rilascio

2,0,1521	• È stato dichiarato obsoleto il flag –`block` dei comandi reset e sysprep `EC2Launch.exe` .
	• È stato aggiornato diventando `EC2Launch.exe` per rilevare e gestire i comandi reset e sysprep utilizzati nelle attività in linea `executeScript` . Questi comandi causano l'interruzione dell'esecuzione dell'agente dopo l'esecuzione dell'operazione `executeScript` .
	• Gli script UserData XML sono stati aggiornati per l'esecuzione in linea per impostazione predefinita.
	• Consente di abilitare l'esecuzione degli script UserData XML in modo indipendente con il nuovo tag `detach`. Per ulteriori dettagli, consultare Script di dati utente.
	• Sono state apportate le seguenti modifiche al log dell'agente.
	  • Sono stati aggiornati i messaggi di log dell'agente.
	  • Sono stati rimossi i contenuti e output `executeScript` dal log dell'agente.
	  • Sono stati rimossi gli argomenti e output `executeProgram` dal log dell'agente.
	• Sono state apportate le seguenti modifiche al log della console.
	  • È stato aggiunto il valore `EnableSCSIPersistentReservations` al log della console.
		3 luglio 2023

Versione	Dettagli	Data di rilascio
2,0,1303	• Sono state aggiunte ulteriori righe di gestione degli errori e di log durante l'aggiunta di percorsi di rete. • Consentiti `executeScript` e `executeProgram` compiti in fase. PreReady • Attività `executeProgram` aggiornata per generare file di output simili all'output dell'attività executeScript. Per ulteriori informazioni, consulta executeProgram. • È stata aggiunta la telemetria per monitorare l'utilizzo dei comandi dell'agente di blocco nei dati utente XML.	3 maggio 2023
2.0.1245	• È stata migliorata la visibilità degli arresti anomali grazie alla registrazione in chiaro degli stack delle chiamate di arresto anomalo. • È stato aggiunto il EventLog servizio come dipendenza di avvio per correggere un arresto anomalo quando il servizio Amazon EC2Launch si avvia più velocemente del servizio. EventLog • I dati utente XML sono stati eseguiti prima del PostReady passaggio dal file di configurazione dell'agente (come EC2Launch v1 e EC2Config). • Sono stati aggiunti i dati utente YAML versione 1.1 per far sì che i dati utente vengano eseguiti prima della PostReady fase dal file di configurazione dell'agente (i dati utente YAML versione 1.0 vengono eseguiti dopo la fase dal file di configura zione dell'agente). PostReady	8 marzo 2023

Versione	Dettagli	Data di rilascio
2.0.1173	• Aggiunge una funzionalità opzionale per visualizzare i tag delle istanze sullo sfondo. Per ulteriori informazioni, consulta setWallpaper. • Aggiunge la gestione degli errori quando il gruppo di sicurezza per Elastic Graphics non è impostato correttamente. • Corregge un timeout quando l'Instance Metadata Service non è abilitato.	6 febbraio 2023
2,01121	• Risolve un problema a causa del quale un errore 404 viene visualizzato sullo sfondo quando non viene assegnato alcun indirizzo IPv4 pubblico. • Risolve un problema a causa del quale il file system del volume è formattato come `RAW` invece di `NTFS` quando la lettera di unità del dispositivo è impostata su `D`. • Risolve un problema a causa del quale i volumi SSD NVMe vengono erroneamente identificati come volumi EBS. • Risolve un errore durante l'attivazione di Windows quando IMDS è disabilitato.	4 gennaio 2023

Versione	Dettagli	Data di rilascio
2,0,1082	• Risolve un problema per cui il campo `setWallpaper : privateIpAddress` è vuoto quando IMDS è disabilitato. • Risolve un problema relativo all'impostazione del nome host sull'indirizzo IPv4 privato quando IMDS è disabilitato. • Risolve un problema relativo all'inizializzazione dei volumi su Windows Server 2012. • Risolve un problema relativo all'impostazione dei frame jumbo. • Risolve un errore che si verifica quando non viene specificata alcuna chiave SSH all'avvio dell'istanza. • Corregge un errore su Windows Server 2012 quando Windows non dispone di una chiave di registro «». ReleaseId	7 dicembre 2022
2.0.1011	• Corregge la logica per la ricerca dell'adattatore di rete quando PnPDeviceID è vuoto.	11 novembre 2022
2,0,1009	• Utilizza le informazioni sui segmenti PCI per selezionare la porta della console.	8 novembre 2022

Versione	Dettagli	Data di rilascio
2,0,982	• Aggiunge la logica dei tentativi per ottenere informazioni su RDP. • Corregge gli errori durante l'inizializzazione dei volumi sulle istanze `d2.8xlarge` . • Risolve il problema per cui è possibile selezionare un adattatore di rete non corretto dopo un riavvio. • Rimuove il messaggio di errore di falso allarme quando ACPI SPCR non è disponibile.	31 ottobre 2022
2,0,863	• Aggiorna la logica di attesa IMDS per effettuare solo richieste IMDSv2. • Aggiunge la logica per l'assegnazione di una lettera di unità a volumi già inizializzati ma non montati. • Stampa un messaggio di errore più specifico quando il tipo di coppia di chiavi non è supportato. • Risolve bug del codice di riavvio 3010. • Aggiunge il controllo per dati utente con codifica base64 non validi.	6 luglio 2022
2,0,698	• Corregge gli errori di battitura nell'output del log durante l'esecuzione di script.	30 gennaio 2022

Versione	Dettagli	Data di rilascio
2,0674	• La telemetria carica il controllo della privacy. enabled/disabled • Corregge i bug `index out of bounds`. • Rimuove le scorciatoie da sfondo durante `sysprep`.	15 novembre 2021
2.0.651	• Aggiunge la logica per disinstallare gli agenti legacy durante l'installazione di EC2Launch v2. • Risolve il problema `list-volume` della CLI quando il volume root non è elencato come volume 0.	7 ottobre 2021
2,0,592	• Corregge i bug per segnalare correttamente lo stato della fase. • Rimuove falsi messaggi di errore di allarme quando i file di log sono chiusi. • Aggiunge dati di telemetria.	31 agosto 2021
2,0,548	• Aggiunge zeri iniziali per il nome host IP esadecimale. • Risolve le autorizzazioni dei file per l'incarico `enableOpenSsh` . • Risolve il crash del comando sysprep.	4 agosto 2021

Versione	Dettagli	Data di rilascio
2,0,470	• Corregge il bug in fase di rete in attesa di DHCP per assegnare un IP all'istanza. • Corregge il bug con `setDnsSuffix` quando `SearchList` la chiave di registro non esiste. • Corregge il bug nella logica di devoluzione DNS in `setDnsSuffix` . • Aggiunge route di rete dopo i riavvii intermedi. • Consente a `initializeVolume` di ripetere la lettera dei volumi esistenti. • Rimuove informazioni aggiuntive dal sottocomando versione.	20 luglio 2021
2.0.285	• Aggiunge l'opzione per eseguire script utente in un processo scollegato. • I dati utente legacy (dati utente XML) vengono ora eseguiti in un processo scollegato, che è simile a quello dell'agente di avvio precedente. • Aggiunge il flag CLI ai comandi `sysprep` e `reset`, consenten done il blocco fino all'arresto del servizio. • Limita le autorizzazioni della cartella di configurazione.	8 marzo 2021

Versione	Dettagli	Data di rilascio
2.0.207	• Aggiunge il campo facoltativo `hostName` all'attività `setHostName` . • Corregge il bug di riavvio. Riavviare le attività `executeScript` e `executeProgram` verrà contrassegnato come in esecuzione. • Aggiunge altri codici di ritorno al comando di stato. • Aggiunge il servizio bootstrap per risolvere il problema di startup durante l'esecuzione sul tipo di istanza `t2.nano`. • Risolve i problemi legati alla modalità di installazione pulita per rimuovere i file non monitorati dal programma di installazione.	2 febbraio 2021
2.0.160	• Corregge il comando `validate` per rilevare il nome dello stadio non valido. • Aggiunge il comando `w32tm resync` nell'attività `addroutes` . • Risolve il problema con la modifica dell'ordine di ricerca del suffisso DNS. • Aggiunge condizioni di controllo per segnalare meglio i dati utente non validi.	4 dicembre 2020
2.0.153	Aggiunge la funzionalità Sysprep in. UserData	3 novembre 2020

Versione	Dettagli	Data di rilascio
2.0.146	• Risolve il problema relativo alle AMI non inglesi RootExtend . • Concede ai gruppi di utenti l'autorizzazione di scrittura per i file del log • Crea partizione riservata MS per i volumi GPT. • Aggiunge il comando list-volumes e il menu a discesa del volume nelle impostazioni di Amazon EC2Launch. • Aggiunge il comando get-agent-config per la stampa del file agent-config.yml in formato yaml o json. • Cancella la password statica se non viene rilevata alcuna chiave pubblica.	6 ottobre 2020
2.0.124	• Aggiunge l'opzione per visualizzare la versione del sistema operativo sullo sfondo. • Inizializza volumi EBS crittografati. • Aggiunge route per i VPC senza un nome DNS locale.	10 settembre 2020
2.0.104	• Crea l'elenco di ricerca dei suffissi DNS se non esiste. • Ignora l'ibernazione se non richiesta.	12 agosto 2020
2.0.0	Versione iniziale.	30 giugno 2020

Utilizza l'agente EC2Launch v1 per eseguire attività durante l'avvio dell'istanza EC2 Windows

Le AMI gestite da Amazon per Windows Server 2016 e 2019 comprendono una serie di script Windows Powershell chiamati EC2Launch. EC2Launch esegue le operazioni durante l'avvio dell'istanza iniziale. Per informazioni sulle versioni di EC2Launch incluse nelle AMI AWS Windows, vedere Windows AMI Reference AWS .

> **Note**
>
> L'agente di avvio più recente per Windows Server 2016 e versioni successive del sistema operativo è EC2Launch v2 che sostituisce sia EC2Config che EC2Launch. È preinstallato sulle AMI AWS Windows Server 2016 e 2019, con nomi che iniziano con `EC2LaunchV2-Windows_Server-*`. Puoi anche installare e configurare manualmente l'agente su Windows Server 2016 e 2019. Per ulteriori informazioni, consulta Installare EC2Launch v2.
> Per utilizzare EC2Launch con IMDSv2, la versione deve essere 1.3.2002730 o versione successiva.

È possibile utilizzare il seguente PowerShell comando di Windows per verificare la versione installata di EC2Launch.

```
Test-ModuleManifest -Path "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1" | Select Version
```

Attività EC2Launch

EC2Launch esegue le seguenti operazioni per impostazione predefinita durante l'avvio dell'istanza iniziale:

- Imposta un nuovo sfondo che esegue il rendering delle informazioni riguardanti l'istanza.
- Imposta il nome del computer sull'indirizzo IPv4 privato dell'istanza.
- Invia le informazioni di istanza alla console Amazon EC2.
- Invia l'impronta del certificato RDP alla console EC2.
- Imposta una password casuale per l'account dell'amministratore.
- Aggiunge i suffissi DNS.

- Estende in modo dinamico la partizione del sistema operativo per includere qualsiasi spazio non partizionato.
- Esegue i dati utente (se specificato). Per ulteriori informazioni sulla specifica dei dati utente, consulta Esegui i comandi quando avvii un'istanza EC2 con l'input dei dati utente.
- Imposta routing statici persistenti per raggiungere il servizio di metadati e i server AWS KMS .

> **Important**
>
> Se da questa istanza viene creata un'AMI personalizzata, i routing vengono acquisiti come parte della configurazione del sistema operativo e qualsiasi nuova istanza avviata dall'AMI avrà gli stessi routing, indipendentemente dal posizionamento della sottorete. Per aggiornare i percorsi, vedere. Aggiorna i metadata/KMS percorsi per Server 2016 e versioni successive quando si avvia un'AMI personalizzata

Le seguenti attività contribuiscono a mantenere la retrocompatibilità con il servizio EC2Config. È anche possibile configurare EC2Launch in modo che esegua queste attività durante li startup:

- Inizializzare i volumi EBS secondari.
- Inviare i log di eventi di Windows ai log della console EC2.
- Inviare il messaggio Windows is ready to use (Windows è pronto per l'utilizzo) alla console EC2.

Struttura della directory di EC2Launch

Per impostazione predefinita, EC2Launch viene installato sulle AMI di Windows Server 2016 o versione successiva nella directory radice `C:\ProgramData\Amazon\EC2-Windows\Launch`.

> **Note**
>
> Per impostazione predefinita, Windows nasconde i file e le cartelle in `C:\ProgramData`. Per visualizzare le directory e i file di EC2Launch, è necessario digitare il percorso in Windows Explorer risorse o modificare le proprietà della cartella per visualizzare i file e le cartelle nascosti.

La directory `Launch` contiene le sottodirectory seguenti.

- `Scripts`— Contiene PowerShell gli script che compongono EC2Launch.
- `Module` - Contiene il modulo per la creazione di script relativi a Amazon EC2.
- `Config` - Contiene file di configurazione dello script che si possono personalizzare.
- `Sysprep` - Contiene risorse Sysprep.
- `Settings` - Contiene un'applicazione per l'interfaccia utente grafica di Sysprep.
- `Library`: contiene librerie condivise per gli agenti di avvio di EC2.
- `Log`: contiene sottodirectory per gli script e i file di log generati dagli script.

Telemetria

La telemetria è un'informazione aggiuntiva che aiuta AWS a comprendere meglio i requisiti, diagnosticare i problemi e fornire funzionalità per migliorare l'esperienza con i servizi. AWS

EC2Launch versione `1.3.2003498` e successive raccolgono dati di telemetria, ad esempio parametri ed errori di utilizzo. Questi dati vengono raccolti dall'istanza Amazon EC2 su cui viene eseguito EC2Launch. Sono incluse tutte le AMI Windows di proprietà di. AWS

EC2Launch raccoglie i seguenti tipi di telemetria:

- Informazioni di utilizzo: comandi dell'agente, metodo di installazione e frequenza di esecuzione pianificata.
- Errori e informazioni diagnostiche: installazione dell'agente ed esecuzione dei codici di errore.

Esempi di dati raccolti:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

La telemetria è abilitata per impostazione predefinita. Puoi disabilitare la raccolta dati di telemetria in qualsiasi momento. Se la telemetria è abilitata, EC2Launch invia i dati di telemetria senza ulteriori notifiche ai clienti.

Viene registrata la scelta di abilitare o disabilitare la telemetria.

È possibile attivare o disattivare la raccolta di telemetria. La propria selezione per attivare o disattivare la telemetria viene raccolta per garantire l'adesione alla propria opzione di telemetria.

Visibilità della telemetria

Quando la telemetria è abilitata, viene visualizzata nell'output della console Amazon EC2 come segue:

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Disabilitare la telemetria su un'istanza

Per disattivare la telemetria impostando una variabile di ambiente di sistema, esegui il comando seguente come amministratore:

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Per disabilitare la telemetria durante l'installazione, eseguire `install.ps1` come riportato:

```
. .\install.ps1 -EnableTelemetry:$false
```

Altri argomenti per EC2Launch

- Installare la versione più recente di EC2Launch
- Configurazione dell'agente EC2Launch v1 sulla istanza di Windows
- Cronologia delle versioni di EC2Launch

Installare la versione più recente di EC2Launch

Per scaricare e installare la versione più recente di EC2Launch sulle istanze, attenersi alla procedura seguente.

Scaricare e installare la versione più recente di EC2Launch

1. Se EC2Launch è già stato installato e configurato su un'istanza, eseguire un backup del file di configurazione di EC2Launch. Il processo di installazione non conserva le modifiche apportate a questo file. Per impostazione predefinita, il file si trova nella directory `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. EC2-Windows-Launch.zipEffettua il download in una directory dell'istanza.

3. Scaricare install.ps1 nella stessa directory in cui è stato scaricato `EC2-Windows-Launch.zip`.
4. Esegui `install.ps1`
5. Se è stato eseguito il backup del file di configurazione di EC2Launch, copiarlo nella directory `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Per scaricare e installare la versione più recente di EC2Launch utilizzando PowerShell

Se EC2Launch è già stato installato e configurato su un'istanza, eseguire un backup del file di configurazione di EC2Launch. Il processo di installazione non conserva le modifiche apportate a questo file. Per impostazione predefinita, il file si trova nella directory `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Per installare l'ultima versione di EC2Launch utilizzando PowerShell, esegui i seguenti comandi da una PowerShell finestra come amministratore:

```
mkdir $env:USERPROFILE\Desktop\EC2Launch
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/EC2-Windows-Launch.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/install.ps1"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
& $env:USERPROFILE\Desktop\EC2Launch\install.ps1
```

> **Note**
>
> Se ricevi un errore durante il download del file e stai utilizzando Windows Server 2016, potrebbe essere necessario abilitare TLS 1.2 per il tuo terminale. PowerShell È possibile abilitare TLS 1.2 per la PowerShell sessione corrente con il comando seguente e riprovare:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```

Verifica l'installazione controllando l'agente di avvio. Esegui i seguenti comandi da una PowerShell finestra come amministratore:

```
Import-Module C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Ec2Launch.psm1
Import-LocalizedData -BaseDirectory C:\ProgramData\Amazon\EC2-Windows\Launch\Module\ -
FileName 'Ec2Launch.psd1' -BindingVariable moduleManifest
$moduleManifest.Get_Item('ModuleVersion')
```

Configurazione dell'agente EC2Launch v1 sulla istanza di Windows

Dopo aver inizializzato l'istanza la prima volta, è possibile configurare EC2Launch in modo che venga eseguito nuovamente ed eseguire diverse attività di avvio.

Attività

- Configurare le attività di inizializzazione
- Pianificare EC2Launch in modo che venga eseguito a ogni avvio
- Inizializzazione delle unità e mappatura delle lettere di unità
- Inviare i log di eventi di Windows alla console EC2.
- Inviare il messaggio Windows is ready (Windows è pronto) dopo un avvio riuscito.

Configurare le attività di inizializzazione

Specificare le impostazioni nel file `LaunchConfig.json` per attivare o disattivare le seguenti attività di inizializzazione:

- Imposta il nome del computer sull'indirizzo IPv4 privato dell'istanza.
- Impostare il monitor in modo che rimanga sempre acceso.
- Impostare un nuovo sfondo.
- Aggiungere l'elenco di suffissi DNS.

> **Note**
>
> Ciò aggiunge una ricerca dei suffissi DNS per il seguente dominio e configura altri suffissi standard. Per ulteriori informazioni sul modo in cui gli agenti di lancio impostano i suffissi DNS, consultare Configura il suffisso DNS per gli agenti di avvio EC2 Windows.
>
> ```
> region.ec2-utilities.amazonaws.com
> ```

- Estendere la dimensione del volume di avvio.

- Impostare la password amministratore

Configurare le impostazioni di inizializzazione

1. Nell'istanza da configurare, aprire il seguente file in un editor di testo: `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\LaunchConfig.json`.
2. Aggiornare le seguenti impostazioni come necessario e salvare le modifiche. Fornire una password in `adminPassword` solo se `adminPasswordtype` è `Specify`.

```
{
 "setComputerName": false,
 "setMonitorAlwaysOn": true,
 "setWallpaper": true,
 "addDnsSuffixList": true,
 "extendBootVolumeSize": true,
 "handleUserData": true,
 "adminPasswordType": "Random | Specify | DoNothing",
 "adminPassword": "password that adheres to your security policy (optional)"
}
```

I tipi di password sono definiti come segue:

`Random`

EC2Launch genera una password e la crittografa utilizzando la chiave dell'utente. Il sistema disattiva questa impostazione dopo l'avvio dell'istanza in modo che questa password rimanga se l'istanza viene riavviata o arrestata e avviata.

`Specify`

EC2Launch utilizza la password specificata in `adminPassword`. Se la password non soddisfa i requisiti di sistema, EC2Launch genera invece una password casuale. La password viene memorizzata in `LaunchConfig.json` come testo non crittografato e viene cancellata dopo che Sysprep ha impostato la password amministratore. EC2Launch crittografa la password utilizzando la chiave dell'utente.

`DoNothing`

EC2Launch utilizza la password specificata nel file `unattend.xml`. Se non si indica una password in `unattend.xml`, l'account amministratore viene disattivato.

3. In Windows PowerShell, esegui il comando seguente per pianificare l'esecuzione dello script come attività pianificata di Windows. Lo script viene eseguito una volta durante l'avvio successivo, poi disabilita la nuova esecuzione di queste attività.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

Pianificare EC2Launch in modo che venga eseguito a ogni avvio

Puoi pianificare EC2Launch in modo che venga eseguito a ogni avvio invece che solo all'avvio iniziale.

Per abilitare EC2Launch in modo che venga eseguito a ogni avvio:

1. Apri Windows PowerShell ed esegui il comando seguente:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
SchedulePerBoot
```

2. Oppure, eseguire l'eseguibile con il seguente comando:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe
```

   Quindi selezionare `Run EC2Launch on every boot`. Puoi specificare che la tua istanza EC2 `Shutdown without Sysprep` o `Shutdown with Sysprep`.

> **Note**
>
> Quando abiliti EC2Launch in modo che sia eseguito a ogni avvio, al successivo avvio di EC2Launch si verifica quanto riportato di seguito:
>
> - Se `AdminPasswordType` è ancora impostato su `Random`, EC2Launch genererà una nuova password al prossimo avvio. Dopo l'avvio, `AdminPasswordType` viene impostato automaticamente su `DoNothing` per impedire a EC2Launch di generare nuove password agli avvii successivi. Per impedire a EC2Launch di generare una nuova password al primo avvio, imposta manualmente `AdminPasswordType` su `DoNothing` prima di riavviare.

- `HandleUserData` verrà di nuovo impostato su `false` a meno che i dati utente non abbiano `persist` impostato su `true`. Per ulteriori informazioni, consulta the section called "Script di dati utente".

Inizializzazione delle unità e mappatura delle lettere di unità

Specificare le impostazioni nel file `DriveLetterMappingConfig.json` per mappare le lettere di unità nei volumi dell'istanza EC2. Lo script inizializza le unità che non sono già inizializzate e partizionate. Per ulteriori informazioni su come ottenere i dettagli del volume in Windows, consulta Get-Volume la documentazione Microsoft.

Mappatura delle lettere di unità nei volumi

1. Apri il file `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` in un editor di testo.
2. Specificare le seguenti impostazioni di volume e salvare le modifiche:

```
{
 "driveLetterMapping": [
  {
   "volumeName": "sample volume",
   "driveLetter": "H"
  }
 ]
}
```

3. Apri Windows PowerShell e usa il comando seguente per eseguire lo script EC2Launch che inizializza i dischi:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Per inizializzare i dischi ogni volta che l'istanza si avvia, aggiungere il contrassegno `-Schedule` come segue:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -Schedule
```

Inviare i log di eventi di Windows alla console EC2.

Specificare le impostazioni nel file `EventLogConfig.json` per inviare i log di eventi di Windows ai log della console EC2.

Configurazione delle impostazioni per inviare i log di eventi di Windows

1. Nell'istanza, aprire il file `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\EventLogConfig.json` in un editor di testo.
2. Configurare le seguenti impostazioni di log e salvare le modifiche:

```
{
 "events": [
  {
   "logName": "System",
   "source": "An event source (optional)",
   "level": "Error | Warning | Information",
   "numEntries": 3
  }
 ]
}
```

3. In Windows PowerShell, esegui il comando seguente in modo che il sistema pianifichi l'esecuzione dello script come attività pianificata di Windows ogni volta che l'istanza viene avviata.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendEventLogs.ps1 -Schedule
```

   Possono essere necessari tre minuti o più prima che i log compaiano nei log della console EC2.

Inviare il messaggio Windows is ready (Windows è pronto) dopo un avvio riuscito.

Il servizio EC2Config ha inviato il messaggio "Windows è pronto" alla console EC2 dopo ogni avvio. EC2Launch invia questo messaggio solo dopo l'avvio iniziale. Per la retrocompatibilità con il servizio EC2Config, è possibile programmare EC2Launch in modo che invii questo messaggio dopo ogni avvio. Nell'istanza, apri Windows PowerShell ed esegui il comando seguente. Il sistema programma l'esecuzione dello script come Windows Scheduled Task.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendWindowsIsReady.ps1 -Schedule
```

Cronologia delle versioni di EC2Launch

Per scaricare e installare la versione più recente di EC2Launch, consultare Installare la versione più recente di EC2Launch.

La tabella seguente descrive le versioni rilasciate di EC2Launch.

Versione	Dettagli	Data di rilascio
1.4.299	• Logica ottimizzata per il recupero EC2WinUtil della versione del driver. • Riduzione del tempo necessario per rendere Windows pronto rimuovendo la richiesta di Hyper-V stato.	3 marzo 2026
1.4.183	• Logica di installazione aggiornata per impedire l'installazione non supportata su Windows Server 2022. • Aggiornato per stampare la versione del EC2WinUtil driver nel registro della console dell'istanza.	4 febbraio 2026
1.4.6	• È stata aggiornata la messaggistica di log dell'agente.	13 ottobre 2025
1.3.2005119	• Risolto un problema a causa del quale `Invoke-Userdata` non funzionava se chiamato senza parametri.	11 febbraio 2025
1.3.2005065	• È stato risolto un problema in cui le informazioni sul certifica to RDP non venivano recuperate o convalidate correttamente. Aggiunta funzionalità per avviare automaticamente i Servizi di Desktop remoto, se necessario.	22 ottobre 2024
1,32005008	• Aggiornato `Set-Wallpaper` per effettuare il fall back a uno sfondo a tinta unita se l'immagine di sfondo predefinita non viene trovata.	6 agosto 2024

Versione	Dettagli	Data di rilascio
1,32004959	• Logica di installazione aggiornata per impedire l'installazione non supportata su Windows Server 2025 o versioni successive.	2 luglio 2024
1,32004891	• È stato risolto un problema in cui `HandleUserData` non era impostato su `false` come previsto. • È stata aggiunta un'opzione per la password `Encrypted` a `LaunchConfig.json` . • Modifica del comportamento di `Settings UI` per crittografare la password specificata dall'utente per impostazione predefinita. • Aggiunto `SetAdminPasswordConfig.ps1` per convertire l'opzione per la password `Specify` nell'opzione per la password `Encrypted` nel file di configurazione dell'agente.	31 maggio 2024
1,32004617	• È stato corretto un errore durante l'impostazione dello sfondo.	15 gennaio 2024

Versione	Dettagli	Data di rilascio
1,32004592	• Autorizzazioni di accesso aggiornate impostate da install.ps1 per `%ProgramData%\Amazon\EC2-Windows\Launch .` • folder/file Accesso limitato a EC2Launch alla lettura ed esecuzione solo per gli account utente standard. • L'agente è stato modificato in modo da non attendere più l'inizializzazione del servizio di metadati di istanza (IMDS) se IMDS non è abilitato per l'istanza. • È stato aggiunto un timeout di cinque minuti in attesa dell'inizializzazione dell'IMDS. • È stato modificato l'agente in modo che scrivesse la telemetria nel log della console dell'istanza prima del messaggio `Windows is Ready` anziché dopo. • È stato aggiunto il supporto per gli sfondi per numerosi nuovi tipi di istanze. Per ulteriori informazioni sulle autorizzazioni di accesso e sulle autorizzazioni degli account utente delle directory EC2Launch , consulta the section called “Struttura della directory di EC2Launch”.	2 gennaio 2024
1.3.2004491	• È stata aggiunta la telemetria per monitorare l'utilizzo dell'opzione Specifica password dell'amministratore.	9 novembre 2023
1,32004462	• Aggiunto uno scarico dopo ogni scrittura sulla console seriale.	18 ottobre 2023

Versione	Dettagli	Data di rilascio
1,32004438	• Limita la devoluzione del nome di dominio in base alla voce del registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Le autorizzazioni `UserdataExecution.log` sono state limitate esclusivamente a `Administrators` . • Sono stati aggiunti messaggi di errore nel log eventi di Windows per i casi in cui l'inizializzazione del log non riesce.	4 ottobre 2023
1,32004256	• Valore `EnableSCSIPersistentReservations` aggiunto al log della console. • È stata aggiunta la funzionalità di riprova per Get-ConsolePort.	7 luglio 2023
1,32004052	• È stato risolto un errore che si verificava quando non veniva specificata alcuna chiave SSH all'avvio dell'istanza. • È stato aggiornato per riprovare ad avviare il servizio Windows AmazonSSMAgent in caso di errore. • Aggiornato in modo da fallire SysprepInstance.ps1 se BeforeSysprep.cmd fallisce con un codice di uscita diverso da zero.	8 marzo 2023
1.3.2003975	• È stato risolto il problema relativo alle build AMI Packer in cui `SysprepInstance.ps1` restituiva un valore di `$LastErrorCode` pari a 1.	24 dicembre 2022

Versione	Dettagli	Data di rilascio
1,32003961	• È stato risolto il problema per cui le password amministratore specificate in modo esplicito venivano sovrascritte con una password casuale nelle istanze avviate rapidamente. • È stato risolto il problema a causa del quale l'agente SSM non si avviava su tipi di istanze più piccoli. • È stato risolto un problema a causa del quale il log della console dell'istanza conteneva `RDPCERTIFICATE-THUMBPRINT: 0000000000000000000000` invece di un valore di impronta digitale del certificato RDP valido.	6 dicembre 2022
1,32003923	• Corregge la logica per la ricerca dell'adattatore di rete quando PnPDeviceID è vuoto.	9 novembre 2022
1,32003919	• Aggiornato Get-ConsolePort per utilizzare le informazioni sui segmenti PCI. • È stato risolto il problema per cui era possibile selezionare un adattatore di rete non corretto dopo un riavvio. • Logica di avvio e SSM-Agent timeout fissa. • È stata corretta la compatibilità con le versioni precedenti degli alias di Send-AdminCredentials funzione.	8 novembre 2022
1.3.2003857	• Assegna priorità agli adattatori con un gateway predefinito quando viene selezionato l'adattatore di rete principale. • Aggiunta la crittografia delle password in memoria.	3 ottobre 2022

Versione	Dettagli	Data di rilascio
1,32003824	• Errore risolto durante `setComputerName` . • Aggiunta una logica per ignorare l'attivazione di Windows quando viene rilevato un codice di fatturazione BYOL. • Aggiunta la crittografia delle password in memoria. • Errore risolto durante l'inizializzazione del volume su `m6id.4xlarge` .	30 agosto 2022
1,32003691	• La logica di attesa IMDS è stata aggiornata per effettuare solo richieste IMDSv2. • Corretto un bug che influisce sull'installazione di eGPU	21 giugno 2022
1,32003639	• Aggiunta la logica di attesa dell'adattatore di rete per impedire l'uso prima dell'inizializzazione. • Risolti problemi poco importanti.	10 maggio 2022
1,32003498	• Aggiunta della telemetria. • Aggiunto il collegamento all'interfaccia utente Impostazioni. • Script formattati. PowerShell • È stato risolto il problema relativo all'arresto che si verificava prima del completamento. BeforeSysprep.cmd	31 gennaio 2022
1.3.2003411	Modificata la logica di generazione delle password per escludere le password a bassa complessità.	4 agosto 2021

Versione	Dettagli	Data di rilascio
1,32003364	Aggiornato Install-EgpuManager con il supporto IMDSv2.	7 giugno 2021
1.3.2003312	• Aggiunte righe di log prima e dopo l'impostazione di `setMonitorAlwaysOn` . • È stata aggiunta la versione del AWS pacchetto Nitro Enclaves al registro della console.	04 maggio 2021
1.3.2003284	Modello di autorizzazione migliorato tramite l'aggiornamento della posizione in cui archiviare i dati dell'utente in `LocalAppData` .	23 marzo 2021
1.3.2003236	• Metodo aggiornato per l'impostazione della password utente in `Set-AdminAccount` e `Randomize-LocalAdminPassword` . • Risolto `InitializeDisks` in modo che verifichi se il disco è impostato per la sola lettura prima di impostarlo su scrivibile.	11 febbraio 2021
1.3.2003210	Correzione della localizzazione per `install.ps1` .	7 gennaio 2021
1.3.2003205	Correzione della protezione `install.ps1` per aggiornare le autorizzazioni sulla directory `%ProgramData%AmazonEC2-WindowsLaunchModuleScripts` .	28 dicembre 2020
1.3.2003189	Aggiunta di `w32tm resync` dopo avere aggiunto gli instradamenti.	4 dicembre 2020
1.3.2003155	Informazioni aggiornate sul tipo di istanza.	25 agosto 2020

Versione	Dettagli	Data di rilascio
1.3.2003150	Aggiunta di `OsCurrentBuild` e `OsReleaseId` all'output della console.	22 aprile 2020
1.3.2003040	Corretta la logica di fallback IMDS versione 1.	7 aprile 2020
1.3.2002730	Aggiunto il supporto per IMDS V2.	3 marzo 2020
1.3.2002240	Risolti problemi poco importanti.	31 ottobre 2019
1.3.2001660	È stato risolto il problema di accesso automatico per gli utenti senza password dopo la prima esecuzione di Sysprep.	2 luglio 2019
1.3.2001360	Risolti problemi poco importanti.	27 marzo 2019
1.3.2001220	Tutti PowerShell gli script sono firmati.	28 febbraio 2019
1.3.2001200	È stato risolto il problema a causa del InitializeDisks.ps1 quale l'esecuzione dello script su un nodo in un cluster di failover di Windows Server formava le unità sui nodi remoti la cui lettera di unità corrispondeva alla lettera dell'unità locale.	27 febbraio 2019
1.3.2001160	Risolto problema sfondo mancante in Windows 2019.	22 febbraio 2019
1.3.2001040	• Plugin aggiunto per impostare il monitor in modo che non si spenga mai per risolvere i problemi di ACPI. • Edizione di SQL Server e versione scritta nella console.	21 gennaio 2019
1.3.2000930	Correzione l'aggiunta di routing ai metadati su ENI abilitate per ipv6.	2 gennaio 2019

Versione	Dettagli	Data di rilascio
1.3.2000760	• Aggiunta la configurazione predefinita per RSS e le impostazioni Receive Queue per i dispositivi ENA. • Ibernazione disabilitata durante Sysprep.	5 dicembre 2018
1.3.2000630	• È stata aggiunta la route 169.254.169. 253/32 per server DNS. • Aggiunto il filtro dell'impostazione dell'utente Admin. • Migliorie apportate all'ibernazione delle istanze. • Aggiunta l'opzione per pianificare l'esecuzione di EC2Launch a ogni avvio.	9 novembre 2018
1.3.2000430.0	• Aggiunta la route 169.254.169. 123/32 al servizio orario AMZN. • Aggiunto il percorso 169.254.169. 249/32 al servizio di licenza GRID. • Aggiunto un timeout di 25 secondi durante il tentativo di avviare Systems Manager.	19 settembre 2018
1.3.200039.0	• Risolto un problema di aggiunta di una lettera di unità non corretta per i volumi EBS NVME. • Aggiunta un'attività di logging per le versioni dei driver NVME.	15 agosto 2018
1.3.2000080	Risolti problemi poco importanti.	
1.3.610	Problema risolto con il reindirizzamento dell'output e degli errori ai file dai dati utente.	

Versione	Dettagli	Data di rilascio
1.3.590	• Tipi di istanze mancanti aggiunti allo sfondo. • È stato risolto un problema con la mappatura delle lettere dell'unità e l'installazione del disco.	
1.3.580	• Risolto `Get-Metadata` per utilizzare le impostazioni predefinite del proxy di sistema per le richieste Web. • Aggiunto un caso speciale per NVMe nell'inizializzazione del disco. • Risolti problemi poco importanti.	
1.3.550	Aggiunta un'opzione `-NoShutdown` per attivare Sysprep senza spegnimento.	
1.3.540	Risolti problemi poco importanti.	
1.3.530	Risolti problemi poco importanti.	
1.3.521	Risolti problemi poco importanti.	
1.3.0	• Corretto un problema di lunghezza esadecimale per la modifica del nome del computer. • Corretto un possibile ciclo di riavvio per la modifica del nome del computer. • Risolto un problema nella configurazione dello sfondo.	

Versione	Dettagli	Data di rilascio
1.2.0	• Aggiornamento per visualizzare le informazioni sul sistema operativo (SO) installato nel log di sistema EC2. • Aggiornamento per visualizzare la versione di EC2Launch e SSM Agent nel log di sistema di EC2. • Risolti problemi poco importanti.	
1.1.2	• Aggiornamento per visualizzare le informazioni del driver ENA nel log di sistema di EC2. • Aggiornamento per escludere Hyper-V dalla logica del filtro NIC primario. • Aggiunti AWS KMS server e porta nella chiave di registro per l'attivazione del KMS. • Impostazione dello sfondo migliorata per più utenti. • Aggiornamento per cancellare i percorsi da uno store persistente. • Aggiornamento per rimuovere la z dalla zona di disponibilità nell'elenco dei suffissi DNS. • Aggiornamento per risolvere un problema con il tag <run AsLocalSystem > nei dati utente.	
1.1.1	Versione iniziale.	

Utilizza il servizio EC2Config per eseguire attività durante l'avvio dell'istanza del sistema operativo Windows legacy EC2

> **Note**
>
> EC2Config ha raggiunto la fine del supporto. Le versioni del sistema operativo su cui viene eseguito non sono più supportate da Microsoft. Consigliamo fortemente di eseguire l'aggiornamento all'agente di avvio più recente.
> L'agente di avvio più recente per Windows Server 2022 e versioni successive del sistema operativo è EC2Launch v2, che sostituisce sia EC2Config che EC2Launch ed è preinstallato sulle AMI Windows Server 2022 e 2025. AWS Puoi anche installare e configurare manualmente l'agente su Windows Server 2016 e 2019. Per ulteriori informazioni, consulta Installare EC2Launch v2.

Le AMI di Windows per le versioni Windows Server precedenti a Windows Server 2016 includono un servizio opzionale, il servizio EC2 Config (`EC2Config.exe`). EC2Config comincia nel momento in cui l'istanza avvia ed esegue attività durante il startup iniziale dell'istanza e tutte le volte che questa viene arrestata o avviata. EC2Config può anche eseguire attività su richiesta. Alcune di queste attività sono abilitate automaticamente, mentre altre devono essere abilitate manualmente. Sebbene il servizio sia opzionale, fornisce accesso a caratteristiche avanzate che altrimenti non sarebbero disponibili. Questo servizio viene eseguito nell'account. LocalSystem

Il servizio EC2Config esegue Sysprep, uno strumento Microsoft che ti permette di creare un'AMI di Windows personalizzato che può essere riutilizzato. Quando EC2Config chiama Sysprep, utilizza i file contenuti in `%ProgramFiles%\Amazon\EC2ConfigService\Settings` per determinare quali operazioni eseguire. Puoi modificare questi file in maniera indiretta tramite la finestra di dialogo di sistema Proprietà del servizio EC2 oppure direttamente utilizzando un editor di testo o XML. Tuttavia esistono alcune impostazioni avanzate che non sono disponibili nella finestra di dialogo di sistema Proprietà del servizio EC2, quindi è necessario modificare direttamente queste voci.

Se crei un'AMI da un'istanza dopo l'aggiornamento delle sue impostazioni, le nuove impostazioni vengono applicate a ogni istanza lanciata dalla nuova AMI. Per informazioni sulla creazione di un'AMI, consulta Crea un' EBS-backed AMI Amazon.

EC2Config utilizza i file di configurazione per controllare la sua operazione. È possibile aggiornare questi file di configurazione usando uno strumento grafico oppure modificando direttamente i file

XML. I binari di servizio e dei file aggiuntivi sono contenuti nella directory `%ProgramFiles%\Amazon\EC2ConfigService`.

Indice

- EC2Config e AWS Systems Manager
- Attività di EC2Config
- File delle impostazioni di EC2Config
- Installazione della versione più recente di EC2Config
- Configurazione delle impostazioni proxy .NET per il servizio EC2Config
- Imposta le proprietà del servizio EC2Config dalla finestra di dialogo di sistema sull'istanza EC2 Windows
- Risoluzione dei problemi relativi all'agente di avvio EC2Config
- Cronologia delle versioni di EC2Config

EC2Config e AWS Systems Manager

Il servizio EC2Config elabora le richieste Systems Manager sulle istanze create dalle AMI per le versioni di Windows Server precedenti a Windows Server 2016 che sono state pubblicate prima di novembre 2016.

Le istanze create dalle AMI, per le versioni di Windows Server precedenti a Windows Server 2016 che sono state pubblicate prima di novembre 2016, includono il servizio EC2Config e SSM Agent. EC2Config esegue tutte le attività descritte precedentemente, mentre SSM Agent elabora le richieste per le funzionalità di Systems Manager come Run Command e Gestione stato.

Puoi utilizzare Run Command per aggiornare le istanze esistenti al fine di utilizzare la versione recente del servizio EC2Config e di SSM Agent. Per ulteriori informazioni, consulta Update SSM Agent using Run Command nella Guida per l'utente di AWS Systems Manager .

Attività di EC2Config

Quando l'istanza viene avviata per la prima volta, EC2Config esegue le attività relative al startup iniziale, quindi le disabilita. Per eseguire nuovamente queste attività, è necessario abilitarle in maniera esplicita prima di arrestare l'istanza o eseguire manualmente Sysprep. Si tratta delle seguenti attività:

- Impostare una password crittografata e casuale per l'account dell'amministratore.

- Generare e installare il certificato dell'host per la Connessione Desktop in remoto.
- Estendere in modo dinamico la partizione del sistema operativo per includere qualsiasi spazio non partizionato.
- Esegue i dati utente specificati (e Cloud-Init, se installati). Per ulteriori informazioni sulla specifica dei dati utente, consulta Esegui i comandi quando avvii un'istanza EC2 con l'input dei dati utente.

EC2Config esegue le seguenti attività ogni volta che viene avviata l'istanza:

- Cambia il nome host in modo che corrisponda all'indirizzo IP privato in notazione esadecimale (questa attività è disabilitata per impostazione predefinita e deve essere abilitata per l'esecuzione all'avvio dell'istanza).
- Configura il server della gestione della chiave (AWS KMS), verifica lo stato di attivazione di Windows e attiva Windows quando necessario.
- Monta tutti i volumi di Amazon EBS e i volumi instance store; mappa i nomi del volume per le lettere di unità.
- Scrivi le voci del registro degli eventi nella console per facilitare la risoluzione dei problemi (questa attività è disabilitata per impostazione predefinita e deve essere abilitata per l'esecuzione all'avvio dell'istanza).
- Scrive alla console quando Windows è pronto.
- Aggiungere un percorso personalizzato alla scheda di rete primaria in modo da abilitare i seguenti indirizzi IP quando vengono collegate una singola scheda NIC o più schede NIC: `169.254.169.250`, `169.254.169.251` e `169.254.169.254`. Questi indirizzi vengono utilizzati dall'attivazione di Windows e quando si accede ai metadati dell'istanza.

> **Note**
>
> Se il sistema operativo Windows è configurato per l'utilizzo di IPv4, è possibile utilizzare questi indirizzi locali di collegamento IPv4. Se il sistema operativo Windows ha lo stack del protocollo di rete IPv4 disabilitato e utilizza invece IPv6, aggiungere `[fd00:ec2::250]` al posto di `169.254.169.250` e `169.254.169.251`. Quindi aggiungere `[fd00:ec2::254]` al posto di `169.254.169.254`.

EC2Config esegue le seguenti attività ogni volta che un utente effettua l'accesso:

- Mostra informazioni a schermo sullo sfondo del desktop.

Mentre l'istanza è in esecuzione, puoi richiedere che EC2Config esegua la seguente attività su richiesta:

- Esegue Sysprep e arresta l'istanza per poter creare un'AMI da questa attività. Per ulteriori informazioni, consulta Creare un'AMI Amazon EC2 utilizzando Windows Sysprep.

File delle impostazioni di EC2Config

I file di impostazione controllano l'operazione del servizio EC2Config. Questi file si trovano nella directory `C:\Program Files\Amazon\Ec2ConfigService\Settings`:

- `ActivationSettings.xml`: controlla l'attivazione del prodotto tramite un server di gestione della chiave (AWS KMS).
- `AWS.EC2.Windows.CloudWatch.json`—Controlla a quali contatori delle prestazioni inviare CloudWatch e quali registri inviare a Logs. CloudWatch
- `BundleConfig.xml` – Controlla in che modo EC2Config prepara un'istanza supportata dall'instance store per la creazione delle AMI.
- `Config.xml` – Controlla le impostazioni primarie.
- `DriveLetterConfig.xml` – Controlla le mappature delle lettere di unità.
- `EventLogConfig.xml` – Controlla le informazioni dei log evento mostrati sulla console all'avvio dell'istanza.
- `WallpaperSettings.xml` – Controlla le informazioni mostrate sullo sfondo del desktop.

ActivationSettings.xml

Questo file contiene le impostazioni che controllano l'attivazione del prodotto. All'avvio di Windows, il servizio EC2Config verifica se Windows è già stato attivato. Se Windows non è stato ancora attivato, il servizio prova ad attivarlo cercando lo specifico server AWS KMS .

- `SetAutodiscover`: indica se un AWS KMS verrà rilevato automaticamente.
- `TargetKMSServer`—Memorizza l'indirizzo IP privato di un. AWS KMS Il AWS KMS deve trovarsi nella stessa regione della tua istanza.
- `DiscoverFromZone`—Rileva il AWS KMS server dalla zona DNS specificata.
- `ReadFromUserData`—Ottiene il server da. AWS KMS UserData
- `LegacySearchZones`—Rileva il AWS KMS server dalla zona DNS specificata.

- `DoActivate` – Tenta l'attivazione tramite le impostazioni specificate nella sezione. Questo valore può essere `true` o `false`.
- `LogResultToConsole` – Mostra i risultati sulla console.

BundleConfig.xml

Questo file contiene le impostazioni che controllano in che modo EC2Config prepara un'istanza per la creazione di AMI.

- `AutoSysprep` – Indica la possibilità di utilizzare Sysprep in modo automatico. Modifica il valore su `Yes` per utilizzare Sysprep.
- `SetRDPCertificate` – Imposta un certificato autofirmato per il server del desktop remoto. Questa operazione ti permette di utilizzare l'RDP in modo sicuro nell'istanza. Modifica il valore su `Yes` se la nuova istanza possiede il certificato.

  Questa impostazione non si utilizza per istanze con versioni del sistema operativo precedenti a Windows Server 2016, perché possono di generare i propri certificati.
- `SetPasswordAfterSysprep` – Imposta una password casuale in un'istanza appena avviata, la crittografa con la chiave di lancio dell'utente e invia la password crittografata alla console. Modifica il valore di questa impostazione su `No` se le nuove istanze non sono impostate per creare una password criptata casuale.

Config.xml

Plug-ins

- `Ec2SetPassword` – Genera una password criptata casuale ogni volta che avvii un'istanza. Questa caratteristica si disattiva per impostazione predefinita dopo il primo lancio, affinché il riavvio di questa istanza non modifichi una password impostata dall'utente. Modifica questa impostazione su `Enabled` per continuare a generare password ogni volta che lanci un'istanza.

  Questa impostazione è importante se si desidera creare un'AMI dalla propria istanza.
- `Ec2SetComputerName` – Imposta il nome host dell'istanza come nome univoco basato sull'indirizzo IP dell'istanza e la riavvia. Per impostare il tuo nome host o per prevenire che il nome host esistente venga modificato, è necessario disabilitare questa impostazione.
- `Ec2InitializeDrives` – Inizializza e formatta tutti i volumi durante il startup. Questa caratteristica viene attivata per impostazione predefinita.

- `Ec2EventLog` – Mostra le voci di log evento nella console. Per impostazione predefinita, vengono mostrate le tre voci di errore più recenti dai log evento del sistema. Per specificare quali voci di log evento mostrare, modifica il file `EventLogConfig.xml` che si trova nella directory `EC2ConfigService\Settings`. Per informazioni riguardanti le impostazioni in questo file, consulta la pagina relativa alla Chiave Eventlog.
- `Ec2ConfigureRDP` – Imposta un certificato autofirmato sull'istanza, così che gli utenti possano accedere in modo sicuro all'istanza tramite il desktop remoto. Questa impostazione non si utilizza per istanze con versioni del sistema operativo precedenti a Windows Server 2016, perché possono di generare i propri certificati.
- `Ec2OutputRDPCert` – Mostra le informazioni del certificato del desktop remoto sulla console, così che l'utente possa verificarlo con quello dell'identificazione personale.
- `Ec2SetDriveLetter` – Imposta le lettere di unità dei volumi montati secondo le impostazioni definite dall'utente. Per impostazione predefinita, quando un volume Amazon EBS viene collegato a un'istanza, questa non può essere montata tramite la lettera di unità nell'istanza. Per specificare le mappature della lettera di unità, modifica il file `DriveLetterConfig.xml` che si trova nella directory `EC2ConfigService\Settings`.
- `Ec2WindowsActivate` – Il plug-in gestisce l'attivazione di Windows. Esegue una verifica per controllare se Windows è stato attivato. In caso contrario, aggiorna le impostazioni del AWS KMS client e quindi attiva Windows.

  Per modificare le AWS KMS impostazioni, modifica il `ActivationSettings.xml` file che si trova nella `EC2ConfigService\Settings` directory.
- `Ec2DynamicBootVolumeSize`—Estende il disco 0/Volume 0 per includere qualsiasi spazio non partizionato.
- `Ec2HandleUserData` — Crea ed esegue gli script creati dall'utente al momento del primo avvio di un'istanza, dopo che Sysprep viene eseguito. I comandi racchiusi nei tag di script vengono salvati in un file batch e i comandi racchiusi nei PowerShell tag vengono salvati in un file .ps1 (corrisponde alla casella di controllo Dati utente nella finestra di dialogo del sistema Ec2 Service Properties).
- `Ec2ElasticGpuSetup` – Installa il pacchetto software delle GPU Elastiche, se l'istanza è associata a una GPU elastica.
- `Ec2FeatureLogging` – Invia a Windows l'installazione della funzionalità e il corrispondente stato dei servizi alla console. Supportato solo per la Hyper-V funzionalità Microsoft e il corrispondente servizio vmms.

Impostazioni generali

- `ManageShutdown`—Assicura che le istanze avviate dalle S3-backed AMI Amazon non vengano terminate durante l'esecuzione di Sysprep.
- `SetDnsSuffixList` – Abilita il suffisso DNS della scheda di rete per Amazon EC2. Questa operazione consente la risoluzione DNS dei server in esecuzione su Amazon EC2 senza fornire il nome di dominio completo.

  > **Note**
  >
  > Ciò aggiunge una ricerca dei suffissi DNS per il seguente dominio e configura altri suffissi standard. Per ulteriori informazioni sul modo in cui gli agenti di lancio impostano i suffissi DNS, consultare Configura il suffisso DNS per gli agenti di avvio EC2 Windows.
  >
  > ```
  > region.ec2-utilities.amazonaws.com
  > ```

- `WaitForMetaDataAvailable` – Assicura che il servizio EC2Config attenderà che i metadati siano accessibili e che la rete sia disponibile prima di proseguire con l'avvio. Questa verifica assicura che EC2Config riesca a ottenere informazioni dai metadati per l'attivazione e per gli altri plug-in.
- `ShouldAddRoutes` – Aggiunge un percorso personalizzato per la scheda di rete primaria in modo da abilitare i seguenti indirizzi IP quando vengono collegate più schede NIC: 169.254.169.250, 169.254.169.251 e 169.254.169.254. Questi indirizzi vengono utilizzati dall'attivazione di Windows e quando si accede ai metadati dell'istanza.
- `RemoveCredentialsfromSyspreponStartup`—Rimuove la password dell'amministratore da `Sysprep.xml` al successivo avvio del servizio. Per essere sicuro che questa password persista, modifica questa impostazione.

DriveLetterConfig.xml

Questo file contiene le impostazioni che controllano le mappature della lettera di unità. Per impostazione predefinita, un volume può essere mappato su qualsiasi lettera di unità disponibile. È possibile montare un volume su una determinata lettera di unità come segue.

```
<?xml version="1.0" standalone="yes"?>
<DriveLetterMapping>
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
```

```
  </Mapping>
  . . .
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
</DriveLetterMapping>
```

- `VolumeName` – L'etichetta del volume. Ad esempio, *`My Volume`*. Per specificare una mappatura per un volume dello archiviazione dell'istanza, utilizzare l'etichetta `Temporary Storage X`, dove `X` è un numero compreso tra 0 e 25.
- `DriveLetter`—La lettera dell'unità. Ad esempio, *`M:`*. Se la lettera di unità è già in uso, la mappatura avrà esito negativo.

EventLogConfig.xml

Questo file contiene le impostazioni che controllano le informazioni dei log evento mostrati sulla console all'avvio dell'istanza. Per impostazione predefinita, vengono mostrate le tre voci di errore più recenti dai log evento di sistema.

- `Category` – La chiave del log evento da monitorare.
- `ErrorType` – Il tipo di evento, ad esempio `Error`, `Warning`, `Information`.
- `NumEntries` – Il numero di eventi archiviati per questa categoria.
- `LastMessageTime` – Per evitare che lo stesso messaggio venga inviato ripetutamente, il servizio aggiorna questo valore ogni volta che viene inviato un messaggio.
- `AppName` – L'origine o l'applicazione dell'evento che lo ha registrato.

WallpaperSettings.xml

Questo file contiene le impostazioni che controllano le informazioni mostrate sullo sfondo del desktop. Le seguenti informazioni sono mostrate per impostazione predefinita.

- `Hostname` – Mostra il nome del computer.
- `Instance ID` – Mostra l'ID dell'istanza.
- `Public IP Address` – Mostra l'indirizzo IP pubblico dell'istanza.
- `Private IP Address` – Mostra l'indirizzo IP privato dell'istanza.

- `Availability Zone` – Mostra la zona di disponibilità in cui viene eseguita l'istanza.
- `Instance Size` – Mostra il tipo di istanza.
- `Architecture` – Mostra l'impostazione della variabile ambiente `PROCESSOR_ARCHITECTURE`.

Cancellando la voce di una qualsiasi informazione mostrata come predefinita, è possibile rimuoverla. Puoi aggiungere ulteriori metadati dell'istanza affinché vengano mostrati come di seguito.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>metadata</source>
  <identifier>meta-data/path</identifier>
</WallpaperInformation>
```

Puoi aggiungere ulteriori variabili ambiente del sistema affinché vengano mostrate come di seguito.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>EnvironmentVariable</source>
  <identifier>variable-name</identifier>
</WallpaperInformation>
```

InitializeDrivesSettings.xml

Questo file contiene le impostazioni che controllano in che modo EC2Config inizializza i drive.

Per impostazione predefinita, EC2Config inizializza i drive che non sono stati messi online dal sistema operativo. Puoi personalizzare il plug-in come di seguito.

```
<InitializeDrivesSettings>
    <SettingsGroup>setting</SettingsGroup>
</InitializeDrivesSettings>
```

Utilizza un gruppo di impostazioni per specificare in che modo desideri inizializzare i drive:

FormatWithTRIM

> Abilita il comando TRIM al momento della formattazione dei drive. Dopo che un drive è stato formattato e inizializzato, il sistema ripristina la configurazione TRIM.

A partire dalla versione 3.18 di EC2Config, il comando TRIM viene disabilitato per impostazione predefinita durante l'operazione di formato disco. Tutto ciò migliora il tempo di formattazione. Utilizza questa impostazione per abilitare il comando TRIM durante l'operazione di formato disco, per le versioni 3.18 e successive di EC2Config.

FormatWithoutRIFINISCI

Disabilita il comando TRIM quando si formattano i drive e migliora i tempi di formattazione su Windows. Dopo che un drive è stato formattato e inizializzato, il sistema ripristina la configurazione TRIM.

DisableInitializeDrives

Disabilita la formattazione per i nuovi drive. Utilizza questa impostazione per inizializzare manualmente i drive.

Installazione della versione più recente di EC2Config

> **Note**
>
> L'agente di avvio più recente per Windows Server 2022 e versioni successive del sistema operativo è EC2Launch v2, che sostituisce sia EC2Config che EC2Launch. EC2Launch v2 è preinstallato sulle AMI AWS Windows Server 2022 e 2025. Puoi anche installare e configurare manualmente l'agente su Windows Server 2016 e 2019. Per ulteriori informazioni, consulta Installare EC2Launch v2.

Per informazioni su come ricevere notifiche sugli aggiornamenti di EC2Config, consulta Sottoscrizione alle notifiche dell'agente di avvio EC2 Windows. Per informazioni sulle variazioni di ogni versione, consulta Cronologia delle versioni di EC2Config.

Prima di iniziare

- Verifica di possedere la versione 3.5 SP1 o successiva di .NET framework.
- Per impostazione predefinita, l'opzione Setup sostituisce i tuoi file di configurazione con dei file di configurazione predefiniti durante l'installazione; inoltre riavvia il servizio EC2Config quando viene completata l'installazione. Se hai modificato le impostazioni del servizio EC2Config, copia il file `config.xml` dalla directory `%Program Files%\Amazon\Ec2ConfigService\Settings`. Dopo aver aggiornato il servizio EC2Config, puoi ripristinare questo file per mantenere le modifiche della configurazione.

Verificare la versione di EC2Config

Utilizza la procedura seguente per verificare la versione di EC2Config installata sulla tua istanza.

Per verificare la versione installata di EC2Config

1. Lancia un'istanza dall'AMI e connettila.
2. Sul pannello di controllo, seleziona Programs and Features (Programmi e caratteristiche).
3. Sulla lista dei programmi installati, cerca `Ec2ConfigService`. Il numero della versione viene mostrato nella colonna Version (Versione).

Aggiornamento di EC2Config

Per scaricare e installare la versione più recente di EC2Config sulle istanze, attenersi alla procedura seguente.

Scaricare e installare la versione più recente di EC2Config

1. Scarica e decomprimi il programma di installazione di EC2Config.
2. Esegui `EC2Install.exe`. Per un elenco completo delle opzioni, esegui `EC2Install` con l'opzione `/?`. Per impostazione predefinita, la configurazione mostra i prompt. Per eseguire il comando senza alcun prompt, utilizza l'opzione `/quiet`.

   > **Important**
   >
   > Per mantenere le impostazioni personalizzate dal file `config.xml` che hai salvato, esegui `EC2Install` con l'opzione `/norestart`, ripristina le tue impostazioni e riavvia manualmente il servizio EC2Config.

3. Se stai eseguendo la versione 4.0 o successiva di EC2Config, sarà necessario riavviare SSM Agent sull'istanza dall'applicazione Microsoft Services.

   > **Note**
   >
   > Le informazioni aggiornate sulla versione di EC2Config non verranno visualizzate nel Log di sistema o nel controllo di Trusted Advisor dell'istanza fino a che non viene riavviata o arrestata e avviata l'istanza.

Per scaricare e installare la versione più recente di EC2Config utilizzando PowerShell

Per scaricare, decomprimere e installare l'ultima versione di EC2Config utilizzando PowerShell, esegui i seguenti comandi da una finestra: PowerShell

```
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Config/EC2Install.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\" + $(Split-Path -Path $Url -Leaf)
$ExtractPath = "$env:USERPROFILE\Desktop\"
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$ExtractShell = New-Object -ComObject Shell.Application
$ExtractFiles = $ExtractShell.Namespace($DownloadZipFile).Items()
$ExtractShell.NameSpace($ExtractPath).CopyHere($ExtractFiles)
Start-Process $ExtractPath
Start-Process `
    -FilePath $env:USERPROFILE\Desktop\EC2Install.exe `
    -ArgumentList "/S"
```

> **Note**
>
> Se ricevi un errore durante il download del file e stai utilizzando Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il tuo terminale. PowerShell Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il comando seguente e riprovare:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```

Verifica dell'installazione controllando `C:\Program Files\Amazon\` per la directory `Ec2ConfigService`.

Configurazione delle impostazioni proxy .NET per il servizio EC2Config

È possibile configurare il servizio EC2Config per comunicare tramite un proxy utilizzando uno dei seguenti metodi: l' AWS SDK per .NET, l'`system.net`elemento o Microsoft Group Policy e Internet Explorer. L'utilizzo dell' AWS SDK per .NET è il metodo preferito perché è possibile specificare le credenziali di accesso.

Metodi

- Configura le impostazioni del proxy utilizzando AWS SDK per .NET (Preferito)
- Configurazione delle impostazioni proxy utilizzando l'elemento system.net

- Configurazione delle impostazioni proxy con la policy del gruppo Microsoft e con Microsoft Internet Explorer

Configura le impostazioni del proxy utilizzando AWS SDK per .NET (Preferito)

Puoi configurare le impostazioni del proxy per il servizio EC2Config specificando l'elemento `proxy` nel file `Ec2Config.exe.config`. Per ulteriori informazioni, consulta Configuration Files Reference for AWS SDK for .NET.

Per specificare l'elemento proxy in Ec2Config.exe.config

1. Modifica il file `Ec2Config.exe.config` sull'istanza dove desideri che il servizio EC2Config comunichi attraverso un proxy. Per impostazione predefinita, il file si trova nella directory seguente: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Aggiungi il seguente elemento `aws` sulla `configSections`. Non aggiungerlo per nessun `sectionGroups` esistente.

   Per la versione 3.17 di EC2Config o precedente

   ```
   <configSections>
      <section name="aws" type="Amazon.AWSSection, AWSSDK"/>
   </configSections>
   ```

   Per la versione 3.18 di EC2Config o successiva

   ```
   <configSections>
        <section name="aws" type="Amazon.AWSSection, AWSSDK.Core"/>
   </configSections>
   ```
3. Aggiungi il seguente elemento `aws` per il file `Ec2Config.exe.config`.

   ```
   <aws>
      <proxy
        host="string value"
        port="string value"
        username="string value"
        password="string value" />
   </aws>
   ```
4. Salva le modifiche.

Configurazione delle impostazioni proxy utilizzando l'elemento system.net

Puoi specificare le impostazioni del proxy in un elemento `system.net` sul file `Ec2Config.exe.config`. Per ulteriori informazioni, consulta la pagina relativa all'elemento defaultProxy (impostazioni di rete).

Per specificare l'elemento system.net in Ec2Config.exe.config

1. Modifica il file `Ec2Config.exe.config` sull'istanza dove desideri che il servizio EC2Config comunichi attraverso un proxy. Per impostazione predefinita, il file si trova nella directory seguente: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Aggiungi una voce `defaultProxy` per `system.net`. Per ulteriori informazioni, consulta la pagina relativa all'elemento defaultProxy (impostazioni di rete).

   La seguente configurazione, ad esempio, instrada tutto il traffico per consentire l'uso del proxy attualmente configurato per Internet Explorer, fatta eccezione per il traffico dei metadati e della licenza, che ignoreranno il proxy.

   ```
   <defaultProxy>
       <proxy usesystemdefault="true" />
       <bypasslist>
           <add address="169.254.169.250" />
           <add address="169.254.169.251" />
           <add address="169.254.169.254" />
           <add address="[fd00:ec2::250]" />
           <add address="[fd00:ec2::254]" />
       </bypasslist>
   </defaultProxy>
   ```
3. Salva le modifiche.

Configurazione delle impostazioni proxy con la policy del gruppo Microsoft e con Microsoft Internet Explorer

Il servizio EC2Config esegue l'account utente nel LocalSystem. Dopo aver modificato le impostazioni della policy del gruppo sull'istanza, puoi specificare le impostazioni del proxy di tutte le istanze per l'account su Internet Explorer.

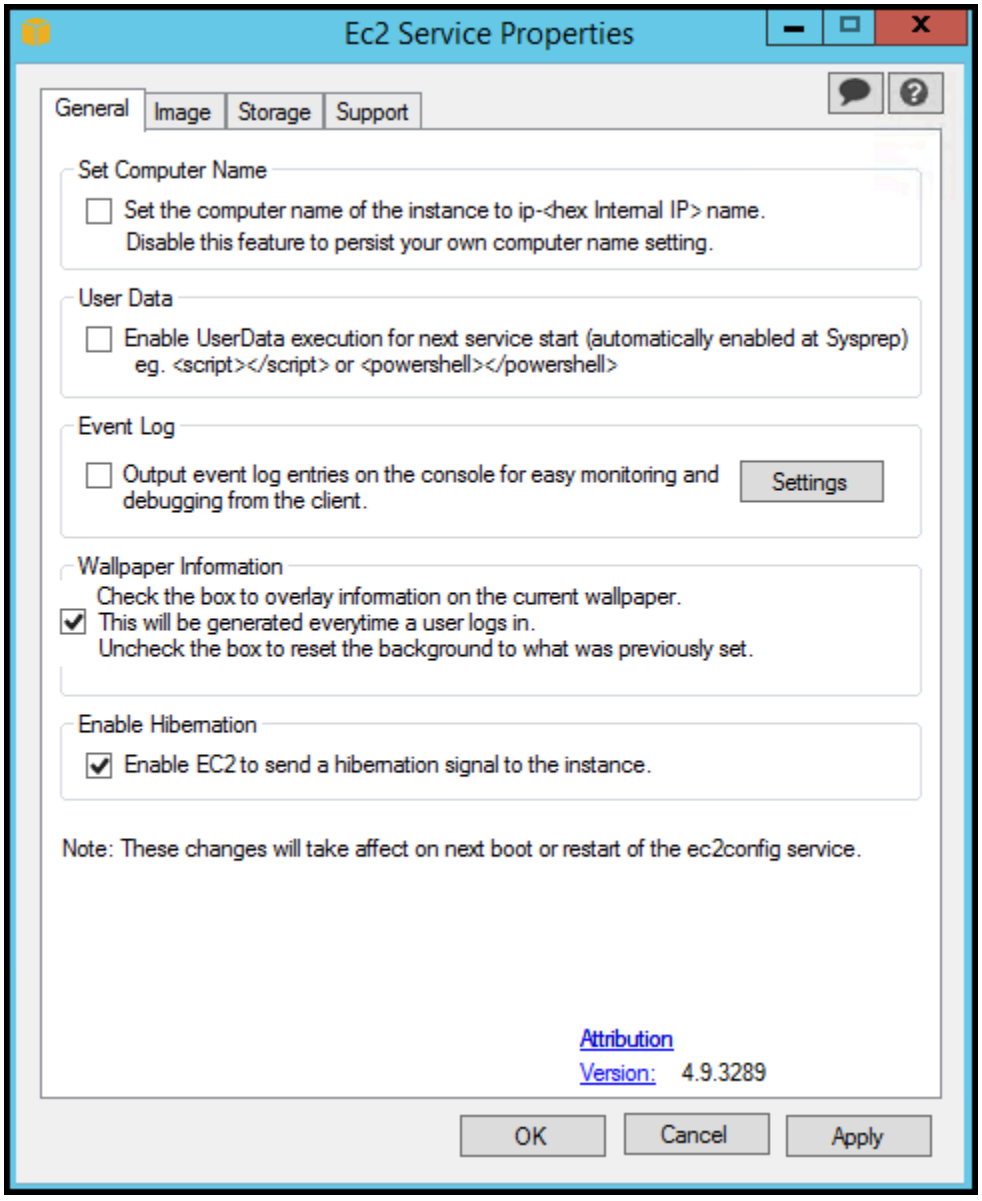
Per configurare le impostazioni del proxy con la policy del gruppo e Internet Explorer

1. Sull'istanza dove desideri che il servizio EC2Config comunichi attraverso un proxy, apri un prompt Command (Comando) come amministratore, digita **`gpedit.msc`** e premi Invio.
2. Nell'editor della policy del gruppo locale, su Local Computer Policy (Policy computer locale), scegli Computer Configuration (Configurazione del computer), Administrative Templates (Modelli amministrativi), Windows Components (Componenti di Windows), Internet Explorer.
3. Nel riquadro a destra, scegli Make proxy settings per-machine (rather than per-user) (Attiva impostazioni proxy per la macchina, anziché per l'utente), quindi scegli Edit policy setting (Modifica impostazione proxy).
4. Seleziona Enabled (Abilitato), quindi Apply (Applica).
5. Apri Internet Explorer e scegli il pulsante Tools (Strumenti).
6. Seleziona Internet Option (Opzioni internet), quindi scegli la scheda Connections (Connessioni).
7. Seleziona LAN settings (Impostazioni LAN).
8. Sotto Proxy server (Server proxy), scegliere l'opzione Use a proxy server for your LAN (Usa un server proxy per la LAN).
9. Specifica le informazioni della porta e dell'indirizzo e scegli OK.

Imposta le proprietà del servizio EC2Config dalla finestra di dialogo di sistema sull'istanza EC2 Windows

La procedura seguente descrive come utilizzare la finestra di dialogo Proprietà del servizio EC2 per abilitare o disabilitare le impostazioni.

1. Avviare l'istanza Windows e connettersi a essa.
2. Dal menu Start, scegli Tutti i programmi, quindi scegli EC2ConfigService Impostazioni.



3. Nella scheda General (Generali) della finestra di dialogo di sistema Proprietà del servizio EC2, è possibile abilitare o disabilitare le seguenti impostazioni.

   Set Computer Name (Imposta il nome del computer)

   Se questa impostazione è abilitata (è disabilitata per impostazione predefinita), il nome host viene confrontato con il corrente indirizzo IP interno a ogni avvio. Se il nome host e l'indirizzo IP interno non corrispondono, il nome host viene ripristinato per contenere l'indirizzo IP interno; quindi il sistema si riavvia per prendere il nuovo nome host. Per impostare il tuo nome host o per prevenire che il nome host esistente venga modificato, non abilitare questa opzione.

User Data (Dati utente)

L'esecuzione dei dati utente ti permette di specificare gli script nei metadati dell'istanza. Per impostazione predefinita, questi script vengono eseguiti durante il lancio iniziale. Inoltre, puoi configurare gli script per eseguirli al prossimo avvio e riavvio dell'istanza o ogni volta che avvii o riavvii l'istanza.

Se possiedi uno script di grandi dimensioni, ti raccomandiamo di utilizzare i dati utente per scaricare lo script per poi eseguirlo.

Per ulteriori informazioni, consulta Esecuzione dei dati utente.

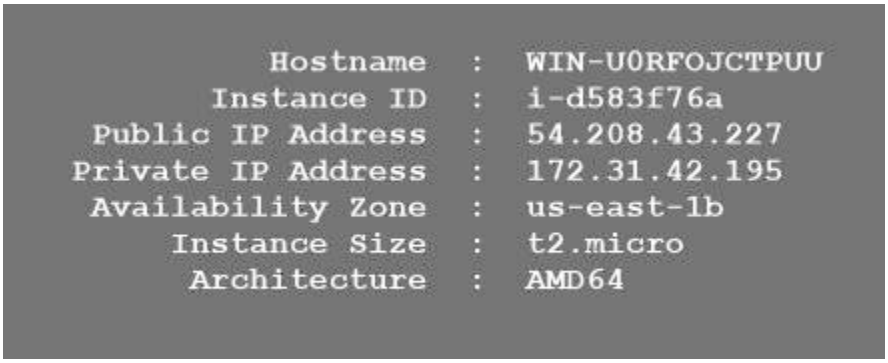
Event Log (Log eventi)

Utilizza questa impostazione per mostrare le voci dei log evento sulla console all'avvio, così da poter effettuare più facilmente il monitoraggio e il debug.

Scegli Impostazioni per specificare i filtri per le voci di registro inviate alla console. Il filtro predefinito invia le tre voci di errore più recenti dai log evento di sistema alla console.

Wallpaper Information (Informazioni sfondo)

Utilizza questa impostazione per mostrare le informazioni di sistema sullo sfondo del desktop. L'esempio seguente riguarda le informazioni mostrate sullo sfondo del desktop

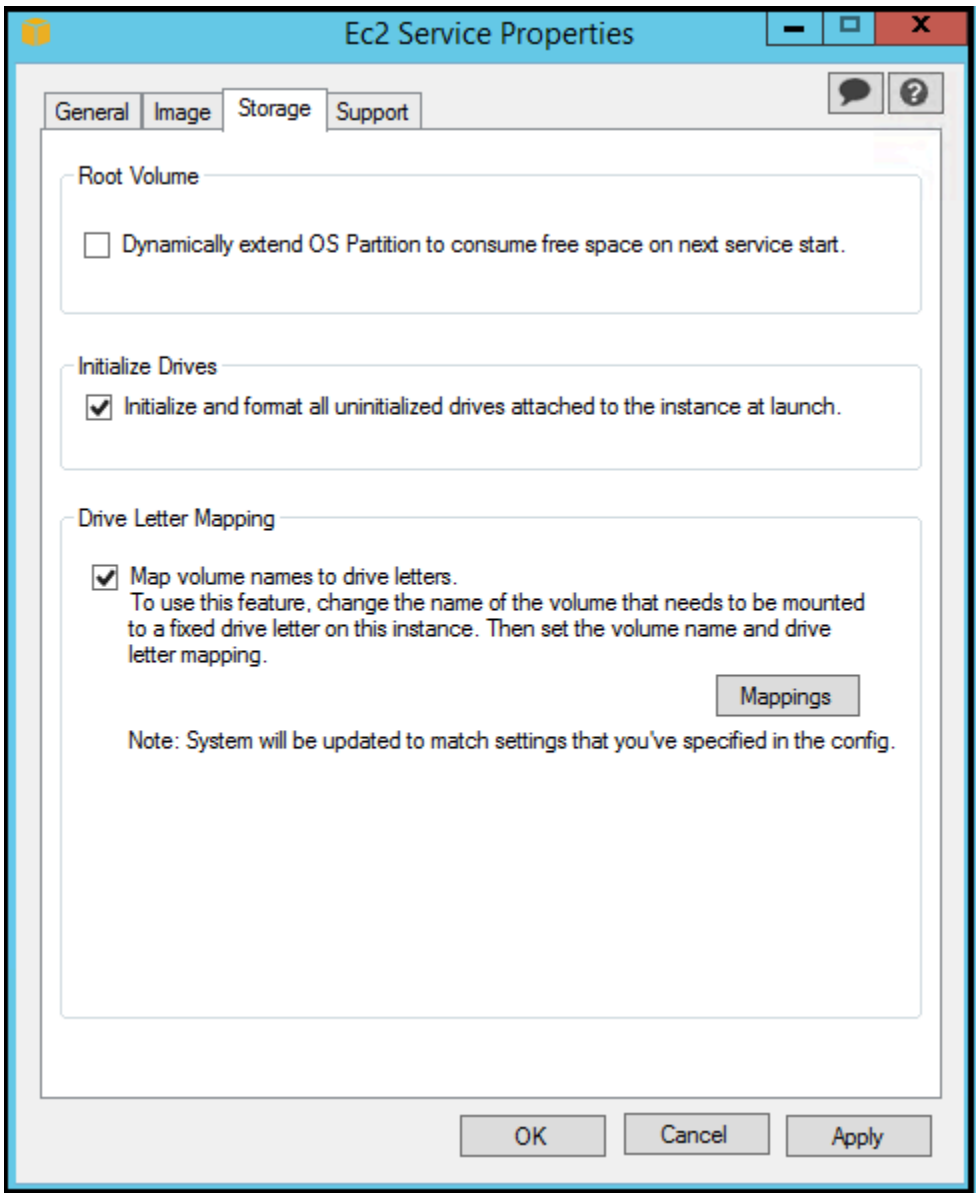


Le informazioni mostrate sullo sfondo del desktop sono controllate dal file delle impostazioni `EC2ConfigService\Settings\WallpaperSettings.xml`.

Abilitazione ibernazione

Utilizza questa impostazione affinché EC2 sia in grado di segnalare al sistema operativo di eseguire l'ibernazione.

4. Scegli la scheda Archiviazione. Puoi abilitare o disabilitare le seguenti impostazioni.



Root Volume (Volume root)

Questa impostazione estende dinamicamente il disco 0/Volume 0 per includere qualsiasi spazio non partizionato. Ciò può essere utile quando l'istanza viene avviata da un volume root di dimensioni personalizzate.

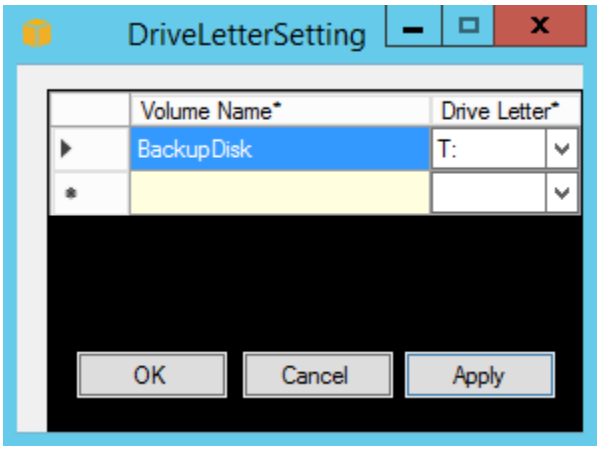
Initialize Drives (Inizializza unità)

Questa impostazione formatta e monta tutti i volumi collegati all'istanza durante l'avvio.

Drive Letter Mapping (Mappatura lettera unità)

Il sistema mappa i volumi collegati a un'istanza per le lettere di unità. Per i volumi Amazon EBS, l'impostazione predefinita assegna le lettere di unità che vanno dalla D: alla Z:. Ad esempio, memorizza i volumi, l'impostazione predefinita dipende dal driver. AWS I driver PV e i driver Citrix PV assegnano ai volumi degli archivi delle istanze le lettere di unità che vanno da Z: ad A:. I driver Red Hat assegnano, ai volumi instance store, lettere di unità che vanno dalla D: alla Z:.

Per scegliere le lettere unitarie per i volumi, scegliete Mappings. Nella DriveLetterSetting finestra di dialogo, specificate i valori del nome del volume e della lettera di unità per ciascun volume, scegliete Applica, quindi scegliete OK. Ti raccomandiamo di selezionare lettere di unità che evitino conflitti con lettere di unità che potrebbero essere in uso, come le lettere di unità al centro dell'alfabeto.



Dopo aver specificato una mappatura della lettera di unità e collegato un volume con la stessa etichetta dei nomi volume specificati, EC2Config assegna automaticamente la lettera di unità specificata per quel volume. Tuttavia, se la lettera di unità è già in uso, la mappatura della lettera di unità avrà esito negativo. Nota che EC2Config, non modifica le lettere di unità dei volumi che sono già stati montati dopo aver specificato la mappatura della lettera di unità.

5. Per salvare le impostazioni e continuare a lavorarci in seguito, scegli OK per chiudere la finestra di dialogo del sistema EC2 Service Properties. Se hai terminato con la personalizzazione della tua istanza e desideri creare un'AMI da quella istanza, consulta Creare un'AMI Amazon EC2 utilizzando Windows Sysprep.

Risoluzione dei problemi relativi all'agente di avvio EC2Config

Le informazioni seguenti possono essere utili per risolvere i problemi con il servizio EC2Config

Aggiornamento di EC2Config su un'istanza irraggiungibile

Utilizza la procedura seguente per aggiornare il servizio EC2Config su un'istanza Windows Server inaccessibile tramite desktop remoto.

Per aggiornare EC2Config su un'istanza Amazon EBS-backed Windows a cui non puoi connetterti

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Individua l'istanza interessata. Selezionare l'istanza e scegliere Instance state (Stato istanza), quindi Stop (Arresta).

   > **Warning**
   >
   > Quando si arresta un'istanza, i dati sui volumi dell'archivio di istanze vengono persi. Per preservare questi dati, esegui il backup su uno storage persistente.

4. Scegli Launch instances (Avvia le istanze) e crea un'istanza temporanea `t2.micro` nella stessa Zona di disponibilità dell'istanza interessata. Utilizza un'AMI differente rispetto a quella utilizzata per lanciare l'istanza interessata.

   > **Important**
   >
   > Se non crei l'istanza nella stessa Zona di disponibilità dell'istanza interessata, non potrai collegare il volume root dell'istanza interessata sulla nuova istanza.

5. Nella console EC2, scegliere Volumes (Volumi).
6. Individua il volume root dell'istanza interessata. Scollega il volume e collega il volume all'istanza temporanea creata in precedenza. Collegala con il nome del dispositivo predefinito (xvdf).
7. Utilizzare Desktop remoto per collegarsi all'istanza temporanea, quindi usare l'utilità Disk Management (Gestione disco) per rendere il volume disponibile per l'uso.
8. Scaricare la versione più recente del servizio EC2Config. Estrarre i file dal file `.zip` nella directory `Temp` sull'unità collegata.
9. Nell'istanza temporanea, aprire la finestra di dialogo Run (Esegui), digitare **`regedit`** e premere Invio.

10. Scegli `HKEY_LOCAL_MACHINE`. Dal menu File scegliere Load Hive (Carica Hive). Scegli il drive, quindi individua e apri il file seguente: `Windows\System32\config\SOFTWARE`. Quando richiesto, specifica un nome chiave.
11. Selezionare la chiave appena caricata e passare a `Microsoft\Windows\CurrentVersion`. Scegli la chiave `RunOnce`. Se questa chiave non esiste, scegliere `CurrentVersion` dal menu contestuale (pulsante destro del mouse), quindi New (Nuovo) e selezionare Key (Chiave). Rinomina la chiave `RunOnce`.
12. Dal menu contestuale (pulsante destro del mouse) scegliere la chiave `RunOnce`, quindi New (Nuovo) e selezionare String Value (Valore stringa). Immettere il nome `Ec2Install` e i dati `C:\Temp\Ec2Install.exe /quiet`.
13. Scegli la chiave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`. Dal menu contestuale (pulsante destro del mouse) scegliere New (Nuovo), quindi selezionare String Value (Valore stringa). Immettere **`AutoAdminLogon`** come nome e **`1`** come dati valore.
14. Scegli la chiave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon>`. Dal menu contestuale (pulsante destro del mouse) scegliere New (Nuovo), quindi selezionare String Value (Valore stringa). Immettere **`DefaultUserName`** come nome e **`Administrator`** come dati valore.
15. Scegli la chiave `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`. Dal menu contestuale (pulsante destro del mouse) scegliere New (Nuovo), quindi selezionare String Value (Valore stringa). Digitare **`DefaultPassword`** come nome e inserire una password nei dati valore.
16. Nel riquadro di navigazione del Registry editor, scegli la chiave temporanea che hai creato alla prima apertura del Registry Editor.
17. Dal menu File, scegliere Unload Hive (Scarica Hive).
18. Nell'utilità Disk Management (Gestione disco), scegliere l'unità collegata in precedenza, aprire il menu contestuale (pulsante destro del mouse) e scegliere Offline.
19. Nella console Amazon EC2 distaccare il volume interessato dall'istanza temporanea e ricollegalo all'istanza con il nome del dispositivo console, `/dev/sda1`. Devi specificare questo nome del dispositivo per indicare il volume come volume root.
20. Avvio e arresto di un'istanza Amazon EC2 l'istanza.
21. All'avvio dell'istanza, verificare il log di sistema e accertarsi di visualizzare il messaggio Windows is ready to use (Windows è pronto per l'utilizzo).

22. Apri il Registry Editor e scegli `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`. Elimina le chiavi String Value create in precedenza: AutoAdminLogon, DefaultUserName, e DefaultPassword.
23. Cancella o interrompi l'istanza temporanea creata durante questa procedura.

Cronologia delle versioni di EC2Config

La tabella seguente descrive le versioni rilasciate di EC2Config. Per ulteriori informazioni sugli aggiornamenti per SSM Agent, consulta l'articolo relativo alle note di rilascio di SSM Agent Systems Manager.

> **Important**
>
> EC2Config ha raggiunto la fine del supporto. Soltanto la versione più recente dell'agente EC2Config è disponibile per il download. Le versioni precedenti sono indicate come private.

Versione	Dettagli	Data di rilascio
4.9.5777	• Problema risolto in cui la configurazione RSS era impostata in modo errato per alcuni tipi di istanza. • Nuova versione di SSM Agent `3.3.484.0` .	17 giugno 2024
4,95554	• Limita la devoluzione del nome di dominio in base alla voce del registro: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Nuova versione di SSM Agent `3.2.1630.0` .	4 ottobre 2023
4,9,5467	• È stata aggiunta la funzionalità di riprova per scoprire la porta della console. •	1° agosto 2023

Versione	Dettagli	Data di rilascio
	Nuova versione di SSM Agent `3.1.2282.0` .	
4,9,5288	• SDK del core di AWS aggiornato alla versione `3.7.103.23` . • È stato risolto il problema a causa del quale il documento SSM `AWS-UpdateEC2Config` non aggiornava `EC2Config` nelle istanze abilitate solo con IMDSv2. • Nuova versione di SSM Agent `3.1.2144.0` .	8 marzo 2023
4,9,5231	• Nuova versione di SSM Agent 3.1.1927.0.	14 febbraio 2023
4,9,5103	• È stato risolto un problema a causa del quale i volumi effimeri venivano erroneamente identificati nelle famiglie di istanze r5d e i4i. • Nuova versione di SSM Agent 3.1.1856.0.	5 dicembre 2022
4,9,5064	• È stato effettuato un aggiornamento per utilizzare le informazioni sui segmenti PCI per selezionare la porta della console. • PowerShell Script firmati e intestazioni di copyright aggiunte. • Logica di selezione dell'adattatore di rete primario fisso. • Nuova versione di SSM Agent 3.1.1732.0.	16 novembre 2022
4.9.4588	• La logica di attesa IMDS è stata aggiornata per effettuare solo richieste IMDSv2. • È stata aggiunta la libreria condivisa dell'agente di avvio libec2launch.dll. • Nuova versione di SSM Agent 3.1.1188.0.	31 maggio 2022

Versione	Dettagli	Data di rilascio
4,9,4556	• Aggiunta la logica di attesa per garantire l'inizializzazione completa della scheda NIC prima dell'uso. • La nuova versione di Log4Net 2.0.14.0 include la patch di sicurezza. • La nuova versione di SSM Agent 3.1.1045.0 include la patch di sicurezza.	1 marzo 2022
4,9,4536	• Risolto il problema di arresto anomalo di userdata quando manca la cartella Temp. • Nuova versione di SSM Agent 3.1.804.0.	31 gennaio 2022
4,9508	• Risolto il problema per calcolare correttamente il percorso dello script diskpart. • Nuova versione di SSM Agent 3.1.338.0.	6 ottobre 2021
4,9500	• `Install-EgpuManagerConfig` aggiornato con il supporto di IMDS v2. • Link Web aggiornati per utilizzare https. • Nuova versione di SSM Agent (3.1.282.0)	7 settembre 2021
4,94419	• Corretta la logica di fallback IMDS versione 1 • È stato aggiornato l'intero utilizzo della directory temporanea di Windows alla directory temporanea EC2config • Nuova versione dell'SSM Agent (3.0.1124.0)	2 giugno 2021

Versione	Dettagli	Data di rilascio
4.9.4381	• È stato aggiunto il supporto per lo schema del documento SSM versione 2.2 in EC2ConfigUpdater • È stata aggiunta la versione del pacchetto AWS Nitro Enclaves al registro della console • Nuova versione dell'SSM Agent (3.0.529.0)	4 maggio 2021
4.9.4326	• Rimossi tutti i collegamenti nell'interfaccia utente delle impostazioni • Questa è l'ultima versione di EC2config che supporta Windows Server 2008.	3 marzo 2021
4.9.4279	• Risolto il problema di protezione relativo all'attività pianificata `Ec2ConfigMonitor` • Risolto il problema della mappatura delle lettere di unità e il conteggio dei dischi temporanei • Aggiunta di `OsCurrentBuild` e `OsReleaseId` all'output della console • Nuova versione dell'SSM Agent 2.3.871.0	11 dicembre 2020
4.9.4222	• Corretta la logica di fallback IMDS versione 1 • Nuova versione dell'SSM Agent 2.3.842.0	7 aprile 2020
4.9.4122	• Aggiunto il supporto per IMDS V2. • Nuova versione dell'SSM Agent 2.3.814.0	4 marzo 2020
4.9.3865	• Corretto errore di individuazione della porta COM per Windows Server 2008 R2 su istanze metal • Nuova versione dell'SSM Agent (2.3.722.0)	31 ottobre 2019
4.9.3519	• Nuova versione dell'SSM Agent 2.3.634.0	18 giugno 2019

Versione	Dettagli	Data di rilascio
4.9.3429	• Nuova versione dell'SSM Agent (2.3.542.0)	25 aprile 2019
4.9.3289	• Nuova versione dell'SSM Agent 2.3.444.0	11 febbraio 2019
4.9.3270	• Plugin aggiunto per impostare il monitor in modo che non si spenga mai per risolvere i problemi di ACPI • Edizione di SQL Server e versione scritta nella console • Nuova versione dell'SSM Agent 2.3.415.0	22 gennaio 2019
4.9.3230	• La descrizione Drive Letter Mapping è stata aggiornata per essere maggiormente in linea con la funzionalità • Nuova versione dell'SSM Agent 2.3.372.0	10 gennaio 2019
4.9.3160	• Tempo di attesa aumentate per il filtro NIC primario • Aggiunta la configurazione predefinita per RSS e le impostazi oni Receive Queue per i dispositivi ENA • Ibernazione disabilitata durante Sysprep • Nuova versione dell'SSM Agent 2.3.344.0 • SDK aggiornato alla versione 3.3.29.13 AWS	15 dicembre 2018
4.9.3067	• Migliorie apportate all'ibernazione delle istanze • Nuova versione dell'SSM Agent 2.3.235.0	8 Novembre 2018
4.9.3034	• Aggiunta la route 169.254.169. 253/32 per server DNS • Nuova versione dell'SSM Agent 2.3.193.0	24 ottobre 2018
4.9.2986	• Aggiunta la firma per tutti i binari correlati EC2Config • Nuova versione dell'SSM Agent 2.3.136.0	11 ottobre 2018
4.9.2953	Nuova versione dell'SSM Agent (2.3.117.0)	2 ottobre 2018

Versione	Dettagli	Data di rilascio
4.9.2926	Nuova versione dell'SSM Agent (2.3.68.0)	18 settembre 2018
4.9.2905	• Nuova versione dell'SSM Agent (2.3.50.0) • Aggiunta la route 169.254.169. 123/32 al servizio orario AMZN • Aggiunto il percorso 169.254.169. 249/32 al servizio di licenza GRID • Risolto un problema per cui i volumi EBS NVMe venivano contrassegnati come temporanei	17 settembre 2018
4.9.2854	Nuova versione dell'SSM Agent (2.3.13.0)	17 agosto 2018
4.9.2831	Nuova versione dell'SSM Agent (2.2.916.0)	7 agosto 2018
4.9.2818	Nuova versione dell'SSM Agent (2.2.902.0)	31 luglio 2018
4.9.2756	Nuova versione dell'SSM Agent (2.2.800.0)	27 giugno 2018
4.9.2688	Nuova versione dell'SSM Agent (2.2.607.0)	25 maggio 2018
4.9.2660	Nuova versione dell'SSM Agent (2.2.546.0)	11 maggio 2018
4.9.2644	Nuova versione dell'SSM Agent (2.2.493.0)	26 aprile 2018
4.9.2586	Nuova versione dell'SSM Agent (2.2.392.0)	28 marzo 2018

Versione	Dettagli	Data di rilascio
4.9.2565	• Nuova versione dell'SSM Agent (2.2.355.0) • Corretto un problema sulle istanze M5 e C5 (impossibile trovare i driver PV) • Aggiunta registrazione della console per tipo di istanza, driver PV più recenti e driver NVMe	13 marzo 2018
4.9.2549	Nuova versione dell'SSM Agent (2.2.325.0)	8 marzo 2018
4.9.2461	Nuova versione dell'SSM Agent (2.2.257.0)	15 febbraio 2018
4.9.2439	Nuova versione dell'SSM Agent (2.2.191.0)	6 febbraio 2018
4.9.2400	Nuova versione dell'SSM Agent (2.2.160.0)	16 gennaio 2018
4.9.2327	• Nuova versione dell'SSM Agent (2.2.120.0) • Aggiunta individuazione porta COM sulle istanze bare metal di Amazon EC2 • È stata aggiunta la registrazione Hyper-V dello stato sulle istanze bare metal di Amazon EC2	2 gennaio 2018
4.9.2294	Nuova versione dell'SSM Agent (2.2.103.0)	4 dicembre 2017
4.9.2262	Nuova versione dell'SSM Agent (2.2.93.0)	15 novembre 2017
4.9.2246	Nuova versione dell'SSM Agent (2.2.82.0)	11 novembre 2017

Versione	Dettagli	Data di rilascio
4.9.2218	Nuova versione dell'SSM Agent (2.2.64.0)	29 ottobre 2017
4.9.2212	Nuova versione dell'SSM Agent (2.2.58.0)	23 ottobre 2017
4.9.2203	Nuova versione dell'SSM Agent (2.2.45.0)	19 ottobre 2017
4.9.2188	Nuova versione dell'SSM Agent (2.2.30.0)	10 ottobre 2017
4.9.2180	• Nuova versione dell'SSM Agent (2.2.24.0) • Aggiunto plug-in GPU elastico per istanze GPU	5 ottobre 2017
4.9.2143	Nuova versione dell'SSM Agent (2.2.16.0)	1 ottobre 2017
4.9.2140	Nuova versione dell'SSM Agent (2.1.10.0)	
4.9.2130	Nuova versione dell'SSM Agent (2.1.4.0)	
4.9.2106	Nuova versione dell'SSM Agent (2.0.952.0)	
4.9.2061	Nuova versione dell'SSM Agent (2.0.922.0)	
4.9.2047	Nuova versione dell'SSM Agent (2.0.913.0)	
4.9.2031	Nuova versione dell'SSM Agent (2.0.902.0)	
4.9.2016	• Nuova versione dell'SSM Agent (2.0.879.0) • È stato corretto il percorso della directory CloudWatch Logs per Windows Server 2003	

Versione	Dettagli	Data di rilascio
4.9.1981	• Nuova versione dell'SSM Agent (2.0.847.0) • Corretto il problema relativo a `important.txt` che è stato generato sui volumi EBS.	
4.9.1964	Nuova versione dell'SSM Agent (2.0.842.0)	
4.9.1951	• Nuova versione dell'SSM Agent (2.0.834.0) • Corretto un problema relativo alla lettera di unità, la quale non veniva mappata a partire dalla Z per le unità temporanee.	
4.9.1925	• Nuova versione dell'SSM Agent (2.0.822.0) • [Bug] Questa versione non è una destinazione di aggiornam ento valida per l'SSM Agent v4.9.1775.	
4.9.1900	Nuova versione dell'SSM Agent (2.0.805.0)	
4.9.1876	• Nuova versione dell'SSM Agent (2.0.796.0) • È stato risolto un problema di output/error reindirizzamento per l'esecuzione dei dati degli utenti amministratori.	
4.9.1863	• Nuova versione dell'SSM Agent (2.0.790.0) • Corretto un problema relativo al collegamento di più volumi EBS su un'istanza Amazon EC2. • È stato migliorato CloudWatch il percorso di configurazione, mantenendo la compatibilità con le versioni precedenti.	
4.9.1791	Nuova versione dell'SSM Agent (2.0.767.0)	

Versione	Dettagli	Data di rilascio
4.9.1775	Nuova versione dell'SSM Agent (2.0.761.0)	
4.9.1752	Nuova versione dell'SSM Agent (2.0.755.0)	
4.9.1711	Nuova versione dell'SSM Agent (2.0.730.0)	
4.8.1676	Nuova versione dell'SSM Agent (2.0.716.0)	
4.7.1631	Nuova versione dell'SSM Agent (2.0.682.0)	
4.6.1579	• Nuova versione dell'SSM Agent (2.0.672.0) • Corretto il problema dell'aggiornamento dell'agente per v4.3, v4.4 e v4.5	
4.5.1534	Nuova versione dell'SSM Agent (2.0.645.1)	
4.4.1503	Nuova versione dell'SSM Agent (2.0.633.0)	
4.3.1472	Nuova versione dell'SSM Agent (2.0.617.1)	
4.2.1442	Nuova versione dell'SSM Agent (2.0.599.0)	
4.1.1378	Nuova versione dell'SSM Agent (2.0.558.0)	

Versione	Dettagli	Data di rilascio
4.0.1343	• Run Command, State Manager, l' CloudWatch agente e il supporto per l'aggiunta al dominio sono stati spostati in un altro agente chiamato SSM Agent. SSM Agent verrà installato come parte dell'aggiornamento EC2Config. Per ulteriori informazioni, consulta EC2Config e AWS Systems Manager. • Se disponi di una configurazione del proxy su EC2Config, sarà necessario aggiornare le impostazioni proxy dell'SSM Agent prima dell'aggiornamento. Se non aggiorni le impostazioni del proxy, non potrai utilizzare il comando di esecuzione per gestire le tue istanze. Per evitarlo, prima di eseguire l'aggiornamento alla versione più recente, consulta Installazione e configurazione dell'SSM Agent sulle istanze Windows nella Guida per l'utente di AWS Systems Manager . • Se in precedenza hai abilitato CloudWatch l'integrazione sulle tue istanze utilizzando un file di configurazione locale (`AWS.EC2.Windows.CloudWatch.json`), dovrai configurare il file per funzionare con SSM Agent.	
3.19.1153	• Re-enabled plug-in di attivazione per istanze con configurazione precedente. AWS KMS Salta l'attivazione per gli utenti BYOL. • Modifica il comportamento TRIM predefinito da disabilitare durante l'operazione di formattazione del disco e aggiungi FormatWith TRIM per sovrascrivere il InitializeDisks plug-in con userdata.	

Versione	Dettagli	Data di rilascio
3.18.1118	• Introdotta una correzione per aggiungere instradamenti in modo affidabile all'adattatore di rete primario. • Aggiornamenti per migliorare il supporto per i AWS servizi.	
3.17.1032	• Apportate correzioni ai log di sistema duplicati, i quali vengono visualizzati quando i filtri impostano la stessa categoria. • Introdotte correzioni per evitare blocchi durante l'inizial izzazione del disco.	
3.16.930	Aggiunto il supporto per registrare l'evento "Window is Ready to use" (Windows pronto all'uso) all'avvio del log di eventi di Windows.	
3.15.880	Apportata una correzione per permettere il caricamento dell'outp ut di Run Command per Systems Manager in nomi di bucket S3 con un carattere "." (punto).	
3.14.786	È stato aggiunto il supporto per sovrascrivere le impostazioni InitializeDisks del plugin. Ad esempio, per velocizzare l'inizial izzazione del disco SSD, puoi disattivare temporaneamente TRIM specificando nei dati utente come segue: < InitializeDrivesSettings >< > TRIM</ SettingsGroup ></ FormatWithout SettingsGroup InitializeDrivesSettings	
3.13.727	Run Command di Systems Manager – Apportate correzioni per elaborare in modo affidabile i comandi dopo il riavvio della finestra.	

Versione	Dettagli	Data di rilascio
3.12.649	• Correzione per gestire correttamente il riavvio durante l'esecuzione. commands/scripts • Apportata una correzione per cancellare in modo affidabile l'esecuzione dei comandi. • Aggiungi il supporto per (facoltativamente) il caricamento dei log MSI su S3 durante l'installazione delle applicazioni tramite Systems Manager Run Command.	
3.11.521	• Correzioni per abilitare la generazione dell'impronta RDP per Windows Server 2003. • Correzioni per includere l'offset UTC e timezone nelle linee log di EC2Config. • Supporto di Systems Manager per eseguire comandi Run Command in parallelo. • Roll back della modifica precedente per trasferire online i dischi partizionati.	
3.10.442	• Corretti gli errori di configurazione di Systems Manager durante l'installazione di applicazioni MSI. • Apportata una correzione per trasferire in modo affidabile online i dischi archiviazione. • Aggiornamenti per migliorare il supporto per i servizi. AWS	

Versione	Dettagli	Data di rilascio
3.9.359	• Introdotta una correzione nello script post Sysprep per lasciare la configurazione dell'aggiornamento di Windows nello stato predefinito. • Corretto il plug-in per la generazione della password per migliorare l'affidabilità delle impostazioni della policy per la password GPO. • Limita le autorizzazioni delle cartelle di EC2Config/SSM registro al gruppo Administrators locale. • Aggiornamenti per migliorare il supporto per i AWS servizi.	
3.8.294	• È stato risolto un problema CloudWatch che impediva il caricamento dei log quando non si trovavano sull'unità principale. • Migliorato il processo di inizializzazione del disco tramite l'aggiunta della logica di ripetizione. • È stata aggiunta una migliore gestione degli errori quando il SetPassword plug-in occasionalmente non funzionava durante la creazione dell'AMI. • Aggiornamenti per migliorare il supporto per AWS i servizi.	

Versione	Dettagli	Data di rilascio
3.7.308	• Apportate migliorie all'utilità ec2config-cli per i test config e per la risoluzione dei problemi di un'istanza. • Evita di aggiungere route statiche AWS KMS e servizi di metadati su un adattatore OpenVPN. • Risolto un problema a causa del quale l'esecuzione dei dati utente non stavano onorando il tag "persist". • Migliorata la gestione degli errori quando l'accesso alla console EC2 non è disponibile. • Aggiornamenti per migliorare il supporto per i servizi. AWS	
3.6.269	• Correzione dell'affidabilità dell'attivazione di Windows all'indirizzo locale del collegamento al primo utilizzo 169.254.0.250/251 per l'attivazione di Windows tramite AWS KMS • Migliorata la gestione del proxy per Systems Manager, l'attivazione di Windows e gli scenari del collegamento del dominio • Corretto un problema secondo il quale doppie linee degli account utente non venivano aggiunte al file di risposta Sysprep	
3.5.228	• È stato risolto uno scenario in cui il CloudWatch plug-in potrebbe consumare CPU e memoria eccessive nella lettura dei registri degli eventi di Windows • È stato aggiunto un collegamento alla documentazione di CloudWatch configurazione nell'interfaccia utente delle impostazioni di EC2Config	

Versione	Dettagli	Data di rilascio
3.4.212	• Correzioni a EC2Config se usato in combinazione con. VM-Import • Risolto il problema di denominazione del servizio sul programma d'installazione WiX.	
3.3.174	• Migliorata la gestione dell'eccezione per Systems Manager e gli errori di aggiunta del dominio • Apportata modifica per supportare la funzione Versioni multiple dello schema SSM di Systems Manager • Corretta la formattazione di dischi temporanei su Win2K3. • Apportata modifica per supportare la configurazione delle dimensioni del disco maggiori di 2TB. • Ridotto l'utilizzo della memoria virtuale attraverso l'imposta zione della modalità GC su predefinita. • Supporto per scaricare gli artefatti dal percorso UNC sui plug-in `aws:psModule` e `aws:application` . • Migliorato l'accesso per i plug-in dell'attivazione di Windows.	

Versione	Dettagli	Data di rilascio
3.2.97	• Apportati dei miglioramenti alle prestazioni tramite il ritardo del caricamento delle assembly SSM per Systems Manager. • Migliorata la gestione dell'eccezione per sysprep2008.xml difettoso. • Introdotto il supporto della riga di comando per la configura zione "Apply" di Systems Manager. • Apportata una modifica per supportare l'aggiunta del dominio nel caso in cui ci fosse una denominazione del computer in attesa. • Introdotto un supporto per parametri opzionali sul plug-in `aws:applications` . • Introdotto un supporto per la matrice di comando nel plug-in `aws:psModule` .	
3.0.54	• Abilitazione del supporto per Systems Manager. • Il dominio unisce automaticamente le istanze EC2 Windows a una directory tramite Systems Manager. AWS • Configura e carica CloudWatch logs/metrics tramite Systems Manager. • Installa PowerShell i moduli tramite Systems Manager. • Installa le applicazioni MSI tramite Systems Manager.	

Versione	Dettagli	Data di rilascio
2.4.233	• Aggiunta attività programmata per ripristinare EC2Config dagli errori relativi ail startup del servizio. • Apportate migliorie ai messaggi di errore del log della console. • Aggiornamenti per migliorare il supporto per i AWS servizi.	
2.3.313	• È stato risolto un problema relativo all'elevato consumo di memoria in alcuni casi quando la funzione CloudWatch Registri è abilitata. • Corretto un bug relativo all'aggiornamento, così che le versioni di EC2Config precedenti alla 2.1.19 possono essere aggiornat e alle più recenti ora. • Aggiornata l'eccezione dell'apertura del porto COM affinché sia più facile da usare e utile sui log. • Ec2configServiceSettings L'interfaccia utente ha disabilitato il ridimensionamento e corretto il posizionamento dell'attr ibuzione e della visualizzazione della versione nell'interfaccia utente.	
2.2.12	• Gestito NullPointerException durante l'interrogazione di una chiave di registro per determinare lo stato di Windows Sysprep che occasionalmente restituiva null. • Liberate le risorse non gestite nel blocco finally.	
2.2.11	È stato risolto un problema nel CloudWatch plug-in per la gestione delle righe di registro vuote.	

Versione	Dettagli	Data di rilascio
2.2.10	• Rimossa la configurazione delle impostazioni CloudWatch dei log tramite l'interfaccia utente. • Consenti agli utenti di definire le impostazioni CloudWatch dei log nel `%ProgramFiles%\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json` file per consentire miglioramenti futuri.	
2.2.9	Corretta l'eccezione non gestita e aggiunto il logging.	
2.2.8	• Corretta la verifica della versione del sistema operativo Windows sul programma di installazione di EC2Config per il supporto di Windows Server 2003 SP1 e versioni successive. • Corretta la gestione del valore nullo al momento della lettura di chiavi di registro, le quali erano correlate all'aggiornamento dei file config di Sysprep.	
2.2.7	• Aggiunto un supporto per EC2Config da eseguire durante l'esecuzione di Sysprep per Windows 2008 e versioni successive. • Migliorata la gestione e il logging dell'eccezione per una migliore diagnostica	
2.2.6	• È stato ridotto il carico sull'istanza e sui CloudWatch log durante il caricamento degli eventi di registro. • Risolto un problema di aggiornamento per cui il plug-in CloudWatch Logs non rimaneva sempre abilitato	

Versione	Dettagli	Data di rilascio
2.2.5	• È stato aggiunto il supporto per caricare i log su CloudWatch Log Service. • È stato risolto un problema relativo alle condizioni di gara nel Ec2OutputRDPCert plug-in • È stata modificata l'opzione di ripristino del servizio EC2Config da cui riavviare TakeNoAction • Aggiunte maggiori informazioni di eccezione quando EC2Config si arresta in modo anomalo	
2.2.4	• È stato corretto un errore di battitura in PostSysprep.cmd • Corretto un bug per il quale EC2Config non si bloccava sul menu di avvio per OS2012+	

Versione	Dettagli	Data di rilascio
2.2.3	• Aggiunta l'opzione per installare EC2Config senza che il servizio cominci subito dopo l'installazione. Per utilizzarlo, esegui 'Ec2Install.exestart=false' dal prompt dei comandi • È stato aggiunto un parametro nel plugin per controllare lo sfondo. adding/removing Per utilizzarlo, esegui 'Ec2WallpaperInfo.exeset' o 'Ec2WallpaperInfo.exe revert' dal prompt dei comandi • Aggiunto il controllo della RealTimeIsUniversal chiave, invia alla console le impostazioni errate della chiave di RealTimeIsUniveral registro • Rimossa la dipendenza di EC2Config sulla cartella temp di Windows • È stata rimossa la dipendenza di UserData esecuzione da .Net 3.5	
2.2.2	• Aggiunta verifica per i comportamenti di blocco del servizio, al fine di controllare che le risorse siano state rilasciate • Risolto un problema legato a lunghi tempi di esecuzione al momento dell'aggiunta al dominio	

Versione	Dettagli	Data di rilascio
2.2.1	• Aggiornato il programma di esecuzione per permettere gli aggiornamenti delle versioni più datate • Risolto Ec2WallpaperInfo un bug in. Net4.5 unico ambiente • Risolto un bug di rilevamento intermittente dei driver • Aggiunta un'opzione di installazione in modalità silenzios a. Esegui Ec2Install.exe con l'opzione '-q'. Ad esempio: '-q' Ec2Install.exe	
2.2.0	• È stato aggiunto il supporto per .Net4 e. Net4.5 solo ambienti • Aggiornato il programma di installazione	
2.1.19	• Aggiunto il supporto per l'etichettatura del disco temporane o quando si utilizza il driver di rete Intel (ad esempio tipo di istanza C3). Per ulteriori informazioni, consulta Rete migliorata per le istanze Amazon EC2. • Aggiunti supporti Nome origine AMI e Versione origine AMI all'output della console • Sono state apportate modifiche all'output della console per renderle coerenti formatting/parsing • Aggiornato file di aiuto	

Versione	Dettagli	Data di rilascio
2.1.18	• È stato aggiunto l'oggetto WMI EC2Config per la notifica di completamento (-Namespace root\ Amazon -Class EC2_) ConfigService • Le prestazioni della query WMI al startup con un ampio utilizzo di log eventi, potrebbe causare un'attività elevata e prolungata della CPU durante l'esecuzione iniziale	
2.1.17	• È stato risolto UserData il problema di esecuzione con il riempimento del buffer Standard Output e Standard Error • Risolto un problema relativo all'impronta RDP errata che a volte compariva nell'output della console per >= Sistema operativo w2k8 • Console Output ora contiene 'RDPCERTIFICATE-Su bjectName:' per Windows 2008+, che contiene il valore del nome del computer • Aggiunto D:\ nell'elenco a cascata della mappatura della lettera di unità • Il pulsante Aiuto è stato spostato in alto a destra e modificato look/feel • Aggiunto un collegamento del sondaggio sul feedback in alto a destra	

Versione	Dettagli	Data di rilascio
2.1.16	• La scheda Generali contiene un collegamento alla pagina per scaricare le versioni più recenti di EC2Config • L'overlay dello sfondo del desktop ora è archiviato nella cartella Appdata locale degli utenti anziché in My Documents per supportare il reindirizzamento MyDoc • Nome MSSQLServer sincronizzato con il sistema in script (2008+) Post-Sysprep • Riordinata la cartella dell'applicazione (spostati i file sulla directory Plug-in e rimossi i file duplicati) • Modificato l'output del log di sistema (console): • *Modificati i formati di valore, nome e data per un'analisi più semplice (Inizia a migrare le dipendenze nel nuovo formato) • *Aggiunto lo stato del plugin '' Ec2SetPassword • *Aggiunta l'ora di inizio e di fine di Sysprep • Risolto un problema per il quale i dischi temporanei non venivano etichettati come 'Storage Temporary (Archiviazione temporanea)' per i sistemi operativi non in lingua inglese • Risolti errori relativi alla disinstallazione di EC2Config dopo aver eseguito Sysprep	

Versione	Dettagli	Data di rilascio
2.1.15	• Ottimizzate le richieste per il servizio di metadati • I metadati ora bypassano le impostazioni Proxy • Dischi temporanei etichettati come «Archiviazione temporane a» e Important.txt collocati nel volume quando vengono trovati (solo driver Citrix PV). Per ulteriori informazioni, consulta Aggiornamento dei driver PV sulle istanze Windows EC2. • I dischi temporanei assegnavano lettere di unità dalla Z alla A (solo driver Citrix PV) – questo incarico può essere sovrascri tto tramite il plug-in della mappatura della lettera di unità con le etichette del volume 'Temporary Storage X (Archiviazione temporanea X)', dove x è un numero compreso tra 0 e 25. • UserData ora viene eseguito immediatamente dopo «Windows è pronto»	
2.1.14	Risolti problemi relativi allo sfondo del desktop	
2.1.13	• Lo sfondo del desktop mostrerà l'hostname per impostazione predefinita • Rimossa dipendenza sul servizio Windows Time • Aggiunta route per i casi in cui più IP venivano assegnati a una singola interfaccia	

Versione	Dettagli	Data di rilascio
2.1.11	• Apportate modifiche al plug-in Ec2Activation • - Verifica lo stato di attivazione ogni 30 giorni • - Se mancano 90 giorni alla scadenza del periodo di grazia (su 180 giorni), riprova l'attivazione	
2.1.10	• La sovrapposizione dello sfondo del desktop non persiste più con Sysprep o con l'arresto senza Sysprep • L'opzione Userdata da eseguire su ogni servizio inizia con <persist>true</persist> • Posizione e nome modificati da/a/DisableWinUpdate.cmd Scripts/PostSysprep.cmd • La password dell'amministratore è impostata per non scadere per impostazione predefinita in/Scripts/PostSysprep.cmd • La disinstallazione rimuoverà lo script EC2Config PostSysprep da c:\windows\setup\script\ CommandComplete.cmd • Aggiunta una route che supporta i parametri dell'interfaccia personalizzata	
2.1.9	UserData L'esecuzione non è più limitata a 3851 caratteri	

Versione	Dettagli	Data di rilascio
2.1.7	• La versione del sistema operativo e l'identificatore della lingua sono scritti nella console • La versione di EC2Config è scritta nella console • La versione del driver PV è scritta nella console • Rilevamento della verifica dei bug e dell'output per la console al prossimo riavvio, se riscontrati • Aggiunta opzione su config.xml così che le credenziali di Sysprep persistano • Aggiunta logica di ripetizione dei tentativi route nel caso in cui ENI non sia disponibile all'avvio • Il PID di esecuzione dei dati utente è scritto nella console • La lunghezza minima della password generata viene recuperata dal GPO • Impostato l'avvio del servizio affinché compia 3 tentativi • Sono stati aggiunti esempi di file S3_ DownloadFile.ps1 e S3_Upload file.ps1 nella cartella /Scripts	

Versione	Dettagli	Data di rilascio
2.1.6	• Informazioni della versione aggiunte sulla scheda Generali • Rinominata la scheda Bundle in Immagine • Semplificato il processo di specificazione della password; spostata la password dell'interfaccia utente dalla scheda Generali alla scheda Immagine • Rinominata la scheda Impostazioni disco in archiviazione • Aggiunta una scheda Supporto con strumenti comuni per la risoluzione di problemi • Impostato `sysprep.ini` di Windows Server 2003 per estendere la partizione del sistema operativo per impostazi one predefinita • Aggiunto l'indirizzo IP privato allo sfondo • Indirizzo IP privato mostrato sullo sfondo • Aggiunta logica di ripetizione dei tentativi per l'output della console • Risolto un problema relativo all'eccezione della porta Com per l'accessibilità dei metadati – che causava l'interruzione di EC2Config prima che venisse mostrato l'output della console • Introdotte verifiche dello stato di attivazione per ogni avvio – si attiva se necessario • È stato risolto il problema dei percorsi relativi, causato dall'esecuzione manuale di un collegamento allo sfondo dalla cartella di avvio, che puntava a Administrator/logs	

Versione	Dettagli	Data di rilascio
	• Corretto il colore dello sfondo predefinito per l'utente di Windows Server 2003 (oltre che per l'amministratore)	

Versione	Dettagli	Data di rilascio
2.1.2	• Time stamp della console su UTC (Zulù) • Rimosso l'aspetto del collegamento ipertestuale sulla scheda Sysprep • Aggiunta la caratteristica che permette di espandere in maniera dinamica il Volume root al primo avvio su Windows 2008+ • Quando Set-Password è abilitato, ora abilita automaticamente EC2Config per impostare la password • EC2Config verifica lo stato di attivazione prima di eseguire Sysprep (vengono mostrati avvisi se questo non è attivato) • Per impostazione predefinita, `Sysprep.xml` su Windows Server 2003 ora imposta il fuso orario su UTC anziché sul fuso orario del Pacifico • Randomizzati i server di attivazione • Rinominata la scheda Mappatura del drive su Impostazioni disco • Spostati gli elementi dell'interfaccia utente per inizializzare i drive dalla scheda Generali a Impostazioni disco • Il pulsante Aiuto indirizza ora al file di aiuto HTML • Aggiornato il file di aiuto HTML con modifiche • Aggiornato il testo 'Note' per le mappature della lettera di unità •	

Versione	Dettagli	Data di rilascio
	Aggiunto InstallUpdates.ps1 alla cartella /Scripts per automatizzare le patch e la pulizia prima di Sysprep	
2.1.0	• Lo sfondo del desktop mostra le informazioni sull'istanza per impostazione predefinita al primo accesso (non) disconnect/reconnect • PowerShell può essere eseguito dai dati utente racchiudendo il codice con<powershell></powershell>	

Usa EC2 Fast Launch per le tue istanze Windows

Quando configuri un'AMI Windows Server per EC2 Fast Launch, Amazon EC2 crea una serie di snapshot con pre-provisioning da utilizzare per un avvio più rapido, come indicato di seguito.

1. Amazon EC2 avvia una serie di istanze t3 temporanee, in base alle tue impostazioni.
2. Quando ogni istanza temporanea completa i passaggi di avvio standard, Amazon EC2 crea uno snapshot con pre-provisioning dell'istanza. Archivia lo snapshot nel tuo bucket Amazon S3.
3. Quando lo snapshot è pronto, Amazon EC2 termina l'istanza t3 associata per mantenere i costi delle risorse il più bassi possibile.
4. Quando Amazon EC2 avvia un'istanza da un'AMI con EC2 Fast Launch abilitato, utilizza uno degli snapshot per ridurre notevolmente il tempo di avvio.

Amazon EC2 reintegra automaticamente gli snapshot disponibili poiché gli utilizza per avviare istanze dall'AMI abilitata a EC2 Fast Launch.

Qualunque account che abbia accesso a un'AMI abilitata a EC2 Fast Launch può beneficiare di tempi di avvio ridotti. Quando il proprietario dell'AMI concede l'accesso all'avvio delle istanze, gli snapshot pre-assegnati provengono dall'account del proprietario dell'AMI.

Se un'AMI che supporta EC2 Fast Launch è condivisa con te, puoi abilitare o disabilitare tu stesso l'avvio più rapido sull'AMI condivisa. Se abiliti un'AMI condivisa per EC2 Fast Launch, Amazon EC2

crea gli snapshot con pre-provisioning direttamente nel tuo account. Se esaurisci gli snapshot nel tuo account, puoi comunque utilizzare gli snapshot dall'account del proprietario dell'AMI.

> **Note**
>
> EC2 Fast Launch elimina gli snapshot con pre-provisioning non appena vengono utilizzate da un avvio per ridurre al minimo i costi di archiviazione e impedirne il riutilizzo. Tuttavia, se gli snapshot eliminati soddisfano una regola di conservazione, il Cestino li conserva automaticamente. Ti consigliamo di esaminare l'ambito delle regole di conservazione del Cestino in modo che ciò non accada. Per ulteriori informazioni, consulta Cestino nella Guida per l'utente di Amazon EBS.
>
> Questa funzionalità è diversa dal ripristino rapido degli snapshot EBS. Devi abilitare esplicitamente il ripristino rapido degli snapshot EBS per ogni snapshot, ciò prevede costi associati.

Il video seguente mostra come configurare l'AMI Windows per un avvio più rapido con una rapida panoramica dei termini chiave correlati e delle relative definizioni: Avvio delle istanze EC2 Windows fino al 65% più velocemente. AWS

Costi delle risorse

Non è previsto alcun costo di servizio per configurare le AMI di Windows per EC2 Fast Launch. Tuttavia, i prezzi standard si applicano a tutte le AWS risorse sottostanti utilizzate da Amazon EC2. Per ulteriori informazioni sui costi delle risorse associate e su come gestirli, consulta Gestione dei costi per le risorse sottostanti di EC2 Fast Launch.

Indice

- Termini chiave
- EC2 Prerequisiti di Fast Launch per Windows
- Configura le impostazioni di EC2 Fast Launch per la tua AMI Windows Server Amazon EC2
- Visualizza le AMI con EC2 Fast Launch abilitato
- Gestione dei costi per le risorse sottostanti di EC2 Fast Launch
- Monitora l'avvio EC2 rapido
- Service-linked ruolo per EC2 Fast Launch
- Risolvi i problemi relativi a Windows EC2 Fast Launch

Termini chiave

La funzionalità EC2 Fast Launch utilizza i seguenti termini chiave:

Snapshot con pre-provisioning

Uno snapshot di un'istanza che è stata avviata da un'AMI Windows con EC2 Fast Launch abilitato e che ha completato i seguenti passaggi di avvio di Windows, riavviando secondo necessità.

- Specializzazione di Sysprep
- Windows Out of Box Experience (OOBE)

Al termine di questi passaggi, EC2 Fast Launch interrompe l'istanza e crea uno snapshot che viene successivamente utilizzato per un avvio più rapido dall'AMI in base alla tua configurazione.

Frequenza di avvio

Controlla il numero di snapshot con pre-provisioning che Amazon EC2 può avviare entro il periodo di tempo specificato. Quando abiliti EC2 Fast Launch per la tua AMI, Amazon EC2 crea la serie iniziale di snapshot con pre-provisioning in background. Ad esempio, se la frequenza di avvio è impostata su cinque avvii all'ora, che è il valore predefinito, EC2 Fast Launch crea un set iniziale di cinque snapshot con pre-provisioning.

Quando Amazon EC2 avvia un'istanza da un'AMI con EC2 Fast Launch abilitato, utilizza uno degli snapshot con pre-provisioning per ridurre il tempo di avvio. Man mano che gli snapshot vengono utilizzati, vengono automaticamente riforniti, fino al numero specificato dalla frequenza di lancio.

Se è previsto un picco del numero di istanze avviate dall'AMI, ad esempio durante un evento speciale, è possibile aumentare la frequenza di lancio in anticipo per coprire le istanze aggiuntive necessarie. Quando la frequenza di avvio torna alla normalità, è possibile regolarla nuovamente.

Quando avviene un numero di avvii superiore al previsto, potresti utilizzare tutti gli snapshot con pre-povisioning disponibili. Ciò non causa il fallimento di alcun avvio. Tuttavia, può comportare che alcune istanze passino attraverso il processo di avvio standard, fino a quando non è possibile reintegrare gli snapshot.

Numero di risorse di destinazione

Il numero di snapshot con pre-provisioning da tenere a disposizione per l'AMI Windows Server Amazon EC2 con EC2 Fast Launch abilitato.

Numero massimo di avvi paralleli

Controlla quante istanze Amazon EC2 può avviare contemporaneamente per creare snapshot con pre-provisioning per EC2 Fast Launch. Se il numero di risorse di destinazione è superiore al numero massimo di avvii paralleli configurato, Amazon EC2 avvia il numero di istanze specificato dall'impostazione Numero massimo di avvii paralleli per la creazione degli snapshot. Quando queste istanze completano il processo, Amazon EC2 acquisisce lo snapshot e arresta l'istanza. Quindi continua ad avviare altre istanze fino a quando il numero totale di snapshot disponibili non raggiunge il numero di risorse di destinazione. Il valore in Numero massimo di avvi paralleli deve essere pari o superiore a 6.

EC2 Prerequisiti di Fast Launch per Windows

Prima di configurare EC2 Fast Launch, verifica di aver soddisfatto i seguenti prerequisiti necessari per creare istantanee per il tuo computer: AMIs Account AWS

- Se fornisci un modello di avvio personalizzato quando configuri EC2 Fast Launch, il servizio utilizza il VPC e altre impostazioni di configurazione che hai definito nel modello di avvio. Per ulteriori informazioni, consulta Usa un modello di avvio quando configuri EC2 Fast Launch.
- Se non utilizzi un modello di avvio personalizzato per configurare le impostazioni, devi collegare la EC2FastLaunchFullAccess policy al tuo ruolo IAM corrente prima di abilitare EC2 Fast Launch. Quindi il servizio crea automaticamente uno CloudFormation stack con le seguenti risorse nel tuo Account AWS.
  - Un cloud privato virtuale (VPC)
  - Sottoreti private in più zone di disponibilità
  - Un modello di lancio configurato con Instance Metadata Service versione 2 () IMDSv2
  - Un gruppo di sicurezza senza regole in entrata o in uscita
- Private EC2 Fast Launch AMIs deve supportare l'esecuzione di script di dati utente.
- Per configurare EC2 Fast Launch per un'AMI, è necessario creare l'AMI utilizzando Sysprep l'opzione shutdown. La funzionalità EC2 Fast Launch attualmente non supporta AMIs le istanze create da un'istanza in esecuzione.

  Per creare un'AMI tramite Sysprep, consultare Creare un'AMI Amazon EC2 utilizzando Windows Sysprep.
- Per abilitare EC2 Fast Launch per un'AMI crittografata che utilizza una chiave gestita dal cliente per la crittografia, è necessario concedere al ruolo collegato al servizio per EC2 Fast Launch

l'autorizzazione a utilizzare la CMK. Per ulteriori informazioni, consulta the section called "Accesso alle chiavi gestite dal cliente".

- La quota predefinita per il numero massimo di lanci paralleli su all AMIs in an Account AWS è 40 per regione. Puoi richiedere un aumento delle Service Quotas per il tuo account, come indicato di seguito.

  1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/.
  2. Nel pannello di navigazione, scegli Servizi AWS.
  3. Nella barra di ricerca, inserisci **`EC2 Fast Launch`** e seleziona il risultato.
  4. Seleziona il link Avvii di istanze parallele per aprire la pagina dei dettagli della quota di servizio.
  5. Scegli Richiedi un aumento a livello di account.

  Per ulteriori informazioni, consulta Richiesta di un aumento di quota nella Guida per l'utente di Service Quotas.

Configura le impostazioni di EC2 Fast Launch per la tua AMI Windows Server Amazon EC2

Puoi configurare le AMI EC2 Fast Launch per Windows di tua proprietà o le AMI condivise con te tramite API Console di gestione AWS CloudFormation, SDK o (). AWS Command Line Interface AWS CLI Prima di configurare EC2 Fast Launch, verifica che la tua AMI soddisfi i prerequisiti necessari per creare gli snaphost con pre-provisioning. Per ulteriori informazioni, consulta EC2 Prerequisiti di Fast Launch per Windows.

Quando abiliti un avvio più rapido per le istanze Windows, Amazon EC2 verifica di disporre delle autorizzazioni necessarie per avviare le istanze dall'AMI e dal modello di avvio specificati (se forniti), incluse le autorizzazioni per le AMI crittografate. Per evitare errori durante il processo di avvio dell'istanza, il servizio convalida le autorizzazioni prima che EC2 Fast Launch sia abilitato. Se non disponi delle autorizzazioni richieste, il servizio restituisce un errore e non abilitato EC2 Fast Launch.

EC2 Fast Launch si integra con EC2 Image Builder per aiutarti a creare immagini personalizzate con EC2 Fast Launch abilitato. Per ulteriori informazioni, consulta Creazione di impostazioni di distribuzione per un'AMI Windows con EC2 Fast Launch abilitato (AWS CLI)nella Guida per l'utente di EC2 Image Builder.

Abilita EC2 Fast Launch

Prima di modificare queste impostazioni, assicurati che l'AMI e la regione in cui è eseguita soddisfino tutti EC2 Prerequisiti di Fast Launch per Windows.

Console

Per abilitare EC2 Fast Launch

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di spostamento, in Images (Immagini), scegliere AMI.
3. Selezionare l'AMI da aggiornare selezionando la casella di controllo accanto al Name (Nome).
4. Dal menu Operazioni sopra l'elenco delle AMI, scegli Configura avvio rapido. Si apre la pagina Configura avvio rapido, in cui configuri le impostazioni per EC2 Fast Launch.
5. Per iniziare a utilizzare snapshot con pre-provisioning per avviare più rapidamente le istanze dall'AMI Windows, seleziona la casella di spunta Abilita avvio rapido di Windows.
6. Dall'elenco a discesa Set anticipated launch frequency (Imposta la frequenza di lancio prevista), scegliere un valore per specificare il numero di snapshot creati e mantenuti per coprire il volume di avvio dell'istanza previsto.
7. Una volta completate le modifiche, scegliere Save (Salva).

> **Note**
>
> Se devi utilizzare un modello di avvio per specificare un VPC o per configurare impostazioni di metadati per IMDSv2, consulta Usa un modello di avvio quando configuri EC2 Fast Launch.

AWS CLI

Per abilitare EC2 Fast Launch

Utilizza il comando enable-fast-launch per abilitare EC2 Fast Launch per l'AMI specificata, avviando sei istanze parallele per il pre-provisioning.

```
aws ec2 enable-fast-launch \
```

```
    --image-id ami-0abcdef1234567890  \
    --max-parallel-launches 6 \
    --resource-type snapshot
```

Di seguito è riportato un output di esempio.

```
{
 "ImageId": "ami-0abcdef1234567890",
 "ResourceType": "snapshot",
 "SnapshotConfiguration": {
     "TargetResourceCount": 10
 },
 "LaunchTemplate": {},
 "MaxParallelLaunches": 6,
 "OwnerId": "0123456789123",
 "State": "enabling",
 "StateTransitionReason": "Client.UserInitiated",
 "StateTransitionTime": "2022-01-27T22:16:03.199000+00:00"
}
```

PowerShell

Per abilitare EC2 Fast Launch

Utilizza il Enable-EC2FastLaunch cmdlet per abilitare EC2 Fast Launch per l'AMI specificata, avviando sei istanze parallele per il pre-provisioning.

```
Enable-EC2FastLaunch `
 -ImageId ami-0abcdef1234567890 `
 -MaxParallelLaunch 6 `
 -Region us-west-2 `
 -ResourceType snapshot
```

Di seguito è riportato un output di esempio.

```
ImageId              : ami-0abcdef1234567890
 LaunchTemplate       :
 MaxParallelLaunches  : 6
 OwnerId              : 0123456789123
 ResourceType         : snapshot
 SnapshotConfiguration : Amazon.EC2.Model.FastLaunchSnapshotConfigurationResponse
```

```
State                 : enabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:24:11 PM
```

Disabilita EC2 Fast Launch

Prima di modificare queste impostazioni, assicurati che l'AMI e la regione in cui è eseguita soddisfino tutti EC2 Prerequisiti di Fast Launch per Windows.

Console

Per disabilitare EC2 Fast Launch

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di spostamento, in Images (Immagini), scegliere AMI.
3. Selezionare l'AMI da aggiornare selezionando la casella di controllo accanto al Name (Nome).
4. Dal menu Operazioni sopra l'elenco delle AMI, scegli Configura avvio rapido. Si apre la pagina Configura avvio rapido, in cui configuri le impostazioni per EC2 Fast Launch.
5. Deseleziona la casella di spunta Abilita avvio rapido di Windows per disabilitare EC2 Fast Launch e rimuovere gli snapshot con pre-provisioning. Ciò comporta d'ora in poi che AMI utilizzi il processo di lancio standard per ogni istanza.

   > **Note**
   >
   > Quando disabiliti l'ottimizzazione delle immagini di Windows, tutti gli snapshot con pre-provisioning esistenti vengono eliminati automaticamente. Questo passaggio deve essere completato prima di poter ricominciare a utilizzare la funzione.

6. Una volta completate le modifiche, scegliere Save (Salva).

AWS CLI

Per disabilitare EC2 Fast Launch

Utilizza il seguente comando disable-fast-launch per disabilitare EC2 Fast Launch sull'AMI specificata, e rimuovi gli snapshot con pre-provisioning esistenti.

```
aws ec2 disable-fast-launch --image-id ami-01234567890abcedf
```

Di seguito è riportato un output di esempio.

```
{
    "ImageId": "ami-01234567890abcedf",
    "ResourceType": "snapshot",
    "SnapshotConfiguration": {},
    "LaunchTemplate": {
        "LaunchTemplateId": "lt-01234567890abcedf",
        "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
        "Version": "1"
    },
    "MaxParallelLaunches": 6,
    "OwnerId": "0123456789123",
    "State": "disabling",
    "StateTransitionReason": "Client.UserInitiated",
    "StateTransitionTime": "2022-01-27T22:47:29.265000+00:00"
}
```

PowerShell

Per disabilitare EC2 Fast Launch

Utilizza il Disable-EC2FastLaunch cmdlet per disabilitare EC2 Fast Launch sull'AMI specificata e pulire gli snapshot preimpostati esistenti.

```
Disable-EC2FastLaunch -ImageId ami-0abcdef1234567890
```

Di seguito è riportato un output di esempio.

```
ImageId               : ami-0abcdef1234567890
 LaunchTemplate        :
 Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
 MaxParallelLaunches   : 6
 OwnerId               : 0123456789123
 ResourceType          : snapshot
 SnapshotConfiguration :
 State                 : disabling
 StateTransitionReason : Client.UserInitiated
```

```
StateTransitionTime   : 2/25/2022 1:10:08 PM
```

Usa un modello di avvio quando configuri EC2 Fast Launch

Con un modello di avvio puoi configurare una serie di parametri di avvio che Amazon EC2 utilizza ogni volta che avvia un'istanza da tale modello. Puoi specificare elementi come un'AMI da utilizzare per l'immagine di base, tipi di istanza, storage, impostazioni di rete e altro.

I modelli di avvio sono facoltativi, tranne nei casi specifici seguenti, in cui devi utilizzare un modello di avvio per l'AMI Windows quando configuri un avvio più rapido:

- Devi utilizzare un modello di avvio per specificare un VPC esistente per l'AMI Windows. Questo non si applica se utilizzi il VPC predefinito per il tuo Account AWS.
- Se il tuo account include una policy che applica IMDSv2 per istanze Amazon EC2, devi creare un modello di avvio che specifichi la configurazione dei metadati per applicare IMDSv2.

  Utilizza il modello di avvio che include la configurazione dei metadati dalla console EC2 o quando esegui il comando enable-fast-launch nell'azione o chiami l'API. AWS CLI EnableFastLaunch

EC2 Fast Launch non supporta la seguente configurazione quando si utilizza un modello di avvio. Se utilizzi un modello di avvio per EC2 Fast Launch, non devi necessariamente specificare le seguenti informazioni:

- Script di dati utente
- Termination protection (Protezione da cessazione)
- Metadati disabilitati
- Opzione Spot
- Comportamento di arresto che chiude l'istanza
- Tag di risorse per interfaccia di rete, grafica elastica o richieste di istanze spot

Specifica un VPC

Fase 1: creazione di un modello di avvio

Crea un modello di avvio che specifica i seguenti dettagli per le tue istanze di Windows:

- La sottorete VPC.

- Un tipo di istanza di `t3.xlarge`.

Per ulteriori informazioni, consulta Creare un modello di avvio Amazon EC2.

Passaggio 2: specifica il modello di avvio per l'AMI con EC2 Fast Launch

Console

Per specificare il modello di avvio per EC2 Fast Launch

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di spostamento, in Images (Immagini), scegliere AMI.
3. Selezionare l'AMI da aggiornare selezionando la casella di controllo accanto al Name (Nome).
4. Dal menu Operazioni sopra l'elenco delle AMI, scegli Configura avvio rapido. Si apre la pagina Configura avvio rapido, in cui configuri le impostazioni per EC2 Fast Launch.
5. La casella Modello di avvio esegue una ricerca filtrata che trova modelli di avvio nel tuo account nella regione corrente che corrispondono al testo che hai inserito. Specifica parte o tutto il nome o l'ID del modello di avvio nella casella per visualizzare un elenco di modelli di avvio corrispondenti. Ad esempio, se inserisci `fast` nella casella, Amazon EC2 trova tutti i modelli di avvio nel tuo account nella regione corrente che includono "fast" nel nome.

   Per creare un nuovo modello di avvio, puoi scegliere Crea modello di avvio.
6. Quando selezioni un modello di avvio, Amazon EC2 mostra la versione predefinita per tale modello nella casella Versione modello origine. Per specificare una versione diversa, evidenzia quella predefinita per sostituirla e inserisci il numero di versione desiderato nella casella.
7. Una volta completate le modifiche, scegliere Save (Salva).

AWS CLI

Per specificare il modello di avvio per EC2 Fast Launch

Utilizza il comando enable-fast-launch con l'opzione `--launch-template`, specificando il nome o l'ID del modello di avvio.

```
--launch-template LaunchTemplateName=my-launch-template
```

PowerShell

Per specificare il modello di avvio per EC2 Fast Launch

Utilizza il Enable-EC2FastLaunch cmdlet con il `-LaunchTemplate_LaunchTemplateId` parametro or. `-LaunchTemplate_LaunchTemplateName`

```
-LaunchTemplate_LaunchTemplateName my-launch-template
```

Per ulteriori informazioni sui modelli di avvio EC2, consulta Archivia i parametri di avvio dell'istanza nei modelli di avvio di Amazon EC2.

Controlli delle autorizzazioni per EC2 Fast Launch

Quando abiliti EC2 Fast Launch con un modello di avvio, puoi specificare una versione numerata del modello. Puoi anche usare la versione `$Latest` or`$Default`. Se utilizzi uno degli alias, l'alias può sovrascrivere le `iam:PassRole` autorizzazioni `ec2:RunInstances` and che intendevi limitare.

Quando abiliti EC2 Fast Launch, Amazon EC2 verifica le tue autorizzazioni rispetto alla versione corrente del modello di lancio. `$Latest`e `$Default` ciascuna si risolve in una versione specifica in quel momento. Questo controllo viene eseguito prima che Amazon EC2 abiliti la funzionalità. Convalida le autorizzazioni necessarie per avviare le istanze, ad esempio le autorizzazioni and. `ec2:RunInstances` `iam:PassRole` A tale scopo, EC2 Fast Launch emette una chiamata a `RunInstances` secco che verifica le autorizzazioni senza avviare un'istanza. Se le tue autorizzazioni non consentono un'azione richiesta, Amazon EC2 non risponde alla richiesta e restituisce un errore che descrive l'autorizzazione mancante. Amazon EC2 non abilita EC2 Fast Launch.

Una volta completato questo controllo iniziale, EC2 Fast Launch crea le istantanee predefinite in background. Quindi avvia le istanze utilizzando le autorizzazioni del suo ruolo collegato al servizio. Ogni volta che avvia un'istanza, utilizza la versione a cui si risolve in quel `$Latest` momento. `$Default` Ciò è vero anche se la versione è cambiata dopo il controllo iniziale. Non ricontrolla le tue autorizzazioni. Di conseguenza, qualcuno in grado di aggiornare il modello di avvio potrebbe passare un ruolo IAM o un profilo di istanza a un'istanza. Ciò può accadere anche se non dispone dell'`iam:PassRole`autorizzazione per quel ruolo.

Per assicurarti che Amazon EC2 utilizzi sempre la versione convalidata quando hai abilitato la funzionalità, specifica una versione numerata del modello di avvio. Non usare `$Latest` o `$Default`.

Se configuri EC2 Fast Launch per utilizzare la versione del modello di `$Default` avvio `$Latest` o Launch, ti consigliamo di limitare gli utenti che possono creare e gestire le

versioni del modello di avvio. Utilizza le policy IAM per limitare l'accesso ad azioni come `ec2:CreateLaunchTemplateVersion` `eec2:ModifyLaunchTemplate`.

Visualizza le AMI con EC2 Fast Launch abilitato

È possibile utilizzare il comando describe-fast-launch-images nel AWS CLI, o il comando Get-EC2FastLaunchImage Tools for PowerShell Cmdlet per ottenere dettagli sulle AMI con EC2 Fast Launch abilitato.

Amazon EC2 fornisce i seguenti dettagli per ogni AMI Windows restituita nei risultati:

- L'ID dell'immagine per un'AMI con EC2 Fast Launch abilitato.
- Il tipo di risorsa utilizzato per il pre-provisioning dell'AMI associata di Windows. Valore supportato: `snapshot`.
- Configurazione snapshot, ovvero un gruppo di parametri per la configurazione del pre-provisioning dell'AMI di Windows associata utilizzando gli snapshot.
- Avviare le informazioni sul modello, inclusi l'ID, il nome e la versione del modello di avvio utilizzato dall'AMI associata quando avvia le istanze Window da snapshot pre-provisioning.
- Il numero massimo di istanze che possono essere avviate contemporaneamente per la creazione di risorse.
- L'ID proprietario per l'AMI associata. Questo campo non è compilato per le AMI condivise con te.
- Lo stato attuale di EC2 Fast Launch per l'AMI associata. I valori supportati includono: `enabling | enabling-failed | enabled | enabled-failed | disabling | disabling-failed`.

> **Note**
>
> Puoi anche controllare lo stato corrente visualizzato nella pagina Gestisci ottimizzazione immagini nella console EC2, come Stato ottimizzazione immagine.

- Il motivo per cui EC2 Fast Launch per l'AMI associata è cambiato allo stato corrente.
- L'orario in cui EC2 Fast Launch per l'AMI associata è cambiato allo stato corrente.

AWS CLI

Per trovare AMI configurate per EC2 Fast Launch

Utilizza il seguente comando describe-fast-launch-images per descrivere i dettagli di ciascuna delle AMI nell'account configurate per EC2 Fast Launch. In questo esempio, una sola AMI nell'account è configurata per EC2 Fast Launch.

```
aws ec2 describe-fast-launch-images
```

Di seguito è riportato un output di esempio.

```
{
    "FastLaunchImages": [
        {
            "ImageId": "ami-01234567890abcedf",
            "ResourceType": "snapshot",
            "SnapshotConfiguration": {},
            "LaunchTemplate": {
                "LaunchTemplateId": "lt-01234567890abcedf",
                "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
                "Version": "1"
            },
            "MaxParallelLaunches": 6,
            "OwnerId": "0123456789123",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated",
            "StateTransitionTime": "2022-01-27T22:20:06.552000+00:00"
        }
    ]
}
```

PowerShell

Per trovare AMI configurate per EC2 Fast Launch

Utilizza il seguente Get-EC2FastLaunchImage cmdlet per descrivere i dettagli di ciascuna delle AMI dell'account configurate per EC2 Fast Launch. In questo esempio, una sola AMI nell'account è configurata per EC2 Fast Launch.

```
Get-EC2FastLaunchImage -ImageId ami-0abcdef1234567890
```

Di seguito è riportato un output di esempio.

```
ImageId               : ami-0abcdef1234567890
```

```
LaunchTemplate        :
 Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 012345678912
ResourceType          : snapshot
SnapshotConfiguration :
State                 : enabled
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:54:43 PM
```

Gestione dei costi per le risorse sottostanti di EC2 Fast Launch

Non sono previsti costi di servizio per configurare Windows AMIs per EC2 Fast Launch. Tuttavia, quando abiliti EC2 Fast Launch per un'AMI Amazon EC2 Windows, si applicano i prezzi standard per AWS le risorse sottostanti che Amazon EC2 utilizza per preparare e archiviare gli snapshot preimpostati. Puoi configurare i tag di allocazione dei costi per aiutarti a monitorare e gestire i costi associati EC2 alle risorse di Fast Launch. Per ulteriori informazioni su come configurare i tag per l'allocazione dei costi, consulta Tieni traccia dei costi di EC2 Fast Launch sulla tua bolletta.

L'esempio seguente mostra come potrebbero essere allocati i costi associati alle istantanee di EC2 Fast Launch.

Scenario di esempio: l'azienda AtoZ Example dispone di un'AMI Windows con un volume root EBS di 50 GiB. Abilitano EC2 Fast Launch per le loro AMI e impostano il numero di risorse target su cinque. Nel corso di un mese, l'utilizzo di EC2 Fast Launch per la loro AMI costa loro circa $5,00 e la ripartizione dei costi è la seguente:

1. Quando AtoZ Example abilita EC2 Fast Launch, Amazon EC2 avvia cinque piccole istanze. Ogni istanza viene eseguita attraverso le fasi di avvio di Sysprep e OOBE di Windows, riavviando secondo necessità. Ciò richiede diversi minuti per ogni istanza (il tempo può variare, in base a quanto è occupata la regione o la zona di disponibilità (AZ) e alle dimensioni dell'AMI).

   Costi

   - Costi di runtime dell'istanza (o runtime minimo, se applicabile): cinque istanze
   - Costi dei volumi: cinque volumi root EBS
2. Una volta completato il processo di pre-provisioning, Amazon EC2 scatta uno snapshot dell'istanza, che archivia in Amazon S3. Gli snapshot generalmente vengono archiviati per 4-8

ore prima di essere utilizzati da un avvio. In questo caso, il costo è di circa 0,02-0,05 USD per snapshot.

Costi

- Archiviazione degli snapshot (Amazon S3): cinque snapshot

3. Dopo che Amazon EC2 ha scattato lo snapshot, interrompe l'istanza. A quel punto, l'istanza non accumula più costi. Tuttavia, i costi del volume EBS continuano ad accumularsi.

   Costi

   - Volumi EBS: i costi continuano per i volumi root EBS associati.

> **Note**
>
> I costi qui riportati sono solo a scopo dimostrativo. I costi variano a seconda del piano tariffario e della configurazione AMI.

Tieni traccia dei costi di EC2 Fast Launch sulla tua bolletta

I tag di allocazione dei costi possono aiutarti a organizzare la AWS fattura in modo da rispecchiare i costi associati a EC2 Fast Launch. Puoi utilizzare il seguente tag che Amazon EC2 aggiunge alle risorse che crea quando prepara e archivia istantanee pre-assegnate per Fast Launch: EC2

Chiave di tag: `CreatedBy`, Valore: `EC2 Fast Launch`

Dopo aver attivato il tag nella console Gestione costi e fatturazione e aver impostato un report di fatturazione dettagliato, la colonna `user:CreatedBy` viene visualizzata nel report. La colonna include i valori di tutti i servizi. Tuttavia, se scarichi il file CSV, puoi importare i dati in un foglio di calcolo e filtrare per `EC2 Fast Launch` nel valore. Queste informazioni vengono visualizzate anche nel momento in AWS Cost and Usage Report cui il tag viene attivato.

Fase 1: attivazione dei tag di allocazione dei costi definiti dall'utente

Per includere i tag delle risorse nei report sui costi, devi prima attivare i tag nella console Gestione costi e fatturazione. Per ulteriori informazioni, consulta la sezione relativa all'attivazione dei tag per l'allocazione dei costi definiti dall'utente nella Guida per l'utente di Gestione costi e fatturazione AWS .

> **Note**
>
> L'attivazione può richiedere fino a 24 ore.

Fase 2: impostazione di un report sui costi

Se hai già impostato un report sui costi, una colonna per il tag viene visualizzata la volta successiva che il report viene eseguito dopo il completamento dell'attivazione. Per impostare i report sui costi per la prima volta, scegli una delle opzioni seguenti.

- Consulta Impostazione di un report di allocazione dei costi mensili nella Guida per l'utente di Gestione costi e fatturazione AWS .
- Consulta Creazione di report su costi e utilizzo nella Guida per l'utente di AWS Cost and Usage Report .

> **Note**
>
> Possono essere necessarie fino a 24 ore prima che inizi AWS a inviare report al tuo bucket S3.

Puoi configurare EC2 Fast Launch for Windows AMIs di tua proprietà o AMIs che è condiviso con te dalla EC2 console Amazon SDKs CloudFormation, dall'API o dai ec2 comandi in AWS CLI. Le seguenti sezioni illustrano i passaggi di configurazione per la EC2 console Amazon e AWS CLI.

È inoltre possibile creare finestre personalizzate AMIs configurate per EC2 Fast Launch con EC2 Image Builder. Per ulteriori informazioni, consulta Creare impostazioni di distribuzione per un'AMI Windows con EC2 Fast Launch abilitato (AWS CLI).

Monitora l'avvio EC2 rapido

Questa sezione spiega come monitorare Amazon EC2 Windows Server AMIs nel tuo account con EC2 Fast Launch abilitato.

Monitora le modifiche allo stato di EC2 Fast Launch EventBridge

Quando lo stato cambia per un'AMI Windows con EC2 Fast Launch abilitato, Amazon EC2 genera un `EC2 Fast Launch State-change Notification` evento. Quindi Amazon EC2 invia l'evento

di modifica dello stato ad Amazon EventBridge (precedentemente noto come Amazon CloudWatch Events).

Puoi creare EventBridge regole che attivano una o più azioni in risposta all'evento di cambio di stato. Ad esempio, è possibile creare una EventBridge regola che rileva quando EC2 Fast Launch è abilitato ed esegue le seguenti azioni:

- Invia un messaggio a un argomento Amazon SNS per avvisare i propri abbonati.
- Richiama una funzione Lambda che esegue una determinata operazione.
- Invia i dati di modifica dello stato ad Amazon Data Firehose per l'analisi.

Per ulteriori informazioni, consulta la sezione Creazione di EventBridge regole Amazon che reagiscono agli eventi nella Amazon EventBridge User Guide.

Eventi di modifica dello stato

La funzione EC2 Fast Launch emette eventi di modifica dello stato in formato JSON nel miglior modo possibile. Amazon EC2 invia gli eventi quasi EventBridge in tempo reale. Questa sezione descrive i campi dell'evento e mostra un esempio del relativo formato.

`EC2 Fast Launch State-change Notification`

imageId

Identifica l'AMI con la modifica dello stato di EC2 Fast Launch.

resourceType

Il tipo di risorsa da utilizzare per il pre-provisioning. Valore supportato: `snapshot`. Il valore predefinito è `snapshot`.

stato

Lo stato attuale della funzionalità EC2 Fast Launch per l'AMI specificata. I valori validi includono quanto segue:

- attivazione: hai abilitato la funzionalità EC2 Fast Launch per l'AMI e Amazon EC2 ha iniziato a creare istantanee per il processo di pre-provisioning.
- enabling-failed: si è verificato un errore che ha causato il fallimento del processo di pre-provisioning la prima volta che hai abilitato Fast EC2 Launch per un'AMI. Questo può accadere in qualsiasi momento durante il processo di pre-provisioning.

- abilitato: la funzionalità EC2 Fast Launch è abilitata. Lo stato cambia non `enabled` appena Amazon EC2 crea la prima snapshot pre-configurata per un'AMI Fast EC2 Launch appena abilitata. Se l'AMI era già abilitata e viene nuovamente sottoposta al pre-provisioning, la modifica dello stato avviene immediatamente.
- enabled-failed: questo stato si applica solo se non è la prima volta che l'AMI Fast EC2 Launch esegue il processo di pre-provisioning. Ciò può verificarsi se la funzionalità EC2 Fast Launch è disabilitata e successivamente riattivata, oppure se si verifica una modifica della configurazione o un altro errore dopo il completamento del pre-provisioning per la prima volta.
- disabilitazione: il proprietario dell'AMI ha disattivato la funzionalità EC2 Fast Launch per l'AMI e Amazon EC2 ha avviato il processo di pulizia.
- disabilitata: la funzione EC2 Fast Launch è disabilitata. Lo stato cambia non `disabled` appena Amazon EC2 completa il processo di pulizia.
- disabling-failed: il processo di pulizia ha avuto esito negativo a causa di un errore. Ciò significa che alcuni snapshot sottoposti a pre-provisioning potrebbero ancora essere presenti nell'account.

stateTransitionReason

Il motivo per cui lo stato è cambiato per l'AMI EC2 Fast Launch.

> **Note**
>
> Tutti i campi di questo messaggio di evento sono obbligatori.

L'esempio seguente mostra un'AMI EC2 Fast Launch appena abilitata che ha lanciato la prima istanza per avviare il processo di pre-provisioning. A questo punto, lo stato è `enabling`. Dopo che Amazon ha EC2 creato la prima istantanea predisposta, lo stato cambia in. `enabled`

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "EC2 Fast Launch State-change Notification",
 "source": "aws.ec2",
 "account": "123456789012",
 "time": "2022-08-31T20:30:12Z",
 "region": "us-east-1",
 "resources": [
```

```
  "arn:aws:ec2:us-east-1:123456789012:image/ami-123456789012"
 ],
 "detail": {
  "imageId": "ami-123456789012",
  "resourceType": "snapshot",
  "state": "enabling",
  "stateTransitionReason": "Client.UserInitiated"
 }
}
```

Monitora le metriche di EC2 Fast Launch con CloudWatch

Amazon EC2 AMIs con EC2 Fast Launch abilitato invia metriche ad Amazon CloudWatch. Puoi utilizzare il Console di gestione AWS AWS CLI, the o un'API per elencare le metriche inviate da EC2 Fast Launch. CloudWatch Il `AWS/EC2` namespace include le seguenti metriche di EC2 Fast Launch:

Metrica	Description
NumberOfAvailableFastLaunchSnapshots	Il numero di istantanee preconfigurate disponibili per ogni AMI abilitata a EC2 Fast Launch.
NumberOfInstancesFastLaunched	Il numero di istanze per ogni AMI abilitata a EC2 Fast Launch che sono state lanciate da istantanee predisposte.
NumberOfInstancesNotFastLaunched	Il numero di istanze per ogni AMI abilitata a EC2 Fast Launch ha comportato un avvio a freddo a causa della mancanza di istantane e preconfigurate disponibili al momento del lancio.
FastLaunchSnapshotUsedToRefillStartTime	Il timestamp in cui Amazon EC2 ha lanciato una nuova immagine da EC2 Fast Launch ha consentito all'AMI di creare un'altra istantanea dopo l'utilizzo di una snapshot esistente.
FastLaunchSnapshotCreationTime	Misura il tempo impiegato EC2 da Amazon per avviare un'istanza e creare uno snapshot per un'AMI abilitata a EC2 Fast Launch.

Service-linked ruolo per EC2 Fast Launch

Amazon EC2 utilizza ruoli collegati ai servizi per le autorizzazioni di cui ha bisogno per eseguire chiamate ad altri Servizi AWS per tuo conto. Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a un. Servizio AWS Service-linked i ruoli forniscono un modo sicuro per delegare le autorizzazioni Servizi AWS perché solo il servizio collegato può assumere un ruolo collegato al servizio. Per ulteriori informazioni sull'utilizzo dei ruoli IAM da parte di Amazon EC2, consultare Ruoli IAM per Amazon EC2.

Amazon EC2 utilizza il ruolo collegato ai servizi denominato AWSServiceRoleForEC2FastLaunch per creare e gestire una serie di snapshot pre-provisioning che riducono il tempo necessario all'avvio delle istanze dall'AMI di Windows.

Autorizzazioni concesse da AWSServiceRoleForEC2FastLaunch

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi AWSServiceRoleForEC2FastLaunch considera attendibile il seguente servizio:

- `ec2fastlaunch.amazonaws.com`

Amazon EC2 utilizza la policy gestita EC2FastLaunchServiceRolePolicy per completare le operazioni seguenti:

- AWS CloudFormation— Consenti a EC2 Fast Launch di ottenere una descrizione degli stack associati CloudFormation .
- Amazon CloudWatch: pubblica i dati metrici associati a EC2 Fast Launch nel namespace Amazon EC2.
- Amazon EC2: viene concesso l'accesso a EC2 Fast Launch per eseguire le seguenti operazioni:
  - Avvia le istanze da un'AMI Windows Server di Amazon EC2 con EC2 Fast Launch abilitato, per eseguire le fasi di provisioning. Specifica inoltre un modello di risorse che consenta `ec2:RunInstances` per un'AMI associata a License Manager.
  - Arresta e termina un'istanza lanciata da EC2 Fast Launch dopo che questa ha creato lo snapshot con pre-provisioning.
  - Descrivi le risorse di immagine e di tipo di istanza utilizzate per avviare istanze da un'AMI Windows Server Amazon EC2 con EC2 Fast Launch abilitato e creare snapshot da esse.
  - Descrivi le risorse del modello di avvio e avvia le istanze da un modello di avvio.
  - Descrivi le istanze, gli attributi dell'istanza e lo stato dell'istanza, i volumi e gli attributi del volume.

  - Descrivi le interfacce di rete.
  - Elimina le risorse create da EC2 Fast Launch, tra cui snapshot, modelli di avvio, volumi e interfacce di rete.
  - Contrassegna le risorse create da EC2 Fast Launch per avviare ed effettuare il pre-provisioning delle istanze Windows, e creare snapshot da utilizzare durante il processo di avvio finale.
- Amazon EventBridge: include l'accesso per creare regole di EventBridge evento e recuperare i dettagli o eliminare le regole che ha creato. EC2 Fast Launch può anche ottenere un elenco di servizi di destinazione che ricevono eventi EC2 Fast Launch inoltrati in base alle regole degli eventi e aggiungere o rimuovere servizi di destinazione dalle regole degli eventi creati.
- IAM: consenti a EC2 Fast Launch di creare il ruolo collegato al servizio `EC2FastLaunchServiceRolePolicy`, di ottenere e utilizzare i profili dell'istanza il cui nome contiene `ec2fastlaunch`, e di avviare istanze per tuo conto utilizzando il profilo dell'istanza dal modello di avvio.
- AWS KMS: include l'accesso per creare sovvenzioni ed elencare quelle create da EC2 Fast Launch che possono essere ritirate. Inoltre, per descrivere o utilizzare le chiavi allo scopo di crittografare o decriptare i volumi collegati alle istanze create da EC2 Fast Launch e per generare chiavi di dati che non siano testo normale.

Per vedere le autorizzazioni per questa policy, consulta EC2FastLaunchServiceRolePolicy nella Guida di riferimento sulle policy gestite da AWS .

Per ulteriori informazioni sulle policy gestite in Amazon EC2, consultare AWS policy gestite per Amazon EC2.

Crea un ruolo collegato al servizio

Non è necessario creare manualmente questo ruolo collegato ai servizi. Quando inizi a utilizzare EC2 Fast Launch per l'AMI, Amazon EC2 crea automaticamente il ruolo collegato ai servizi, se non esiste ancora.

Se il ruolo collegato ai servizi viene eliminato dall'account, puoi abilitare EC2 Fast Launch per un'altra AMI Windows per ricreare il ruolo nell'account. In alternativa, puoi disabilitare EC2 Fast Launch per l'AMI corrente e quindi abilitarla nuovamente. Tuttavia, la disabilitazione della funzionalità comporta l'AMI del processo di avvio standard per tutte le nuove istanze mentre Amazon EC2 rimuove tutti gli snapshot con pre-provisioning. Dopo che tutti gli snapshot con pre-provisioning sono stati rimossi, puoi abilitare nuovamente EC2 Fast Launch per l'AMI.

Accesso alle chiavi gestite dal cliente

Per abilitare EC2 Fast Launch per un'AMI crittografata che utilizza una chiave gestita dal cliente per la crittografia, devi concedere l'autorizzazione al ruolo AWSServiceRoleForEC2FastLaunch per utilizzare la CMK. Per effettuare questa operazione, chiama il comando create-grant. Per `--grantee-principal`, specifica l'ARN per il ruolo AWSServiceRoleForEC2FastLaunch nel tuo account. Per `--operations`, specificare `CreateGrant`.

```
aws kms create-grant \
    --key-id arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2FastLaunch \
    --operations CreateGrant
```

Modifica di un ruolo collegato al servizio

Amazon EC2 non consente di modificare il ruolo collegato ai servizi AWSServiceRoleForEC2FastLaunch. Dopo aver creato un ruolo collegato ai servizi, non è possibile modificarne il nome, perché varie entità possono farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio

È possibile eliminare un ruolo collegato ai servizi solo dopo avere eliminato le risorse correlate. In tal modo, vengono protette le risorse Amazon EC2 associate alla tua AMI Windows Server Amazon EC2 con EC2 Fast Launch abilitato, in quanto impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Usa la console IAM AWS CLI, l'API o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForEC2FastLaunch servizio. Per ulteriori dettagli, consulta Delete a service-linked role nella Guida per l'utente IAM.

Regioni supportate

Amazon EC2 supporta EC2 Fast Launch per il ruolo collegato ai servizi in tutte le regioni in cui è disponibile il servizio Amazon EC2.

Risolvi i problemi relativi a Windows EC2 Fast Launch

Scenari per la risoluzione dei problemi

I seguenti scenari possono diagnosticare e risolvere i problemi comuni che possono verificarsi durante il tentativo di attivazione di EC2 Fast Launch.

Impossibile interrompere l'istanza per la creazione di snapshot

Description

Quando abiliti EC2 Fast Launch, il servizio avvia una serie di istanze utilizzate per creare gli snapshot con pre-provisioning. A ciascuna istanza vengono concessi 30 minuti per completare il processo. Se una delle istanze viene completata correttamente, il servizio imposta lo stato di Fast Launch per l'AMI su `Enabled`. Tuttavia, se un'istanza non riesce a completare il processo entro il tempo assegnato e nessuna delle altre istanze lo ha completato, il servizio termina tutte le istanze e imposta lo stato di Fast Launch per l'AMI su `enabling_failed` e il motivo dello stato di Fast Launch su quanto segue:

```
Unable to stop instance ID=i-1234567890abcdef0 for snapshot creation.
```

Causa

Molto spesso, questo è causato dal tentativo di abilitare EC2 Fast Launch per un'AMI Windows creata da un'istanza in esecuzione o un'AMI che non soddisfa tutti i EC2 Prerequisiti Fast Launch.

Soluzione

Assicurati che l'AMI che usi soddisfi tutti i EC2 Prerequisiti Fast Launch.

Per configurare EC2 Fast Launch per un'AMI, crea l'AMI utilizzando Sysprep con l'opzione di spegnimento. Per ulteriori informazioni, consulta Creare un'AMI Amazon EC2 utilizzando Windows Sysprep.

Hai raggiunto il limite del tuo VPC

Description

Se non utilizzi un modello di avvio per specificare un VPC esistente e non hai definito un VPC predefinito per il tuo account, il servizio crea automaticamente uno CloudFormation stack che include un VPC e altre risorse, come descritto in. EC2 Prerequisiti Fast Launch

Causa

Hai raggiunto il numero massimo di VPC consentiti nel tuo Account AWS per la regione e non hai specificato un VPC esistente che deve essere utilizzato da EC2 Fast Launch. Questo causa il fallimento del processo.

Soluzione

Puoi affrontare questo problema con una delle opzioni seguenti:

- Puoi richiedere un aumento della quota.
- Puoi fornire un modello di avvio che specifichi un VPC esistente

Per richiedere un aumento del numero di VPC che il tuo account può definire per regione, segui questi passaggi:

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/.
2. Nella dashboard della console di servizio, scegli Amazon Virtual Private Cloud (Amazon VPC). Si aprono le quote di servizio di VPC.
3. Filtra su `VPCs per Region` per andare direttamente alla quota.
4. Seleziona VPC per regione e scegli Richiedi aumento a livello di account.

Se hai una richiesta urgente di quote o se la tua richiesta di aumento della quota viene rifiutata, contatta il Supporto per ricevere assistenza. Per ulteriori informazioni, consulta Richiesta di un aumento delle quote nella Guida per l'utente di Service Quotas.

Autorizzazioni insufficienti per abilitare EC2 Fast Launch

Description

Quando abiliti EC2 Fast Launch per la prima volta senza specificare un modello di avvio, EC2 Fast Launch crea uno stack di CloudFormation di proprietà del servizio con risorse predefinite del servizio. Tuttavia, i CloudFormation modelli non verranno distribuiti se il responsabile IAM (ruolo o utente) non dispone delle autorizzazioni necessarie.

Il messaggio di log può essere simile a quanto segue:

```
Can't enable EC2 Fast Launch. The IAM credentials that you are using do not have
 sufficient permissions. Attach EC2FastLaunchFullAccess in the IAM console.
```

Causa

Il tuo ruolo o utente IAM non dispone delle autorizzazioni necessarie per abilitare EC2 Fast Launch.

Soluzione

Verifica che il principale IAM (utente o ruolo) che abilita EC2 Fast Launch disponga della policy di `EC2FastLaunchFullAccess` allegata. Questa policy AWS gestita garantisce l'accesso completo a tutte le risorse EC2 Fast Launch. Per vedere le autorizzazioni per questa policy, consulta la policy EC2FastLaunchFullAccess nella Guida di riferimento sulle policy gestite da AWS .

Modifica della password dell'amministratore Windows per un'istanza Amazon EC2

Se avvii l'istanza da un'AMI AWS Windows, gli agenti di avvio preinstallati impostano la password predefinita come segue:

- Per Windows Server 2022 e versioni successive, EC2Launch v2 genera la password predefinita.
- Per Windows Server 2016 e 2019, l'agente EC2Launch genera la password predefinita.
- Per Windows Server 2012 R2 e versioni precedenti, EC2Config service genera la password predefinita.

> **Note**
>
> Per Windows Server 2016 e AMI successive, `Password never expires` è disattivata per l'amministratore locale. Per le versioni AMI precedenti a Windows Server 2016, `Password never expires` è abilitata per l'amministratore locale.

Modifica della password dell'amministratore dopo la connessione

Quando ti connetti a un'istanza per la prima volta, ti consigliamo di modificare il valore predefinito della password dell'amministratore. La procedura seguente ti permette di modificare la password dell'amministratore per un'istanza Windows.

> **Important**
>
> Conserva la nuova password in un luogo sicuro. Non sarà possibile recuperarla tramite la console Amazon EC2. La console può solo recuperare la password predefinita. Se tenti di

connetterti all'istanza utilizzando la password predefinita dopo averla modificata, riceverai un messaggio di errore "Your credentials did not work" (Le credenziali specificate non funzionano).

Per modificare la password dell'amministratore locale

1. Collegati all'istanza e apri il prompt dei comandi.
2. Esegui il comando riportato qui di seguito. Se la tua nuova password contiene caratteri speciali, racchiudila tra virgolette.

```
net user Administrator "new_password"
```

3. Conserva la nuova password in un luogo sicuro.

Modifica di una password persa o scaduta

Se perdi la password o questa scade, puoi generare una nuova password. Per le procedure di reimpostazione della password, consulta Reimpostazione della password dell'amministratore Windows per un'istanza Amazon EC2 Windows.

Aggiungi componenti Windows Server opzionali alle istanze Amazon EC2 Windows

Per accedere ai componenti opzionali e installarli, devi individuare lo snapshot EBS corretto per la versione in uso di Windows Server, creare un volume dallo snapshot e collegare il volume all'istanza specifica.

Prima di iniziare

Usa lo strumento da riga di comando Console di gestione AWS o per ottenere l'ID dell'istanza e la zona di disponibilità della tua istanza. Devi creare il volume EBS nella stessa zona di disponibilità dell'istanza.

Esegui una delle seguenti procedure per aggiungere i componenti di Windows Server alla tua istanza.

Console

Per aggiungere i componenti di Windows all'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Snapshots (Snapshot).
3. Nella barra Filter (Filtro), scegliere Public Snapshots (Snapshot pubbliche).
4. Aggiungere il filtro Owner (Proprietario) e scegliere Amazon images (Immagini Amazon).
5. Aggiungere il filtro Description (Descrizione) e digitare **`Windows`**.
6. Premere Invio.
7. Selezionare lo snapshot corrispondente all'architettura del sistema e alla preferenza di lingua. Ad esempio, selezionare Windows 2019 English Installation Media (Supporto di installazione Windows 2019 in lingua inglese) se l'istanza in uso esegue Windows Server 2019.
8. Scegliere Actions (Operazioni),Create volume from snapshot (Crea volume da snapshot).
9. In Availability Zone (Zona di disponibilità), selezionare la zona di disponibilità corrispondente all'istanza di Windows. Scegliere Add tag (Aggiungi tag) e specificare **`Name`** per la chiave tag e un nome descrittivo per il valore del tag. Selezionare Create volume (Crea volume).
10. Nel messaggio Successfully created volume (Volume creato correttamente), scegliere il volume appena creato.
11. Scegliere Actions (Operazioni), Attach Volume (Collega volume).
12. Da Instance (Istanza), selezionare l'ID dell'istanza.
13. Per Device name (Nome dispositivo), inserire il nome del dispositivo per l'allegato. In caso di dubbi con il nome del dispositivo, consultare Nomi dei dispositivi per i volumi sulle EC2 istanze Amazon.
14. Scegli Attach volume (Collega volume).
15. Connettersi all'istanza e rendere disponibile il volume. Per ulteriori informazioni, consulta la pagina Rendere un volume Amazon EBS disponibile per l'uso nella Guida per l'utente di Amazon EBS.

    > **Important**
    >
    > Non inizializzare il volume.

16. Aprire Control Panel (Pannello di controllo), Programs and Features (Programmi e funzionalità). Scegliere Turn Windows features on or off (Attiva o disattiva funzionalità

di Windows). Se viene richiesto il supporto di installazione, specificare il volume EBS contenente il supporto di installazione.

17. (Facoltativo) Dopo aver terminato con il supporto di installazione, è possibile scollegare il volume. Dopo aver scollegato il volume, è possibile eliminarlo.

AWS CLI

Per aggiungere i componenti di Windows all'istanza

1. Utilizzare il comando describe-snapshots con il parametro `owner-ids` e il filtro `description` per recuperare l'elenco degli snapshot dei supporti di installazione disponibili.

```
aws ec2 describe-snapshots \
    --owner-ids amazon \
    --filters Name=description,Values=Windows*
```

2. Facendo riferimento all'output annotare l'ID dello snapshot corrispondente all'architettura del sistema e alla preferenza di lingua. Ad esempio:

```
{
    "Snapshots": [
    ...
        {
            "OwnerAlias": "amazon",
            "Description": "Windows 2019 English Installation Media",
            "Encrypted": false,
            "VolumeId": "vol-be5eafcb",
            "State": "completed",
            "VolumeSize": 6,
            "Progress": "100%",
            "StartTime": "2019-10-25T20:00:47.000Z",
            "SnapshotId": "snap-22da283e",
            "OwnerId": "123456789012"
        },
    ...
   ]
}
```

3. Utilizzare il comando create-volume per creare un volume dallo snapshot. Specificare la stessa zona di disponibilità dell'istanza.

```
aws ec2 create-volume \
    --snapshot-id snap-0abcdef1234567890 \
    --volume-type gp2 \
    --availability-zone us-east-1a
```

4. Facendo riferimento all'output, annotare l'ID del volume.

```
{
    "AvailabilityZone": "us-east-1a",
    "Encrypted": false,
    "VolumeType": "gp2",
    "VolumeId": "vol-01234567890abcdef",
    "State": "creating",
    "Iops": 100,
    "SnapshotId": "snap-0abcdef1234567890",
    "CreateTime": "2017-04-18T10:33:10.940Z",
    "Size": 6
}
```

5. Utilizzare il comando attach-volume per collegare il volume all'istanza.

```
aws ec2 attach-volume \
    --volume-id vol-0c98b37f30bcbc290 \
    --instance-id i-01474ef662b89480 \
    --device xvdg
```

6. Connettersi all'istanza e rendere disponibile il volume. Per ulteriori informazioni, consulta la pagina Rendere un volume Amazon EBS disponibile per l'uso nella Guida per l'utente di Amazon EBS.

> **Important**
>
> Non inizializzare il volume.

7. Aprire Control Panel (Pannello di controllo), Programs and Features (Programmi e funzionalità). Scegliere Turn Windows features on or off (Attiva o disattiva funzionalità di Windows). Se viene richiesto il supporto di installazione, specificare il volume EBS contenente il supporto di installazione.

8. (Facoltativo) Al termine del supporto di installazione, utilizzare il comando detach-volume per scollegare il volume dall'istanza. Dopo aver scollegato il volume, è possibile utilizzare il comando delete-volume per eliminare il volume.

PowerShell

Per aggiungere i componenti di Windows all'istanza

1. Utilizza il Get-EC2Snapshot cmdlet con i `description` filtri `Owner` and per ottenere un elenco delle istantanee dei supporti di installazione disponibili.

```
Get-EC2Snapshot `
    -Owner amazon `
    -Filter @{ Name="description"; Values="Windows*" }
```

2. Facendo riferimento all'output annotare l'ID dello snapshot corrispondente all'architettura del sistema e alla preferenza di lingua. Ad esempio:

```
...
DataEncryptionKeyId :
Description         : Windows 2019 English Installation Media
Encrypted           : False
KmsKeyId            :
OwnerAlias          : amazon
OwnerId             : 123456789012
Progress            : 100%
SnapshotId          : snap-0abcdef1234567890
StartTime           : 10/25/2019 8:00:47 PM
State               : completed
StateMessage        :
Tags                : {}
VolumeId            : vol-01234567890abcdef
VolumeSize          : 6
...
```

3. Utilizzare il New-EC2Volume cmdlet per creare un volume dall'istantanea. Specificare la stessa zona di disponibilità dell'istanza.

```
New-EC2Volume `
    -AvailabilityZone us-east-1a `
    -VolumeType gp2 `
```

```
    -SnapshotId snap-0abcdef1234567890
```

4. Facendo riferimento all'output, annotare l'ID del volume.

```
Attachments      : {}
AvailabilityZone : us-east-1a
CreateTime       : 4/18/2017 10:50:25 AM
Encrypted        : False
Iops             : 100
KmsKeyId         :
Size             : 6
SnapshotId       : snap-0abcdef1234567890
State            : creating
Tags             : {}
VolumeId         : vol-01234567890abcdef
VolumeType       : gp2
```

5. Usa il Add-EC2Volume cmdlet per collegare il volume alla tua istanza.

```
Add-EC2Volume `
    -InstanceId i-1234567890abcdef0 `
    -VolumeId vol-01234567890abcdef `
    -Device xvdh
```

6. Connettersi all'istanza e rendere disponibile il volume. Per ulteriori informazioni, consulta la pagina Rendere un volume Amazon EBS disponibile per l'uso nella Guida per l'utente di Amazon EBS.

> **Important**
>
> Non inizializzare il volume.

7. Aprire Control Panel (Pannello di controllo), Programs and Features (Programmi e funzionalità). Scegliere Turn Windows features on or off (Attiva o disattiva funzionalità di Windows). Se viene richiesto il supporto di installazione, specificare il volume EBS contenente il supporto di installazione.

8. (Facoltativo) Al termine del supporto di installazione, utilizza il Dismount-EC2Volume cmdlet per scollegare il volume dall'istanza. Dopo aver scollegato il volume, è possibile utilizzare il Remove-EC2Volume cmdlet per eliminare il volume.

Installazione del sottosistema Windows per Linux sulla tua istanza EC2 Windows

Il Sottosistema Windows per Linux (Windows Subsystem for Linux, WSL) è una funzionalità di Microsoft Windows. Installando WSL sulla tua istanza EC2 Windows, puoi eseguire strumenti Linux nativi direttamente sulla tua istanza Windows.

Esistono due versioni del Sottosistema Windows per Linux: WSL 1 e WSL 2. Per ulteriori informazioni, consulta Documentazione del sottosistema Windows per Linux sul sito Web di Microsoft.

Requisiti

- Il sistema operativo deve essere Windows Server 2019 o versioni successive.
- È possibile installare WSL 1 solo su istanze Windows virtualizzate (la dimensione dell'istanza non supporta `.metal` o non supporta la virtualizzazione annidata).
- È possibile installare WSL 1 o WSL 2 su istanze che supportano la virtualizzazione annidata e che hanno l'opzione CPU abilitata. `NestedVirtualization`
- Puoi installare WSL 1 o WSL 2 sulle istanze bare metal (la dimensione dell'istanza è `.metal`). Per impostazione predefinita, le istanze bare metal forniscono il supporto richiesto per la virtualizzazione annidata.

Per ulteriori informazioni sulla virtualizzazione annidata per EC2, vedere. Usa la virtualizzazione annidata per eseguire hypervisor nelle istanze Amazon EC2

Installazione di WSL sulla tua istanza di Windows

Per installare WSL 1

1. Installa il WSL, Il processo da seguire dipende dalla versione di Windows Server in esecuzione sull'istanza.
   - Windows Server 2022 e successiva: esegui il seguente comando di installazione standard sulla tua istanza EC2.

     ```
     wsl --install --enable-wsl1 --no-launch
     ```

   - Windows Server 2019: abilita il WSL e quindi installa il WSL come descritto in Installare WSL nelle versioni precedenti di Windows Server sul sito Web di Microsoft.

2. Riavviare l'istanza EC2.

```
shutdown -r -t 20
```

3. Per configurare WSL in modo che utilizzi WSL 1, eseguire il seguente comando sulla propria istanza. Questo passaggio è necessario per le istanze virtualizzate (la dimensione dell'istanza non è configurata `.metal` o non è configurata per la virtualizzazione annidata).

```
wsl --set-default-version 1
```

4. Installa la distribuzione predefinita.

```
wsl --install
```

Per installare WSL 2 (.metal o istanze con virtualizzazione annidata abilitata)

esegui il seguente comando di installazione standard sull'istanza EC2. Per impostazione predefinita, è installato WSL 2.

```
wsl --install
```

Utilità per la risoluzione dei problemi di Windows EC2

Il driver `EC2WinUtil` fornisce i seguenti tipi di supporto per la risoluzione dei problemi per l'istanza Windows.

Stack delle chiamate di arresto anomalo

`EC2WinUtil` raccoglie informazioni di base sugli arresti anomali dall'istanza e le scrive sulla console seriale. L'elenco seguente include alcuni dei dettagli chiave che l'utilità scrive sulla console.

- Identificazione del modulo che ha generato l'errore.
- Il codice di errore Windows associato all'evento.
- Una traccia dello stack delle chiamate più recenti.

Con questi dettagli, puoi eseguire un'analisi iniziale della causa principale e determinare se sono necessarie ulteriori analisi. L'output sulla console seriale consente inoltre di AWS tenere traccia

delle tendenze dei crash per i driver Amazon EC2 e di diagnosticare eventi di crash su larga scala.

> **Note**
>
> `EC2WinUtil` non raccoglie dati sui clienti nei suoi stack delle chiamate di arresto anomalo.

Per le note di rilascio del driver, consulta Cronologia delle versioni di EC2 Windows Utility Driver

Cronologia delle versioni di EC2 Windows Utility Driver

La tabella seguente riporta i driver `EC2WinUtil` da eseguire su ciascuna versione di Windows Server su Amazon EC2. Le versioni precedenti del sistema operativo utilizzano il driver preinstallato sulle AMI di AWS Windows Server da cui è stata avviata l'istanza. Nelle AMI condivise con te o a cui ti iscrivi tramite abbonamento Marketplace AWS non è preinstallato il driver.

Versione di Windows Server	EC2WinUtil versione del driver
Windows Server 2025	versione più recente
Windows Server 2022	versione più recente
Windows Server 2019	versione più recente
Windows Server 2016	versione più recente

> **Note**
>
> Prima della versione 3.0.0, il driver `EC2WinUtil` non era disponibile per il download per l'installazione manuale. Le versioni precedenti erano disponibili solo come driver preinstallati per le AMI AWS Windows.

La tabella seguente descrive le versioni rilasciate del driver `EC2WinUtil`.

Versione del pacchetto	Versione driver	Dettagli	Data di rilascio
3.2.0	3.2.0	Meccanismo di registrazione della console migliorato da utilizzare con l'agente EC2Launch v2.	2 giugno 2026
3.1.1	3.1.1	Aumento della lunghezza dello stack di chiamate durante la registrazione all'output della console.	3 marzo 2026
3.1.0	3.1.0	Migliore gestione degli eventi di gestione dell'alim entazione.	4 febbraio 2026
3.0.0	3.0.0	È stato modernizzato il driver per Windows 10 e aggiunto il supporto per l'installazione come driver primitivo.	13 giugno 2024
2.0.0	2.0.0	È stato aggiunto il supporto per l'output su porte seriali MMIO per tipi di istanze metal. Inoltre, è stata migliorat a l'analisi degli arresti anomali e aggiornato il formato di output.	23 agosto 2018
1.0.1	1.0.1	È stato modificato il nome del driver in `EC2WinUtil` per via di un conflitto di spazio dei nomi con Amazon Inspector. Sono incluse diverse correzioni di bug.	1 marzo 2018
1.0.0	1.0.0	Versione iniziale. Il driver è stato inizialmente chiamato `AwsAgent`.	28 novembre 2017

Aggiornamento di un'istanza EC2 Windows a una versione più recente di Windows Server

Se è il momento di aggiornare il sistema operativo Windows Server sulla tua istanza EC2 Windows da una versione precedente, puoi utilizzare uno dei seguenti metodi.

In-place aggiornamento

Un aggiornamento locale opera su un'istanza esistente. Questo processo influisce solo sui file del sistema operativo, mentre le impostazioni, i ruoli del server e i dati rimangono intatti.

Migrazione (nota anche come aggiornamento side-by-side)

La migrazione implica l'acquisizione di impostazioni, configurazioni e dati che vengono trasferiti su un sistema operativo più recente su un'istanza EC2 Windows aggiornata. Puoi avviare la tua istanza da un'AMI Windows pubblica o privata a cui ti Marketplace AWS iscrivi o da un'AMI condivisa con te. Inoltre, puoi creare un'AMI personalizzata con EC2 Image Builder. Per ulteriori informazioni, consulta la Guida per l'utente a Image Builder.

> **Note**
>
> AWS fornisce un set di Amazon Machine Images (AMI) disponibili pubblicamente per le versioni di Windows Server eseguite su istanze EC2. Queste AMI vengono aggiornate su base mensile. Per ulteriori informazioni sulle AMI di Windows più recenti, consulta Riferimenti Windows AMI AWS.

In genere Microsoft consiglia di effettuare la migrazione a una versione più recente di Windows Server invece dell'aggiornamento sul posto. La migrazione può comportare meno errori o problemi di aggiornamento, ma può impiegare più tempo rispetto a un aggiornamento in loco poiché occorre effettuare il provisioning di una nuova istanza, pianificare e trasferire le applicazioni e modificare le impostazioni di configurazione sulla nuova istanza. L'aggiornamento in loco può essere più rapido, ma le incompatibilità del software possono causare degli errori.

Indice

- Esegui un aggiornamento locale dell'istanza EC2 per Windows
- Usa i runbook di automazione per aggiornare un'istanza EC2 per Windows
- Esegui la migrazione di un'istanza EC2 per Windows a un tipo di istanza Nitro-based
- Risolvi i problemi relativi all'aggiornamento del sistema operativo su un'istanza EC2 per Windows

Esegui un aggiornamento locale dell'istanza EC2 per Windows

Prima di eseguire un aggiornamento in loco, devi stabilire quali driver di rete sono in esecuzione sull'istanza. I driver di rete PV ti consentono di accedere all'istanza tramite Desktop remoto. Le

istanze utilizzano i driver AWS PV, Intel Network Adapter o Enhanced Networking. Per ulteriori informazioni, consulta Driver paravirtuali per le istanze Windows.

Prima di avviare un aggiornamento in loco

Completa le attività seguenti e annota i dettagli importanti riportati di seguito prima di avviare l'aggiornamento in loco.

- Leggi la documentazione Microsoft per informazioni sui requisiti di aggiornamento, i problemi noti e le limitazioni. Rivedi inoltre le istruzioni ufficiali di aggiornamento.
  - Opzioni di aggiornamento per Windows Server 2012
  - Opzioni di aggiornamento per Windows Server 2012 R2
  - Opzioni di aggiornamento e conversione per Windows Server 2016 e successivi
  - Aggiornamenti di Windows Server
- Consigliamo di effettuare l'aggiornamento di un sistema operativo su istanze con almeno 2 vCPU e 4GB di RAM. Se necessario, è possibile modificare l'istanza in dimensioni più grandi dello stesso tipo (ad esempio da t2.small a t2.large), eseguire l'aggiornamento e ridimensionarla alle dimensioni originali. Se è necessario mantenere le dimensioni dell'istanza, è possibile monitorare il progresso utilizzando l'acquisizione di screenshot della console. Per ulteriori informazioni, consulta Modifiche del tipo di istanza Amazon EC2.
- Verifica che il volume root dell'istanza Windows disponga di sufficiente spazio libero sul disco. Il processo di Installazione di Windows potrebbe non inviare alcun avviso relativo allo spazio sul disco insufficiente. Per informazioni sulla quantità di spazio sul disco necessaria per aggiornare un sistema operativo specifico, consulta la documentazione Microsoft. Puoi espandere il volume se non è presente spazio sufficiente. Per ulteriori informazioni, consulta Volumi elastici Amazon EBS nella Guida per l'utente di Amazon EBS.
- Scegli il percorso di aggiornamento. È necessario aggiornare il sistema operativo alla stessa architettura. Ad esempio, devi aggiornare un sistema a 32-bit a un sistema a 32-bit. Windows Server 2008 R2 e versioni successive sono solo a 64 -bit.
- Disabilita i firewall e i software antivirus e anti-spyware. Questi tipi di software possono entrare in conflitto con il processo di aggiornamento. Re-enable software e firewall antivirus e antispyware al termine dell'aggiornamento.
- Aggiornamenti agli ultimi driver, come descritto in Esegui la migrazione di un'istanza EC2 per Windows a un tipo di istanza Nitro-based
- Il servizio dell'helper di aggiornamento supporta soltanto le istanze che eseguono i driver Citrix PV. Se l'istanza esegue i driver Red Hat, è necessario innanzitutto aggiornare tali driver manualmente.

Aggiorna un'istanza sul posto con AWS PV, Intel Network Adapter o i driver Enhanced Networking

Completa la procedura seguente per aggiornare un'istanza Windows Server con i driver di rete AWS PV, i driver della scheda di rete Intel o di Reti avanzate.

Per effettuare un aggiornamento in loco

1. Crea un'AMI del sistema che intendi aggiornare per scopi di backup o di testing. È quindi possibile effettuare l'aggiornamento sulla copia per simulare un ambiente di test. Se l'aggiornamento viene completato, è possibile modificare il traffico su questa istanza con un breve intervallo di inattività. Se l'aggiornamento non riesce, è possibile tornare al backup. Per ulteriori informazioni, consulta Crea un' EBS-backed AMI Amazon.
2. Assicurati che l'istanza Windows Server utilizzi i driver di rete più recenti.
    a. Per aggiornare il driver AWS PV, vedere. Aggiornamento dei driver PV sulle istanze Windows EC2
    b. Per aggiornare il driver ENA, consultaInstalla il driver ENA su istanze EC2 Windows.
    c. Per aggiornare i driver Intel, consulta Reti avanzate con l'interfaccia VF Intel 82599 sulle istanze
3. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
4. Nel riquadro di navigazione, seleziona Instances (Istanze). Individua l'istanza. Annota l'ID istanza e la zona di disponibilità dell'istanza. Queste informazioni saranno necessarie più avanti in questa procedura.
5. Se stai effettuando l'upgrade da Windows Server 2012 o 2012 R2 a Windows Server 2016 o successivi, completa la procedura seguente sull'istanza prima di continuare.
    a. Disinstalla il servizio EC2Config. Per ulteriori informazioni, consulta Amministrazione dei servizi Windows per gli agenti EC2Launch v2 ed EC2Config.
    b. Installare EC2Launch v1 o l'agente EC2Launch v2. Per ulteriori informazioni, vedere Utilizza l'agente EC2Launch v1 per eseguire attività durante l'avvio dell'istanza EC2 Windows eUtilizza l'agente EC2Launch v2 per eseguire attività durante l'avvio dell'istanza EC2 Windows.
    c. Installa l'agente AWS Systems Manager SSM. Per ulteriori informazioni, consulta Manually install SSM Agent on Amazon EC2 for Windows Server nella Guida per l'utente di AWS Systems Manager .

6. Crea un nuovo volume da uno snapshot dei supporti di installazione di Windows Server.

   a. Nel pannello di navigazione, in Elastic Block Store selezionare Snapshots (Snapshot).

   b. Nella barra del filtro, scegli Snapshot pubblici.

   c. Nella barra di ricerca, specifica i seguenti filtri:

      - Scegli Alias proprietario, quindi =, poi amazon.
      - Scegli Descrizione, quindi inizia a digitare **`Windows`**. Seleziona il filtro Windows corrispondente all'architettura del sistema e alla preferenza di lingua a cui stai effettuando l'aggiornamento. Ad esempio, scegli Supporto di installazione Windows 2019 in lingua inglese per effettuare l'aggiornamento a Windows Server 2019.

   d. Seleziona la casella di controllo accanto allo snapshot che corrisponde all'architettura di sistema e alla preferenza di lingua a cui stai eseguendo l'aggiornamento, quindi scegli Azioni, Crea volume da snapshot.

   e. Nella pagina Crea volume, scegli la zona di disponibilità corrispondente all'istanza Windows e seleziona Crea volume.

7. Nel *`1234567890example`* banner Volume creato con successo nella parte superiore della pagina, scegli l'ID del volume che hai appena creato.

8. Scegliere Actions (Operazioni), Attach Volume (Collega volume).

9. Nella pagina Allega volume, per Istanza ad esempio, seleziona l'ID dell'istanza della tua istanza di Windows, quindi scegli Allega volume.

10. Rendere disponibile il nuovo volume per l'utilizzo seguendo la procedura descritta in Rendere un volume Amazon EBS disponibile per l'uso.

    > **Important**
    >
    > Non inizializzare il disco perché in questo modo si eliminano i dati esistenti.

11. In Windows PowerShell, passa alla nuova unità di volume. Avviare l'aggiornamento per aprire il volume del supporto dell'installazione collegato all'istanza.

    a. Se si sta effettuando l'aggiornamento a Windows Server 2016 o a versioni più recenti, eseguire quanto riportato di seguito:

    ```
    .\setup.exe /auto upgrade /dynamicupdate disable
    ```

> **Note**
>
> L'esecuzione di setup.exe con l'opzione `/dynamicupdate` impostata su disabilitata impedisce a Windows di installare gli aggiornamenti durante il processo di upgrade di Windows Server, poiché l'installazione degli aggiornamenti durante l'upgrade può causare errori. È possibile installare gli aggiornamenti con Windows Update al termine dell'upgrade.

Se stai effettuando l'aggiornamento a una versione precedente di Windows Server, esegui quanto riportato di seguito:

```
Sources\setup.exe
```

b. In Select the operating system you want to install, seleziona l'opzione di installazione completa dell'istanza Windows Server e scegli Successivo.

c. In Which type of installation do you want? (Seleziona il tipo di installazione desiderato), scegli Upgrade (Aggiornamento).

d. Completa la procedura guidata.

L'installazione di Windows Server copia ed elabora i file. Dopo alcuni istanti, la sessione di Desktop remoto viene chiusa. Il tempo impiegato per l'aggiornamento dipende dal numero di applicazioni e ruoli del server in esecuzione sull'istanza Windows Server. Il processo di aggiornamento può impiegare da 40 minuti a diverse ore. Durante il processo di aggiornamento, l'istanza potrebbe non superare i controlli dello stato. Al termine dell'aggiornamento, tutti i controlli dello stato vengono superati. Puoi controllare nel log di sistema l'output della console o utilizzare le CloudWatch metriche di Amazon per l'attività del disco e della CPU per determinare se l'aggiornamento è in corso.

> **Note**
>
> In caso di aggiornamento a Windows Server 2019, al termine dell'operazione, se lo si desidera, è possibile modificare manualmente lo sfondo del desktop per rimuovere il nome del sistema operativo precedente.

Se l'istanza non ha superato tutti i controlli dello stato dopo diverse ore, consulta Risolvi i problemi relativi all'aggiornamento del sistema operativo su un'istanza EC2 per Windows.

Attività post-aggiornamento

1. Accedere all'istanza per avviare un aggiornamento di .NET Framework e riavviare il sistema quando richiesto.
2. Se non l'hai già fatto in un passaggio precedente, installa l'agente EC2Launch v1 o EC2Launch v2. Per ulteriori informazioni, consulta Utilizza l'agente EC2Launch v1 per eseguire attività durante l'avvio dell'istanza EC2 Windows e. Utilizza l'agente EC2Launch v2 per eseguire attività durante l'avvio dell'istanza EC2 Windows
3. Se hai eseguito l'aggiornamento a Windows Server 2012 R2, ti consigliamo di aggiornare i driver PV ai AWS driver PV. Se hai eseguito l'aggiornamento su un' Nitro-basedistanza, ti consigliamo di installare o aggiornare i driver NVME ed ENA. Per ulteriori informazioni, consulta Driver NVMe o Abilitazione delle reti avanzate su Windows.
4. Re-enable software e firewall antivirus e antispyware.

Usa i runbook di automazione per aggiornare un'istanza EC2 per Windows

È possibile eseguire un aggiornamento automatico delle istanze di Windows e SQL Server con i runbook di Automation. AWS AWS Systems Manager

Indice

- Servizi correlati
- Opzioni di esecuzione
- Aggiornamento di Windows Server
- Aggiornamento di SQL Server

Servizi correlati

Nel processo di aggiornamento automatico vengono utilizzati i seguenti AWS servizi:

- AWS Systems Manager. AWS Systems Manager è un'interfaccia potente e unificata per la gestione centralizzata delle AWS risorse. Per ulteriori informazioni, consulta la Guida per l'utente AWS Systems Manager.

- AWS Systems Manager L'agente (SSM Agent) è un software Amazon che può essere installato e configurato su un'istanza Amazon EC2, un server locale o una macchina virtuale (VM). SSM Agent consente a Systems Manager di aggiornare, gestire e configurare tali risorse. L'agente elabora le richieste dal servizio Systems Manager nel cloud AWS , quindi le esegue come specificato nella richiesta. Per ulteriori informazioni, consulta Utilizzo dell'SSM Agent nella Guida per l'utente di AWS Systems Manager Systems Manager.
- AWS Systems Manager Runbook SSM. Un runbook SSM definisce le operazioni eseguite da Systems Manager sulle istanze gestite. I runbook SSM utilizzano JavaScript Object Notation (JSON) o YAML e includono passaggi e parametri specificati dall'utente. Questo argomento prevede l'uso di due documenti SSM Systems Manager per l'automazione. Per ulteriori informazioni, consulta la Documentazione di riferimento del runbook di automazione di AWS Systems Manager nella Guida per l'utente di AWS Systems Manager .

Opzioni di esecuzione

Una volta selezionato Automation (Automazione) nella console di Systems Manager, selezionare Execute (Esegui). Dopo aver selezionato un documento di automazione, viene richiesto di scegliere un'opzione di esecuzione per l'automazione. Seleziona una delle opzioni seguenti. Nelle fasi per i percorsi forniti più avanti in questo argomento viene utilizzata l'opzione Simple execution (Esecuzione semplice).

Esecuzione semplice

Scegli questa opzione per aggiornare una singola istanza senza però esaminare ogni fase dell'automazione per verificare i risultati. Questa opzione è spiegata nei dettagli nelle fasi di aggiornamento descritte di seguito.

Rate control (Controllo velocità)

Scegli questa opzione per applicare l'aggiornamento a più di una istanza. Puoi definire le impostazioni seguenti.

- Parameter

  Questa impostazione, che è impostata anche nelle impostazioni della regione, definisce il modo in Multi-Account cui l'automazione si ramifica.
- Targets

Seleziona la destinazione in cui applicare l'automazione. Questa impostazione è impostata anche nelle Multi-Account impostazioni della regione.

- Parameter Values

  Utilizza i valori definiti nei parametri del documento di automazione.

- Resource Group

  In AWS, una risorsa è un'entità con cui puoi lavorare. Gli esempi includono istanze Amazon EC2, AWS CloudFormation stack o bucket Amazon S3. Se lavori con più risorse, potrebbe essere utile gestirle in gruppo anziché passare da un AWS servizio all'altro per ogni attività. In alcuni casi potresti voler gestire grandi quantità di risorse correlate, ad esempio delle istanze EC2 che formano un livello applicativo. In questo caso è probabile che sia necessario eseguire contemporaneamente azioni in blocco su queste risorse.

- Tag

  I tag consentono di classificare AWS le risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Questa categorizzazione è utile quando disponi di numerose risorse dello stesso tipo. Puoi così identificare velocemente una risorsa specifica in base ai tag a questa assegnati.

- Rate control

  Il controllo della frequenza è impostato anche nelle Multi-Account impostazioni della regione. Quando imposti i parametri di controllo della velocità, definisci in che misura applicare l'automazione al tuo parco istanze, come conteggio delle destinazioni o come percentuale del parco istanze.

Multi-Account e Regione

Oltre ai parametri specificati in Rate Control, utilizzati anche nelle impostazioni Multi-Account e Region, sono disponibili due impostazioni aggiuntive:

- Accounts and organizational units (OUs)

  Specifica più account su cui eseguire l'automazione.

- Regioni AWS

  Specifica più punti Regioni AWS in cui desideri eseguire l'automazione.

Esecuzione manuale

Simile a Simple execution (Esecuzione semplice), questa opzione consente di entrare in ciascuna fase dell'automazione per verificare i risultati.

Aggiornamento di Windows Server

Il runbook di `AWSEC2-CloneInstanceAndUpgradeWindows` crea un'Amazon Machine Image (AMI) da un'istanza Windows Server nel proprio account e aggiorna l'AMI a una versione supportata di propria scelta. Si tratta di una procedura in più fasi il cui completamento può richiedere fino a due ore.

Nella procedura di aggiornamento automatizzata sono incluse due AMI:

- Istanza attualmente in esecuzione. La prima AMI è l'istanza attualmente in esecuzione, che non è aggiornata. Questa AMI viene utilizzata per avviare un'altra istanza per eseguire l'aggiornamento locale. Una volta completato il processo, l'AMI viene eliminata dall'account, a meno che tu non richieda specificatamente di mantenere l'istanza originale. È un'impostazione gestita dal parametro `KeepPreUpgradeImageBackUp` (il cui valore predefinito è `false`, ovvero di default l'AMI viene rimossa).
- AMI aggiornata. Questa AMI è il risultato della procedura di automazione.

Il risultato finale è un'unica AMI, che è l'istanza aggiornata dell'AMI.

Una volta completato l'aggiornamento, è possibile testare la funzionalità dell'applicazione lanciando la nuova AMI nel Amazon VPC in uso. Al termine del test e prima di eseguire un altro aggiornamento, pianifica il tempo di inattività dell'applicazione prima di passare in modo definitivo all'istanza aggiornata.

Prerequisiti

Per automatizzare l'aggiornamento di Windows Server con il documento AWS Systems Manager Automation, è necessario eseguire le seguenti attività:

- Crea un ruolo IAM con le policy IAM specificate per consentire ad Systems Manager di eseguire le attività di automazione sulle istanze Amazon EC2 e verificare che siano soddisfatti i prerequisiti per utilizzare Systems Manager. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un AWS servizio nella Guida per l'AWS Identity and Access Management utente.

- Seleziona l'opzione per la modalità di esecuzione dell'automazione. Le opzioni di esecuzione sono Esecuzione semplice, Rate control , Region Multi-account e Manual execution. Per ulteriori informazioni su queste opzioni, consulta Opzioni di esecuzione.
- Verificare che SSM Agent sia installato nell'istanza. Per ulteriori informazioni, consulta Installazione e configurazione del SSM Agent sulle istanze Amazon EC2 per Windows Server.
- Windows PowerShell 3.0 o versioni successive deve essere installato sull'istanza.
- Per le istanze che vengono aggiunte a un dominio Microsoft Active Directory, si consiglia di specificare un `SubnetId` che non dispone di connettività ai controller di dominio per evitare conflitti di nomi host.
- La sottorete dell'istanza deve disporre di una connettività in uscita a Internet, che fornisce l'accesso, Servizi AWS ad esempio, ad Amazon S3 e l'accesso al download di patch da Microsoft. Questo requisito è soddisfatto se la sottorete è una sottorete pubblica e l'istanza ha un indirizzo IP pubblico o se la sottorete è una sottorete privata con un percorso che invia il traffico Internet a un dispositivo NAT pubblico.
- Questa automazione funziona con istanze in esecuzione su Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 e Windows Server 2019
- Verificare che l'istanza disponga di 20 GB di spazio sul disco di avvio.
- Se l'istanza non utilizza una licenza Windows fornita da AWS, specifica un ID snapshot di Amazon EBS che includa il supporto di installazione di Windows Server 2012 R2. Per farlo:
  1. Verificare che l'istanza Amazon EC2 esegua Windows Server 2012 o versioni successive.
  2. Creare un volume Amazon EBS da 6 GB nella stessa zona di disponibilità in cui l'istanza è in esecuzione. Collegare il volume all'istanza. Montare il volume, ad esempio come unità D.
  3. Apri il menu contestuale (clic con il pulsante destro del mouse) per l'ISO e montalo su un'istanza come, ad esempio, l'unità E.
  4. Copiare il contenuto dell'oggetto ISO dall'unità E:\ all'unità D:\
  5. Creare uno snapshot Amazon EBS del volume da 6 GB creato nella precedente fase 2.

Limitazioni dell'aggiornamento per Windows Server

Questa automazione non supporta l'aggiornamento di controller di dominio Windows, cluster o sistemi operativi per desktop Windows. Questa automazione, inoltre, non supporta le istanze Amazon EC2 per Windows Server con i seguenti ruoli installati:

- Remote Desktop Session Host (RDSH)

- Remote Desktop Connection Broker (RDCB)
- Remote Desktop Virtualization Host (RDVH)
- Remote Desktop Web Access (RDWA)

Procedura per eseguire un aggiornamento automatico di Windows Server

Segui questi passaggi per aggiornare l'istanza di Windows Server utilizzando il runbook di AWSEC2-CloneInstanceAndUpgradeWindows automazione.

1. Aprire Systems Manager dalla Console di gestione AWS .
2. Nel riquadro di navigazione a sinistra, in Change Management (Gestione delle modifiche), scegliere Automation (Automazione).
3. Selezionare Execute automation (Esegui automazione).
4. Cercare il documento di automazione denominato `AWSEC2-CloneInstanceAndUpgradeWindows`.
5. Quando compare il nome del documento, selezionarlo. Una volta selezionato, vengono visualizzati i dettagli del documento.
6. Scegliere Execute automation (Esegui automazione) per inserire i parametri per questo documento. Lasciare selezionato Simple execution (Esecuzione semplice) in alto nella pagina.
7. Immettere i parametri richiesti in base alle indicazioni seguenti.

   - `InstanceID`

     Tipo: stringa

     (Obbligatorio) L'istanza che esegue Windows Server 2008 R2, 2012 R2, 2016 o 2019 con l'agente SSM installato.

   - `InstanceProfile`.

     Tipo: stringa

     (Obbligatorio) Il profilo dell'istanza IAM. Questo è il ruolo IAM utilizzato per eseguire l'automazione di Systems Manager rispetto all'istanza Amazon EC2 e AWS alle AMI. Per ulteriori informazioni, consulta Configure EC2 instance permissions nella Guida per l'utente di AWS Systems Manager .

   - `TargetWindowsVersion`

Tipo: stringa

(Obbligatorio) Selezionare la versione di Windows di destinazione.

- `SubnetId`

  Tipo: stringa

  (Obbligatorio) La sottorete per la procedura di aggiornamento, in cui risiede l'istanza EC2. Verifica che la sottorete disponga di connettività in uscita ai AWS servizi, incluso Amazon S3, e anche a Microsoft (per scaricare le patch).

- `KeepPreUpgradedBackUp`

  Tipo: stringa

  (Facoltativo) Se questo parametro è impostato su `true`, l'automazione mantiene l'immagine creata dall'istanza. L'impostazione predefinita è `false`.

- `RebootInstanceBeforeTakingImage`

  Tipo: stringa

  (Facoltativo) L'impostazione predefinita è `false` (nessun riavvio). Se questo parametro è impostato su `true`, Systems Manager riavvia l'istanza prima di creare un'AMI per l'aggiornamento.

8. Dopo avere immesso i parametri, selezionare Execute (Esegui). Una volta avviata l'automazione, è possibile monitorare l'avanzamento dell'esecuzione.
9. Terminata l'automazione, sarà visualizzato l'ID dell'AMI. È possibile avviare l'AMI per verificare l'aggiornamento del sistema operativo Windows.

> **Note**
>
> L'automazione non deve necessariamente eseguire tutte le fasi. Le fasi dipendono dal comportamento dell'automazione e dell'istanza. Systems Manager potrebbe ignorare alcuni passaggi non richiesti.
> Inoltre, alcune fasi potrebbero scadere. Systems Manager tenta di aggiornare e installare tutte le patch più recenti. A volte, tuttavia, si verificano timeout in funzione di un'impostazione di timeout definibile per una determinata fase. In questi casi, il servizio di automazione di Systems Manager continua con la fase successiva per garantire

che il sistema operativo interno venga aggiornato alla versione Windows Server di destinazione.

10. Una volta completata l'automazione, è possibile avviare un'istanza Amazon EC2 tramite l'ID dell'AMI per verificare l'aggiornamento. Per ulteriori informazioni su come creare un'istanza Amazon EC2 da un' AWS AMI, vedi Come si avvia un'istanza EC2 da un'AMI personalizzata?

Aggiornamento di SQL Server

Lo script AWSEC2-CloneInstanceAndUpgradeSQLServer crea un'AMI da un'istanza Amazon EC2 con SQL Server in esecuzione nell'account, quindi aggiorna l'AMI a una versione più recente di SQL Server. Si tratta di una procedura in più fasi il cui completamento può richiedere fino a due ore.

In questo flusso di lavoro, l'automazione crea un'AMI dall'istanza e quindi avvia la nuova AMI creata nella sottorete specificata. L'automazione esegue quindi un aggiornamento locale di SQL Server. Una volta completato l'aggiornamento, l'automazione crea una nuova AMI prima di terminare l'istanza aggiornata.

Nella procedura di aggiornamento automatizzata sono incluse due AMI:

- Istanza attualmente in esecuzione. La prima AMI è l'istanza attualmente in esecuzione, che non è aggiornata. Questa AMI viene utilizzata per avviare un'altra istanza per eseguire l'aggiornamento locale. Una volta completato il processo, l'AMI viene eliminata dall'account, a meno che tu non richieda specificatamente di mantenere l'istanza originale. È un'impostazione gestita dal parametro `KeepPreUpgradeImageBackUp` (il cui valore predefinito è `false`, ovvero di default l'AMI viene rimossa).
- AMI aggiornata. Questa AMI è il risultato della procedura di automazione.

Il risultato finale è un'unica AMI, che è l'istanza aggiornata dell'AMI.

Una volta completato l'aggiornamento, è possibile testare la funzionalità dell'applicazione lanciando la nuova AMI nel Amazon VPC in uso. Al termine del test e prima di eseguire un altro aggiornamento, pianifica il tempo di inattività dell'applicazione prima di passare in modo definitivo all'istanza aggiornata.

Prerequisiti

Per automatizzare l'aggiornamento di SQL Server con il documento AWS Systems Manager Automation, è necessario eseguire le seguenti attività:

- Crea un ruolo IAM con le policy IAM specificate per consentire ad Systems Manager di eseguire le attività di automazione sulle istanze Amazon EC2 e verificare che siano soddisfatti i prerequisiti per utilizzare Systems Manager. Per ulteriori informazioni, consulta la pagina relativa alla creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di AWS Identity and Access Management .
- Seleziona l'opzione per la modalità di esecuzione dell'automazione. Le opzioni di esecuzione sono Esecuzione semplice, Controllo della frequenza , Regione Multi-account ed Esecuzione manuale. Per ulteriori informazioni su queste opzioni, consulta Opzioni di esecuzione.
- L'istanza Amazon EC2 deve utilizzare una versione uguale o successiva a di Windows Server 2008 R2 e SQL Server 2008 (o versione successiva).
- Verificare che SSM Agent sia installato nell'istanza. Per ulteriori informazioni, consulta Installazione e configurazione di SSM Agent sulle istanze Amazon EC2 per Windows Server.
- Verificare che l'istanza disponga di sufficiente spazio libero sul disco:
  - Se si esegue l'aggiornamento da Windows Server 2008 R2 a 2012 R2, oppure da Windows Server 2012 R2 a un sistema operativo successivo, verificare di disporre di 20 GB di spazio libero sul disco di avvio dell'istanza.
  - Se si esegue l'aggiornamento da Windows Server 2008 R2 a 2016 o successivo, verificare che l'istanza disponga di 40 GB di spazio libero sul disco di avvio dell'istanza.
- Per istanze che utilizzano una versione Bring-Your-Own-License (uso di licenze proprie) di SQL Server, si applicano i seguenti prerequisiti aggiuntivi:
  - Specificare un ID snapshot Amazon EBS contenente il supporto di installazione di SQL Server. Per farlo:
    1. Verificare che l'istanza Amazon EC2 esegua Windows Server 2008 R2 o versioni successive.
    2. Creare un volume Amazon EBS da 6 GB nella stessa zona di disponibilità in cui l'istanza è in esecuzione. Collegare il volume all'istanza. Montare il volume, ad esempio come unità D.
    3. Aprite il menu contestuale (clic con il pulsante destro del mouse) per l'ISO e montatelo su un'istanza come, ad esempio, l'unità E.
    4. Copiare il contenuto dell'oggetto ISO dall'unità E:\ all'unità D:\
    5. Creare uno snapshot Amazon EBS del volume da 6 GB creato nella fase 2.

Limitazioni dell'aggiornamento automatico per SQL Server

Le seguenti limitazioni si applicano quando si utilizza il AWSEC2-CloneInstanceAndUpgradeSQLServer runbook per eseguire un aggiornamento automatico:

- L'aggiornamento può essere eseguito solo su un'istanza SQL Server che usa l'autenticazione di Windows.
- Verificare che sulle istanze non siano presenti aggiornamenti delle patch di sicurezza in sospeso. Aprire Control Panel (Pannello di controllo), quindi scegliere Check for updates (Verifica disponibilità aggiornamenti).
- Le distribuzioni di SQL Server in modalità HA (High Availability, disponibilità elevata) e mirroring non sono supportate.

Procedura per eseguire un aggiornamento automatico di SQL Server

Segui questi passaggi per aggiornare SQL Server utilizzando il runbook di AWSEC2-CloneInstanceAndUpgradeSQLServer automazione.

1. Se non è già stato fatto, scaricare il file .iso di SQL Server 2016 e montarlo sul server di origine.
2. Una volta completato questo passaggio, copiare tutti i file dei componenti e posizionarli in un volume a scelta.
3. Eseguire uno snapshot Amazon EBS del volume e copiare l'ID snapshot negli appunti per usarlo in un secondo momento. Per ulteriori informazioni, consulta Crea snapshot Amazon EBS nella Guida per l'utente di Amazon EBS.
4. Collegare il profilo dell'istanza all'istanza Amazon EC2 di origine. Ciò consente a Systems Manager di comunicare con l'istanza EC2 ed eseguire comandi su di essa dopo che è stata aggiunta al AWS Systems Manager servizio. Per questo esempio, il ruolo è stato denominato `SSM-EC2-Profile-Role` con la policy `AmazonSSMManagedInstanceCore` collegata al ruolo stesso.
5. Nella AWS Systems Manager console, nel riquadro di navigazione a sinistra, scegli Istanze gestite. Verificare che l'istanza EC2 sia presente nell'elenco delle istanze gestite. Se l'istanza non viene visualizzata dopo qualche secondo, consulta Dove sono le mie istanze? nella Guida per l'utente di AWS Systems Manager .
6. Nel riquadro di navigazione a sinistra, sottoGestione delle modifichescegliereAutomazione.
7. Selezionare Execute automation (Esegui automazione).
8. Cercare il documento di automazione denominato `AWSEC2-CloneInstanceAndUpgradeSQLServer`.
9. Scegliere il documento SSM `AWSEC2-CloneInstanceAndUpgradeSQLServer`, quindi scegliere Next (Successivo).
10. Assicurarsi che sia selezionata l'opzione Simple execution (Esecuzione semplice).

11. Immettere i parametri richiesti in base alle indicazioni seguenti.

    - `InstanceId`

      Tipo: stringa

      (Obbligatorio) L'istanza su cui è in esecuzione SQL Server 2008 R2 (o versioni successive).

    - `IamInstanceProfile`

      Tipo: stringa

      (Obbligatorio) Il profilo dell'istanza IAM.

    - `SQLServerSnapshotId`

      Tipo: stringa

      (Obbligatorio) L'ID snapshot del supporto di installazione di SQL Server. Questo parametro non è richiesto per le istanze di SQL Server. incluse in licenza

    - `SubnetId`

      Tipo: stringa

      (Obbligatorio) La sottorete per la procedura di aggiornamento, in cui risiede l'istanza EC2. Verifica che la sottorete sia connessa in uscita ai AWS servizi, incluso Amazon S3, e anche a Microsoft (per scaricare le patch).

    - `KeepPreUpgradedBackUp`

      Tipo: stringa

      (Facoltativo) Se questo parametro è impostato su `true`, l'automazione mantiene l'immagine creata dall'istanza. L'impostazione predefinita è `false`.

    - `RebootInstanceBeforeTakingImage`

      Tipo: stringa

      (Facoltativo) L'impostazione predefinita è `false` (nessun riavvio). Se questo parametro è impostato su `true`, Systems Manager riavvia l'istanza prima di creare un'AMI per l'aggiornamento.

    - `TargetSQLVersion`

- Tipo: stringa

(Facoltativo) La versione di SQL Server di destinazione. Il valore predefinito è `2016`.

12. Dopo avere immesso i parametri, selezionare Execute (Esegui). Una volta avviata l'automazione, è possibile monitorare l'avanzamento dell'esecuzione.
13. Quando Execution status (Stato esecuzione) indica Riuscito, espandere Outputs (Output) per visualizzare le informazioni sull'AMI. È possibile utilizzare l'ID AMI per avviare l'istanza SQL Server nel VPC preferito.
14. Aprire la console Amazon EC2. Nel riquadro di navigazione a sinistra scegliere AMIs (AMI). Verrà visualizzata la nuova AMI.
15. Per verificare la corretta installazione di SQL Server, scegliere la nuova AMI, quindi Launch (Avvia).
16. Scegliere il tipo di istanza desiderata per l'AMI, il VPC e la sottorete in cui distribuirla e l'archiviazione da utilizzare. Poiché l'avvio della nuova istanza avviene da un'AMI, i volumi sono presentati come un'opzione da includere nell'istanza EC2 da avviare. È possibile rimuovere tali volumi o aggiungerne altri.
17. Aggiungere un tag per facilitare l'identificazione dell'istanza.
18. Aggiungere all'istanza il gruppo o i gruppi di sicurezza.
19. Scegliere Launch Instance (Avvia istanza).
20. Scegliere il nome del tag per l'istanza e selezionare Connect (Connetti) nel menu a discesa Actions (Operazioni).
21. Verificare che la versione di SQL Server sia il nuovo motore di database sulla nuova istanza.

Esegui la migrazione di un'istanza EC2 per Windows a un tipo di istanza Nitro-based

Le AMI AWS Windows sono configurate con le impostazioni predefinite utilizzate dal supporto di installazione Microsoft, con alcune personalizzazioni. Le personalizzazioni includono driver e configurazioni che supportano Nitro-based istanze, come M5 e C5.

Durante la migrazione da Xen-based istanze a istanze, incluse Nitro-based le istanze bare metal, ti consigliamo di seguire i passaggi descritti in questo argomento nei seguenti casi:

- Se si stanno avviando istanze dalle AMI di Windows personalizzate

- Se si stanno avviando istanze dalle AMI di Windows fornite da Amazon create prima di agosto 2018

In alternativa, puoi utilizzare il documento di automazione `AWSSupport-UpgradeWindowsAWSDrivers` per automatizzare le procedure descritte nelle parti 1, 2 e 3. Se scegli di utilizzare la procedura automatizzata, vedi (Alternativa) Aggiornare il AWS Driver PV, ENA e NVMe che utilizzano AWS Systems Manager, quindi continua con le parti 4 e 5.

Per ulteriori informazioni, consulta Aggiornamento di Amazon EC2: altri tipi di istanza, sistema Nitro e opzioni CPU.

> **Note**
>
> Le procedure di migrazione seguenti possono essere eseguite in Windows Server 2016 e versioni successive. Le versioni precedenti del sistema operativo che hanno raggiunto la fine del ciclo di vita non vengono testate e potrebbero non essere compatibili con i tipi di istanze più recenti.
> Per migrare le istanze Linux, consulta the section called "Modifiche del tipo di istanza".

Indice

- Parte 1: installazione e aggiornamento AWS Driver PV
- Parte 2: installare e aggiornare ENA
- Parte 3: aggiornamento AWS Driver NVMe
- Parte 4: aggiornare EC2Config ed EC2Launch
- Parte 5: installare il driver di porta seriale per le istanze bare metal
- Parte 6: aggiornare le impostazioni di risparmio energia
- Parte 7: aggiornare i driver Intel Chipset per nuovi tipi di istanza
- (Alternativa) Aggiornare il AWS Driver PV, ENA e NVMe che utilizzano AWS Systems Manager

Prima di iniziare

Questa procedura presuppone che tu disponga di un'Xen-based istanza, ad esempio M4 o C4, e che tu stia migrando a un'istanza. Nitro-based

È necessario utilizzare la PowerShell versione 3.0 o successiva per eseguire correttamente l'aggiornamento.

> **Note**
>
> Durante la migrazione, le configurazioni di rete DNS personalizzate o l'IP statico sulla carta di interfaccia di rete esistente potrebbero andare perse, poiché l'istanza passerà in modo predefinito a un nuovo dispositivo Enhanced Networking Adapter.

Prima di seguire la procedura della guida, si consiglia di creare un backup dell'istanza. Dalla console EC2 scegli l'istanza che deve effettuare la migrazione, apri il menu contestuale (pulsante destro del mouse) e seleziona Instance State (Stato istanza), quindi Stop (Arresta).

> **Warning**
>
> Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per conservare i dati nei volumi di archivio istanza, eseguire il backup di tutti i dati dei volumi in un'archiviazione persistente.

Apri il menu contestuale (pulsante destro del mouse) dell'istanza nella console EC2, scegli Image (Immagine), quindi Create Image (Crea immagine).

> **Note**
>
> Le parti 4 e 5 delle presenti istruzioni possono essere completate dopo che il tipo di istanza migra o cambia tipo di istanza. Tuttavia, ti consigliamo di completarle prima della migrazione, soprattutto se questa avviene verso un tipo di istanza Bare Metal.

Parte 1: installazione e aggiornamento AWS Driver PV

Sebbene i driver AWS PV non siano utilizzati nel sistema Nitro, dovreste comunque aggiornarli se utilizzate versioni precedenti di Citrix PV o PV. AWS I driver AWS fotovoltaici più recenti risolvono i bug delle versioni precedenti dei driver che possono comparire mentre si utilizza un sistema Nitro o se è necessario migrare nuovamente a un'istanza. Xen-based Come procedura consigliata, consigliamo di eseguire sempre l'aggiornamento ai driver più recenti per le istanze Windows in uso. AWS

Utilizzate la seguente procedura per eseguire un aggiornamento sul posto dei driver AWS PV o per eseguire l'aggiornamento dai driver Citrix PV ai driver AWS PV su Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 o Windows Server 2019. Per ulteriori informazioni, consulta Aggiornamento dei driver PV sulle istanze Windows EC2.

Per aggiornare un controller di dominio, consulta Aggiornare un controller di dominio (AWS Aggiornamento PV)

Per eseguire un aggiornamento di o a AWS Driver PV

1. Connettiti all'istanza utilizzando Desktop remoto e prepara l'istanza per l'aggiornamento. Disconnetti tutti i dischi non del sistema prima di eseguire l'aggiornamento. Se si esegue un aggiornamento sul posto dei driver AWS fotovoltaici, questo passaggio non è necessario. Imposta i servizi non essenziali sull'avvio Manual (Manuale) nella console Servizi.
2. Scarica il pacchetto di driver più recente per l'istanza.
3. Estrai i contenuti della cartella ed esegui `AWSPVDriverSetup.msi`.

Dopo avere eseguito l'MSI, l'istanza si riavvia automaticamente e aggiorna il driver. L'istanza potrebbe non essere disponibile per un massimo di 15 minuti.

Una volta completato l'aggiornamento e dopo che l'istanza ha superato entrambi i controlli dello stato nella console Amazon EC2, connettiti all'istanza utilizzando Desktop remoto e verifica che il nuovo driver sia installato. In Gestione dispositivi, in Controller di storage, individua AWS Scheda host storage PV. Verifica che la versione del driver sia la stessa dell'ultima versione elencata nella tabella della cronologia delle versioni dei driver. Per ulteriori informazioni, consulta AWS Cronologia dei pacchetti driver PV.

Parte 2: installare e aggiornare ENA

Effettua l'aggiornamento al driver Elastic Network Adapter più recente per garantire che siano supportate tutte le funzionalità di rete. Se è stata avviata l'istanza ma la funzionalità di reti avanzate non è già abilitata, è necessario scaricare e installare il driver per la scheda di rete richiesto sull'istanza. Quindi imposta l'attributo di istanza enaSupport per attivare le reti avanzate. Puoi abilitare questo attributo solo sui tipi di istanza supportati e solo se il driver ENA è installato. Per ulteriori informazioni, consulta Abilitazione delle reti avanzate con ENA su istanze EC2.

1. Scarica il driver più recente per l'istanza. Se è necessaria una versione precedente del driver, consulta Cronologia della versione del driver ENA Windows.

2. Estrai l'archivio .zip.
3. Installa il driver eseguendo lo `install.ps1` PowerShell script dalla cartella estratta.

> **Note**
>
> Per evitare errori di installazione, esegui lo script `install.ps1` come amministratore.

4. Verifica che enaSupport sia attivato per l'AMI. In caso contrario, prosegui seguendo la documentazione in Abilitazione delle reti avanzate con ENA su istanze EC2.

Parte 3: aggiornamento AWS Driver NVMe

AWS I driver NVMe vengono utilizzati per interagire con i volumi di storage di istanze Amazon EBS e SSD esposti come dispositivi a blocchi NVMe nel sistema Nitro per prestazioni migliori.

> **Important**
>
> Le seguenti istruzioni vengono modificate specificamente per l'installazione o l'aggiornamento di AWS NVMe su un' Xen-based istanza con l'intenzione di migrare l'istanza su un'istanza. Nitro-based

1. Scarica il pacchetto di driver più recente per l'istanza.

   Se è necessaria una versione precedente del driver, consulta AWS Rilasci dei driver NVMe per Windows per le versioni supportate.
2. Estrai l'archivio .zip.
3. Installare il driver come descritto in `Readme.txt`.
4. Aprire una PowerShell sessione ed eseguire il comando seguente:

```
PS C:\> start rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
```

> **Note**
>
> Per applicare il comando, è necessario eseguire la PowerShell sessione come amministratore. PowerShell le versioni (x86) genereranno un errore.

Questo comando esegue sysprep solo sui driver dei dispositivi. Non esegue la preparazione completa di sysprep.

5. Per Windows Server 2008 R2 e Windows Server 2012, arrestare l'istanza, modificare il tipo di istanza e avviarla, quindi continuare con la Parte 4. Se si riavvia l'istanza su un tipo di Xen-based istanza prima di migrare a un tipo di Nitro-based istanza, non verrà avviata. Per le altre AMI Windows supportate, è possibile modificare il tipo di istanza in qualsiasi momento dopo il sysprep del dispositivo.

Parte 4: aggiornare EC2Config ed EC2Launch

Per le istanze Windows, le ultime utilità EC2Config ed EC2Launch forniscono funzionalità e informazioni aggiuntive, se eseguite sul sistema Nitro, incluso Bare Metal EC2. Per impostazione predefinita, il servizio EC2Config è incluso nelle AMI da prima di Windows Server 2016. EC2Launch sostituisce il servizio EC2Config sulle AMI di Windows Server 2016 o versione successiva.

Quando i servizi EC2Config ed EC2Launch vengono aggiornati, le nuove AMI di Windows da AWS includono la versione più recente del servizio. Tuttavia, è necessario aggiornare le AMI di Windows e le istanze con la versione più recente di EC2Config e di EC2Launch.

Per installare o aggiornare EC2Config

1. Scarica e decomprimi il programma di installazione di EC2Config.
2. Esegui `EC2Install.exe`. Per un elenco completo delle opzioni, esegui `EC2Install` con l'opzione `/?`. Per impostazione predefinita, la configurazione mostra i prompt. Per eseguire il comando senza alcun prompt, utilizza l'opzione `/quiet`.

Per ulteriori informazioni, consulta Installazione della versione più recente di EC2Config.

Per installare o aggiornare EC2Launch

1. Se EC2Launch è già stato installato e configurato su un'istanza, eseguire un backup del file di configurazione di EC2Launch. Il processo di installazione non conserva le modifiche apportate a questo file. Per impostazione predefinita, il file si trova nella directory `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. EC2-Windows-Launch.zipEffettua il download in una directory sull'istanza.
3. Scaricare install.ps1 nella stessa directory in cui è stato scaricato `EC2-Windows-Launch.zip`.

4. Esegui `install.ps1`.

> **Note**
>
> Per evitare errori di installazione, esegui lo script `install.ps1` come amministratore.

5. Se è stato eseguito il backup del file di configurazione di EC2Launch, copiarlo nella directory `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Per ulteriori informazioni, consulta Utilizza l'agente EC2Launch v1 per eseguire attività durante l'avvio dell'istanza EC2 Windows.

Parte 5: installare il driver di porta seriale per le istanze bare metal

Il tipo di `i3.metal` istanza utilizza un dispositivo PCI-based seriale anziché un dispositivo seriale I/O basato su porte. Le AMI Windows più recenti utilizzano automaticamente il dispositivo PCI-based seriale e hanno installato il driver della porta seriale. Se non si utilizza un'istanza avviata da un'AMI Amazon-provided Windows datata 2018.04.11 o successiva, è necessario installare il Serial Port Driver per abilitare il dispositivo seriale per le funzionalità EC2 come la generazione di password e l'output della console. Le ultime utilità EC2Config ed EC2Launch supportano anche i3.metal e forniscono funzionalità aggiuntive, pertanto segui i passaggi della parte 4, se non l'hai ancora fatto.

Per installare il driver di porta seriale

1. Scarica il pacchetto di driver seriale per l'istanza.
2. Estrai il contenuto della cartella, apri il menu contestuale (pulsante destro del mouse) per `aws_ser.INF` e seleziona Install (Installa).
3. Seleziona Okay.

Parte 6: aggiornare le impostazioni di risparmio energia

Il seguente aggiornamento alle impostazioni di Power Management imposta lo spegnimento del display su mai, per consentire arresti regolari del sistema operativo sul sistema Nitro. Tutte le AMI Windows fornite da Amazon al 28.11. 2018 hanno già questa configurazione predefinita.

1. Aprire un prompt dei comandi o una sessione. PowerShell
2. Esegui i comandi seguenti:

```
powercfg /setacvalueindex 381b4222-f694-41f0-9685-ff5bb260df2e 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex a1841308-3541-4fab-bc81-f71556f20b4a 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
```

Parte 7: aggiornare i driver Intel Chipset per nuovi tipi di istanza

I tipi di istanza `u-6tb1.metal`, `u-9tb1.metal` e `u-12tb1.metal` utilizzano l'hardware che richiede i driver chipset precedentemente installati sulle AMI di Windows. Se non si utilizza un'istanza avviata da un'AMI Amazon-provided Windows datata 2018.11.19 o successiva, è necessario installare i driver utilizzando la Intel Chipset INF Utility.

Per installare i driver chipset

1. Utilità INF chipset nell'istanza.
2. Estrai i file.
3. Esegui `SetupChipset.exe`.
4. Accetta l'accordo di licenza del software Intel e installa i driver chipset.
5. Riavviare l'istanza.

(Alternativa) Aggiornare il AWS Driver PV, ENA e NVMe che utilizzano AWS Systems Manager

Il documento di automazione `AWSSupport-UpgradeWindowsAWSDrivers` automatizza le fasi descritte in Parte 1, Parte 2 e Parte 3. Questo metodo può anche riparare un'istanza in cui non è stato possibile eseguire gli aggiornamenti dei driver.

Il documento di `AWSSupport-UpgradeWindowsAWSDrivers` automazione aggiorna o ripara i AWS driver di storage e di rete sull'istanza EC2 specificata. Il documento tenta di installare le versioni più recenti dei AWS driver online chiamando l' AWS Systems Manager agente (agente SSM). Se SSM Agent non è contattabile, il documento può eseguire un'installazione offline dei AWS driver se richiesto esplicitamente.

> **Note**
>
> Questa procedura non andrà a buon fine su un controller di dominio. Per aggiornare i driver su un controller di dominio, consulta Aggiornare un controller di dominio (AWS Aggiornamento PV).

Per aggiornare automaticamente AWS Driver PV, ENA e NVMe che utilizzano AWS Systems Manager

1. Aprire la console di Systems Manager all'indirizzo. https://console.aws.amazon.com/systems-manager
2. Seleziona Automation (Automazione), Execute Automation (Esecuzione automazione).
3. Cerca e seleziona il documento di AWSSupport-UpgradeWindowsAWSDrivers automazione, quindi scegli Esegui automazione.
4. Nella sezione Parametri di input, configura le seguenti opzioni:

   ID istanza

   Immetti l'ID univoco dell'istanza da aggiornare.

   AllowOffline

   (Facoltativo) Seleziona una delle seguenti tre opzioni:

   - `True` — Scegli questa opzione per eseguire l'installazione offline. Durante il processo di aggiornamento, l'istanza viene arrestata e riavviata.

     > **Warning**
     >
     > Quando interrompi un'istanza, i dati presenti sui volumi dell'instance store vengono cancellati. Per conservare i dati nei volumi di instance store, esegui il backup di tutti i dati dei volumi in uno storage persistente.

   - `False` — (Predefinito) Lascia questa opzione selezionata per eseguire l'installazione online. Durante il processo di aggiornamento, l'istanza viene riavviata.

> **Important**
>
> Gli aggiornamenti online e offline creano un'AMI prima di provare le operazioni di aggiornamento. L'AMI persiste dopo il completamento dell'automazione. Proteggi l'accesso all'AMI o eliminarla, se non è più necessaria.

SubnetId

(Facoltativo) Immetti uno dei seguenti valori:

- `SelectedInstanceSubnet` — (Predefinito) Il processo di aggiornamento avvia l'istanza helper nella stessa sottorete dell'istanza da aggiornare. La sottorete deve consentire la comunicazione verso gli endpoint Systems Manager (`ssm.*`).
- `CreateNewVPC` — Il processo di aggiornamento avvia l'istanza helper in un nuovo VPC. Utilizza questa opzione se non sei sicuro che la sottorete dell'istanza di destinazione consenta la comunicazione verso gli endpoint `ssm.*`. L'utente deve disporre delle autorizzazioni per creare un VPC.
- ID di una sottorete specifica — Specificare l'ID di una sottorete specifica in cui avviare l'istanza helper. La sottorete deve trovarsi nella stessa zona di disponibilità dell'istanza da aggiornare e deve consentire la comunicazione con gli endpoint `ssm.*`.

5. Scegli Esegui.
6. Consenti il completamento dell'aggiornamento. Per completare un aggiornamento online possono essere necessari fino a 10 minuti, mentre per quello offline fino a 25 minuti.

Risolvi i problemi relativi all'aggiornamento del sistema operativo su un'istanza EC2 per Windows

AWS fornisce supporto per l'aggiornamento per problemi o problemi con l'Upgrade Helper Service, un' AWS utilità che consente di eseguire aggiornamenti sul posto che coinvolgono i driver Citrix PV.

In seguito all'aggiornamento, durante l'ottimizzazione di .NET Framework da parte del servizio di ottimizzazione di runtime .NET, sull'istanza potrebbe verificarsi un utilizzo della CPU temporaneamente superiore alla media. Questo è il comportamento previsto.

Se l'istanza non ha superato tutti i controlli dello stato dopo diverse ore, consulta quanto segue.

- Se hai effettuato l'aggiornamento a Windows Server 2008 e tutti i controlli dello stato non riescono dopo diverse ore, l'aggiornamento potrebbe non essere riuscito con la visualizzazione del prompt Fare clic su OK per confermare il rollback. Dal momento che la console non è accessibile in questa fase, non è possibile fare clic sul pulsante in alcun modo. Per ovviare a questo problema, esegui un riavvio tramite la console o l'API di Amazon EC2. Per l'inizializzazione del riavvio sono necessari almeno dieci minuti. L'istanza potrebbe diventare disponibile dopo 25 minuti.
- Rimuovi le applicazioni o i ruoli del server dal server e riprova.

Se l'istanza non supera tutti i controlli dello stato dopo la rimozione delle applicazioni o dei ruoli del server dal server, procedi come segue.

- Arresta l'istanza e collega il volume root a un'altra istanza. Per ulteriori informazioni, consulta la descrizione di come arrestare e collegare il volume root a un'altra istanza in "In attesa del servizio di metadati".
- Analizza i file e di log e i log degli eventi di Installazione Windows per verificare la presenza di errori.

Per altri problemi relativi alla migrazione o all'aggiornamento di un sistema operativo, ti consigliamo di consultare gli articoli in Prima di avviare un aggiornamento in loco.

Tutorial: Connessione di un'istanza Amazon EC2 a un database Amazon RDS

Obiettivo del tutorial

L'obiettivo di questo tutorial è imparare a configurare una connessione sicura tra un'istanza Amazon EC2 e un database Amazon RDS utilizzando Console di gestione AWS.

Ci sono diverse opzioni per configurare la connessione. In questo tutorial esploriamo queste tre:

- Opzione 1: connessione automatica dell'istanza al database RDS tramite la console EC2

  Usa la funzione di connessione automatica nella console EC2 per configurare automaticamente la connessione tra l'istanza EC2 e il database RDS così da consentire il traffico tra l'istanza EC2 e il database RDS.
- Opzione 2: connessione automatica dell'istanza al database RDS tramite la console RDS

Usa la funzione di connessione automatica nella console RDS per configurare automaticamente la connessione tra l'istanza EC2 e il database RDS così da consentire il traffico tra l'istanza EC2 e il database RDS.

- Opzione 3: connessione manuale di un'istanza a un database RDS creando dei gruppi di sicurezza

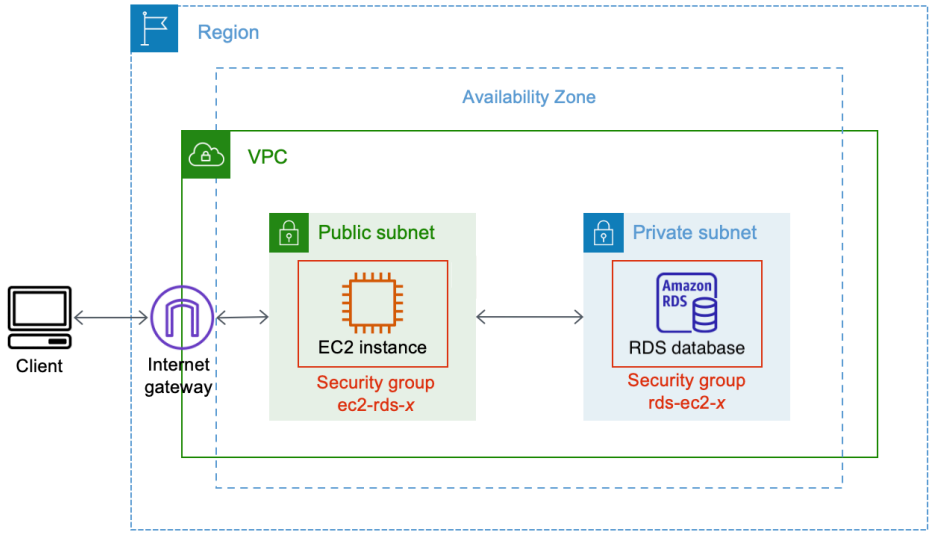
  Configura la connessione tra l'istanza EC2 e il database RDS configurando e assegnando manualmente i gruppi di sicurezza per riprodurre la configurazione creata automaticamente dalla funzione di connessione automatica nelle opzioni 1 e 2.

Contesto

Consideriamo il seguente scenario come il motivo per cui vorresti configurare una connessione tra la tua istanza EC2 e un database RDS: il tuo sito Web presenta un modulo che gli utenti devono compilare. Devi acquisire i dati del modulo in un database. Puoi ospitare il tuo sito Web su un'istanza EC2 configurata come server Web e puoi acquisire i dati del modulo in un database RDS. L'istanza EC2 e il database RDS devono essere connessi tra di loro in modo che i dati del modulo possano passare dall'istanza EC2 al database RDS. Questo tutorial spiega come configurare tale connessione. Nota che questo è solo un esempio di un caso d'uso per connettere un'istanza EC2 e un database RDS.

Architecture

Il diagramma seguente mostra le risorse create e la configurazione architettonica risultante dal completamento di tutti i passaggi di questo tutorial.



Il diagramma illustra le seguenti risorse che creerai:

- Creerai un'istanza EC2 e un database RDS nello stesso VPC e nella stessa Regione AWS zona di disponibilità.
- Creerai l'istanza EC2 in una sottorete pubblica.
- Creerai il database RDS in una sottorete privata.

  Quando utilizzi la console RDS per creare il database RDS e connettere automaticamente l'istanza EC2, il VPC, il gruppo di sottorete database e le impostazioni di accesso pubblico per il database vengono selezionate automaticamente. Il database RDS viene creato automaticamente in una sottorete privata all'interno dello stesso VPC dell'istanza EC2.
- Gli utenti di Internet possono connettersi all'istanza EC2 tramite SSH o HTTP/HTTPS tramite un gateway Internet.
- Gli utenti di Internet non possono connettersi direttamente al database RDS; solo l'istanza EC2 è connessa al database RDS.
- Quando utilizzi la funzione di connessione automatica per consentire il traffico tra l'istanza EC2 e il database RDS, vengono creati e aggiunti automaticamente i gruppi di sicurezza seguenti:
  - Il gruppo di sicurezza ec2-rds- ***x*** viene creato e aggiunto all'istanza EC2. Ha una regola in uscita che fa riferimento al gruppo di sicurezza rds-ec2- come destinazione. ***x*** Ciò consente al traffico proveniente dall'istanza EC2 di raggiungere il database RDS con il gruppo di sicurezza rds-ec2-. ***x***
  - Il gruppo di sicurezza rds-ec2- ***x*** viene creato e aggiunto al database RDS. Ha una regola in entrata che fa riferimento al gruppo di sicurezza ec2-rds- come origine. ***x*** Ciò consente al traffico proveniente dall'istanza EC2 con il gruppo di sicurezza ec2-rds- ***x*** di raggiungere il database RDS.

  Utilizzando gruppi di sicurezza separati (uno per l'istanza EC2 e uno per il database RDS) hai un migliore controllo sulla sicurezza dell'istanza e del database. Se dovessi utilizzare lo stesso gruppo di sicurezza sia sull'istanza sia sul database e quindi modificassi il gruppo di sicurezza per adattarlo, ad esempio, solo al database, la modifica influirebbe sia sull'istanza sia sul database. In altre parole, se dovessi utilizzare un gruppo di sicurezza, potresti modificare involontariamente la sicurezza di una risorsa (l'istanza o il database) avendo dimenticato che il gruppo di sicurezza era associato a tale risorsa.

I gruppi di sicurezza creati automaticamente rispettano inoltre i privilegi minimi in quanto consentono solo la connessione reciproca per tale carico di lavoro sulla porta del database creando una coppia di gruppi di sicurezza specifica per il carico di lavoro.

Considerazioni

Considera quanto segue quando completi i passaggi di questo tutorial:

- Due console: per questo tutorial utilizzerai le due console seguenti:
  - Console Amazon EC2: utilizzerai la console EC2 per avviare istanze, per connettere automaticamente un'istanza EC2 a un database RDS e per l'opzione manuale di configurazione della connessione attraverso la creazione di gruppi di sicurezza.
  - Console Amazon RDS: utilizzerai la console RDS per creare un database RDS e connettere automaticamente un'istanza EC2 a un database RDS.
- Un VPC: per utilizzare la funzione di connessione automatica, l'istanza EC2 e il database RDS devono trovarsi nello stesso VPC.

  Se dovessi configurare manualmente la connessione tra l'istanza EC2 e il database RDS, potresti avviare l'istanza EC2 in un VPC e il database RDS in un altro VPC; tuttavia, dovresti configurare instradamento e configurazione VPC aggiuntivi. Questo scenario non è trattato in questo tutorial.
- Uno Regione AWS: l'istanza EC2 e il database RDS devono trovarsi nella stessa regione.
- Due gruppi di sicurezza: la connettività tra l'istanza EC2 e il database RDS viene configurata da due gruppi di sicurezza: un gruppo di sicurezza per l'istanza EC2 e un gruppo di sicurezza per il database RDS.

  Quando utilizzi la funzione di connessione automatica nella console EC2 o nella console RDS per configurare la connettività (opzione 1 e opzione 2 di questo tutorial), i gruppi di sicurezza vengono creati e assegnati automaticamente all'istanza EC2 e al database RDS.

  Se non utilizzi la funzione di connessione automatica, dovrai creare e assegnare manualmente i gruppi di sicurezza. Puoi farlo nell'opzione 3 di questo tutorial.

È ora di completare il tutorial

30 minuti

Puoi completare l'intero tutorial in una sola sessione oppure puoi completarlo facendo un passo per volta.

Costi

Completando questo tutorial, potresti incorrere in costi per AWS le risorse che crei.

Puoi utilizzare Amazon EC2 con il livello gratuito a condizione che il tuo AWS account sia idoneo per il livello gratuito e configuri le tue risorse in base ai requisiti del livello gratuito. Per ulteriori informazioni, consulta Vantaggi del piano gratuito prima e dopo il 15 luglio 2025.

Ti verranno applicati costi per il trasferimento di dati se l'istanza EC2 e il database RDS si trovano in zone di disponibilità diverse. Per evitare di incorrere in questi costi, l'istanza EC2 e il database RDS devono trovarsi nella stessa zona di disponibilità. Per informazioni sulle tariffe per il trasferimento dei dati, consulta Data Transfer nella pagina dei prezzi di Amazon EC2 On-Demand .

Per evitare di incorrere in costi dopo aver completato il tutorial, assicurati di eliminare le risorse se non sono più necessarie. Per le fasi di eliminazione delle risorse, consulta Attività 4 (Facoltativo): Pulire.

Opzione 1: connessione automatica dell'istanza al database RDS tramite la console EC2

L'obiettivo dell'opzione 1 è comprendere la funzionalità di connessione automatica nella console EC2 che configura automaticamente la connessione tra l'istanza EC2 e il database RDS per consentire il traffico dall'istanza EC2 al database RDS. Nell'opzione 3 imparerai come configurare manualmente la connessione.

Processi

- Prima di iniziare
- Attività 1 (Facoltativo): Creare un database RDS
- Attività 2 (Facoltativo): Avvia un'istanza EC2
- Attività 3: connessione automatica dell'istanza EC2 al database RDS
- Attività 4: verifica della configurazione della connessione
- Attività 5 (Facoltativo): Pulire

Prima di iniziare

Per completare questo tutorial, avrai bisogno di quanto segue:

- un database RDS nello stesso VPC dell'istanza EC2. Puoi utilizzare un database RDS esistente o seguire i passaggi illustrati nell'Attività 1 per creare un nuovo database RDS.
- un'istanza EC2 nello stesso VPC del database RDS. Puoi utilizzare un'istanza EC2 esistente o seguire i passaggi illustrati nell'Attività 2 per creare una nuova istanza EC2.
- Autorizzazioni per effettuare le seguenti operazioni:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Attività 1 (Facoltativo): Creare un database RDS

> **Note**
>
> La creazione di un database Amazon RDS non è l'obiettivo di questo tutorial. Se già disponi di un database RDS e vorresti utilizzarlo in questo tutorial, puoi ignorare questa attività. Se utilizzi un database RDS esistente, assicurati che si trovi nello stesso VPC dell'istanza EC2 in modo da poter utilizzare la funzione di connessione automatica.

L'obiettivo di questa attività è creare un database RDS in modo da poter completare l'Attività 3 che prevede la configurazione della connessione tra l'istanza EC2 e il database RDS. I passaggi di questa attività illustrano la configurazione del database RDS come segue:

- Tipo di motore: MySQL
- Modello: livello gratuito
- DB Instance Identifier (Identificatore istanze database): **`tutorial-database-1`**
- DB instance class (Classe istanza database): `db.t3.micro`

> **Important**
>
> In un ambiente di produzione, dovrai configurare il database in base alle tue esigenze specifiche.

Creazione di un database MySQL RDS

1. Aprire la console Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Dal selettore di regione (in alto a destra), scegli un Regione AWS. Il database e l'istanza EC2 devono trovarsi nella stessa regione per utilizzare la funzionalità di connessione automatica nella console EC2.
3. Sul pannello di controllo seleziona Create database (Crea database).
4. Sotto Choose a database creation method (Seleziona metodo di creazione del database), assicurati che Standard create (Creazione standard) sia selezionato. Il selettore VPC non è disponibile, se scegli Easy create (Creazione facile). È necessario assicurarsi che il database si trovi nello stesso VPC dell'istanza EC2 per utilizzare la funzionalità di connessione automatica nella console EC2.
5. Sotto Engine options (Opzioni del motore) per Engine type (Tipo di motore) scegli MySQL.
6. Sotto Templates (Modelli), scegli un modello di esempio che soddisfi le tue esigenze. Per questo tutorial scegli il Free tier (Livello gratuito) in modo da creare un database RDS gratuitamente. Tuttavia, nota che il piano gratuito è disponibile solo per gli account idonei al livello gratuito. Puoi saperne di più selezionando il link Info (Informazioni) nel campo Free tier (Livello gratuito).
7. In Settings (Impostazioni), procedere come segue:

a. Per il DB instance identifier (Identificatore istanze database) inserire un nome per il database. Per questo tutorial, digita **`tutorial-database-1`**.

b. Per il Nome utente principale, lascia il nome predefinito, che è **`admin`**.

c. Come Master password (Password principale) inserisci una password per questo tutorial che riesci a ricordare quindi per Confirm password (Conferma password) inserisci nuovamente la password.

8. In Configurazione dell'istanza, lascia il valore predefinito per la Classe di istanza DB, che è db.t3.micro. Se il tuo account rientra nel piano gratuito, puoi utilizzare questa classe di database gratuitamente. Per ulteriori informazioni, consulta Piano gratuito di AWS.

9. Sotto Connectivity (Connettività), per Compute resource (Risorsa di calcolo), scegli Don't connect to an EC2 compute resource (Non connetterti a una risorsa di calcolo EC2) perché connetterai l'istanza EC2 e il database RDS più avanti, nell'Attività 3.

   [Più avanti, nell'Opzione 2 di questo tutorial, proverai la funzione di connessione automatica nella console RDS scegliendo Connect to an EC2 compute resource (Connetti a una risorsa di calcolo EC2).]

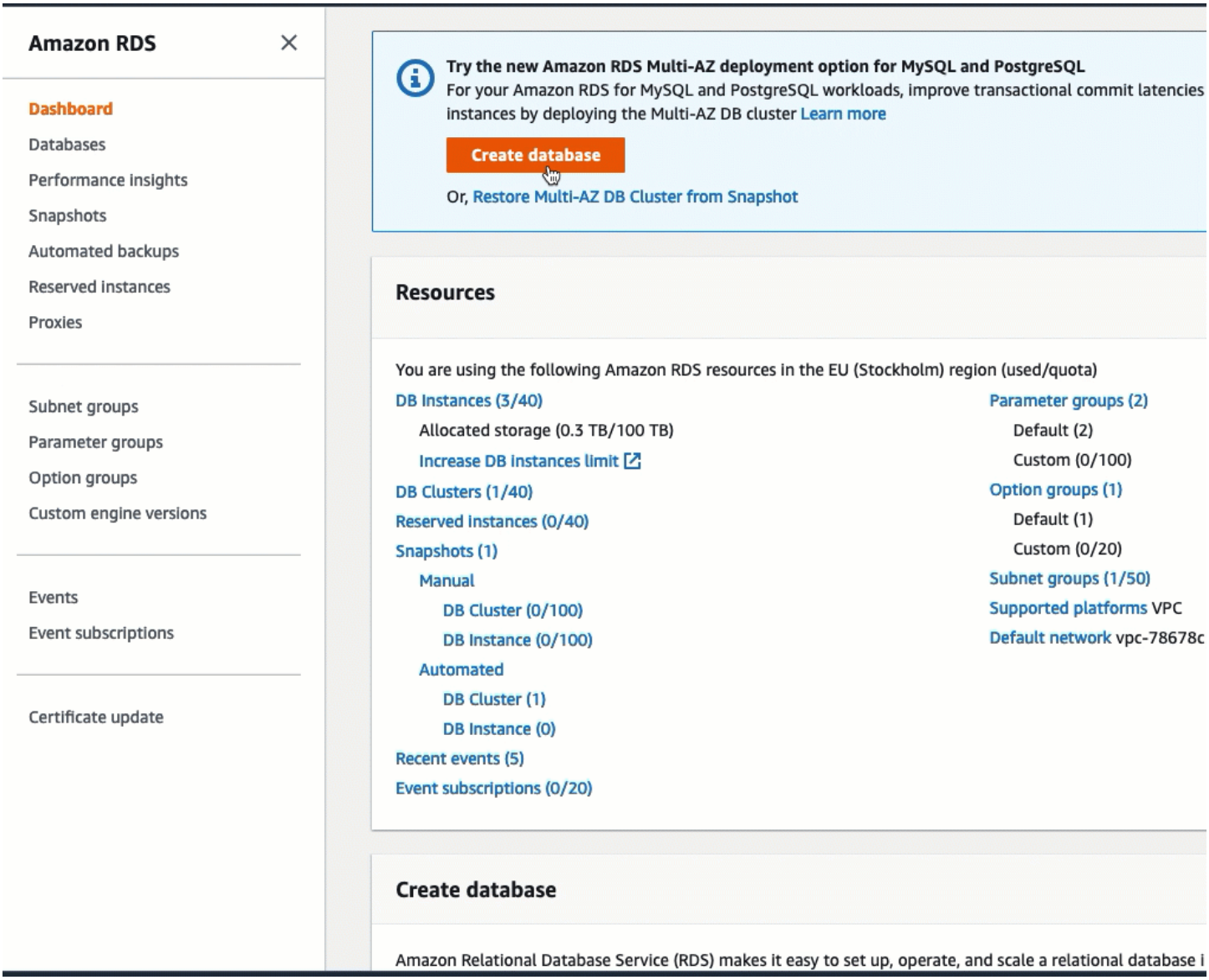
10. Per Virtual private cloud (VPC) [Cloud privato virtuale (VPC)] seleziona un VPC. Il VPC deve avere un gruppo di sottorete database. Per utilizzare la funzione di connessione automatica, l'istanza EC2 e il database RDS devono trovarsi nello stesso VPC.

11. Per tutti gli altri campi di questa pagina mantieni i valori predefiniti.

12. Scegliere Crea database.

    Nella schermata Databases (Database) lo Status (Stato) del nuovo database è Creating fino a quando il database non è pronto per l'uso. Quando lo stato diventa Available (Disponibile), puoi connetterti al database. A seconda della classe del database e della quantità di storage, possono trascorrere fino a 20 minuti prima che il nuovo database sia disponibile.

Visualizzazione di un'animazione: creazione di un database RDS



Attività 2 (Facoltativo): Avvia un'istanza EC2

> **Note**
>
> Il fulcro di questo tutorial non è l'avvio di un'istanza. Se già disponi di un'istanza Amazon EC2 e vorresti utilizzarla in questo tutorial, puoi ignorare questa attività.
> Se utilizzi un'istanza EC2 esistente, assicurati che si trovi nello stesso VPC del database RDS in modo da poter utilizzare la funzione di connessione automatica.

L'obiettivo di questa attività è creare un'istanza EC2 in modo da poter completare l'Attività 3 che prevede la configurazione della connessione tra l'istanza EC2 e il database Amazon RDS. I passaggi di questa attività illustrano la configurazione dell'istanza EC2 come segue:

- nome dell'istanza: **`tutorial-instance-1`**
- AMI: Amazon Linux 2
- tipo di istanza: `t2.micro`
- Auto-assign IP pubblico: abilitato
- gruppo di sicurezza con le tre regole seguenti:
  - Consenti SSH dal tuo indirizzo IP
  - Consenti il traffico HTTPS da qualsiasi luogo
  - Consenti il traffico HTTP da qualsiasi luogo

> **Important**
>
> In un ambiente di produzione, dovrai configurare l'istanza in base alle tue esigenze specifiche.

Per avviare un'istanza EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal selettore di regione (in alto a destra), scegli un Regione AWS. L'istanza e il database RDS devono trovarsi nella stessa regione per utilizzare la funzionalità di connessione automatica nella console EC2.
3. Dal dashboard EC2, scegli Avvia istanza.
4. Sotto Nome e tag, per Nome inserisci un nome per identificare l'istanza. Per questo tutorial inserisci l'istanza **`tutorial-instance-1`**. Sebbene il nome dell'istanza non sia obbligatorio, quando selezioni l'istanza nella console EC2, questo ti aiuterà a identificarla facilmente.
5. Sotto Application and OS Images (Applicazioni e immagini del sistema operativo), scegli un'AMI che soddisfi le esigenze del tuo server web. Questo tutorial utilizza Amazon Linux 2.
6. Sotto Instance type(Tipo di istanza), per Instance type (Tipo di istanza), seleziona un tipo di istanza che soddisfi le esigenze del tuo server web. In questo tutorial si utilizza `t2.micro`.

> **Note**
>
> A seconda di quando hai creato l'account, potresti essere aver diritto a utilizzare Amazon EC2 nell'ambito del piano gratuito.
> Se l'hai creata Account AWS prima del 15 luglio 2025 e ha meno di 12 mesi, puoi utilizzare Amazon EC2 con il livello gratuito selezionando il tipo di istanza t2.micro o il tipo di istanza t3.micro nelle regioni in cui t2.micro non è disponibile. Tieni presente che quando avvii un'istanza t3.micro, l'impostazione predefinita è la modalità Illimitata, che potrebbe comportare costi aggiuntivi in base all'utilizzo della CPU. Se un tipo di istanza può essere utilizzato nell'ambito del Piano gratuito, è etichettato come Idoneo per il Piano gratuito.
> Se hai creato la tua il Account AWS 15 luglio 2025 o dopo, puoi utilizzare i tipi di istanza t3.micro , t3.small, t4g.micro, t4g.small, c7i-flex.large e m7i-flex.large per 6 mesi o fino all'esaurimento dei crediti.
> Per ulteriori informazioni, consulta Vantaggi del piano gratuito prima e dopo il 15 luglio 2025.

7. Sotto Key pair (login) [Coppia di chiavi (login)], per Key pair name (Nome della coppia di chiavi) scegli la tua coppia di chiavi.
8. Sotto Network settings (Impostazioni di rete) effettua le seguenti operazioni:

   a. Per Rete e Sottorete, se non hai apportato modifiche al VPC o alle sottoreti predefiniti, puoi mantenere le impostazioni predefinite.

      Se hai apportato modifiche al tuo VPC o alle sottoreti predefiniti, controlla quanto segue:

      i. Per utilizzare la funzione di connessione automatica, l'istanza deve trovarsi nello stesso VPC del database RDS. Per impostazione predefinita hai a disposizione un solo VPC.

      ii. Il VPC in cui stai avviando l'istanza deve avere un gateway Internet collegato ad esso in modo da poter accedere al tuo server web da Internet. Il tuo VPC predefinito viene configurato automaticamente con un gateway Internet.

      iii. Per assicurarti che la tua istanza riceva un indirizzo IP pubblico, per l'IP pubblico, verifica che l'opzione Abilita sia selezionata. Auto-assign Se è selezionato Disabilita, scegli Modifica (a destra di Impostazioni di rete), quindi, per l'IP Auto-assign pubblico, scegli Abilita.

b. Per connettersi all'istanza tramite SSH, è necessaria una regola del gruppo di sicurezza che autorizzi il traffico SSH (Linux) o RDP (Windows) dall'indirizzo IPv4 pubblico del computer. Per impostazione predefinita, quando si avvia un'istanza, viene creato un nuovo gruppo di sicurezza con una regola che consente il traffico SSH in entrata da qualsiasi luogo.

   Per assicurarti che solo il tuo indirizzo IP possa connettersi alla tua istanza, sotto Firewall (gruppi di sicurezza), dall'elenco a discesa accanto alla casella di controllo Consenti traffico SSH da, scegli Il mio IP.

c. Per consentire il traffico da Internet alla tua istanza, seleziona le caselle di controllo seguenti:

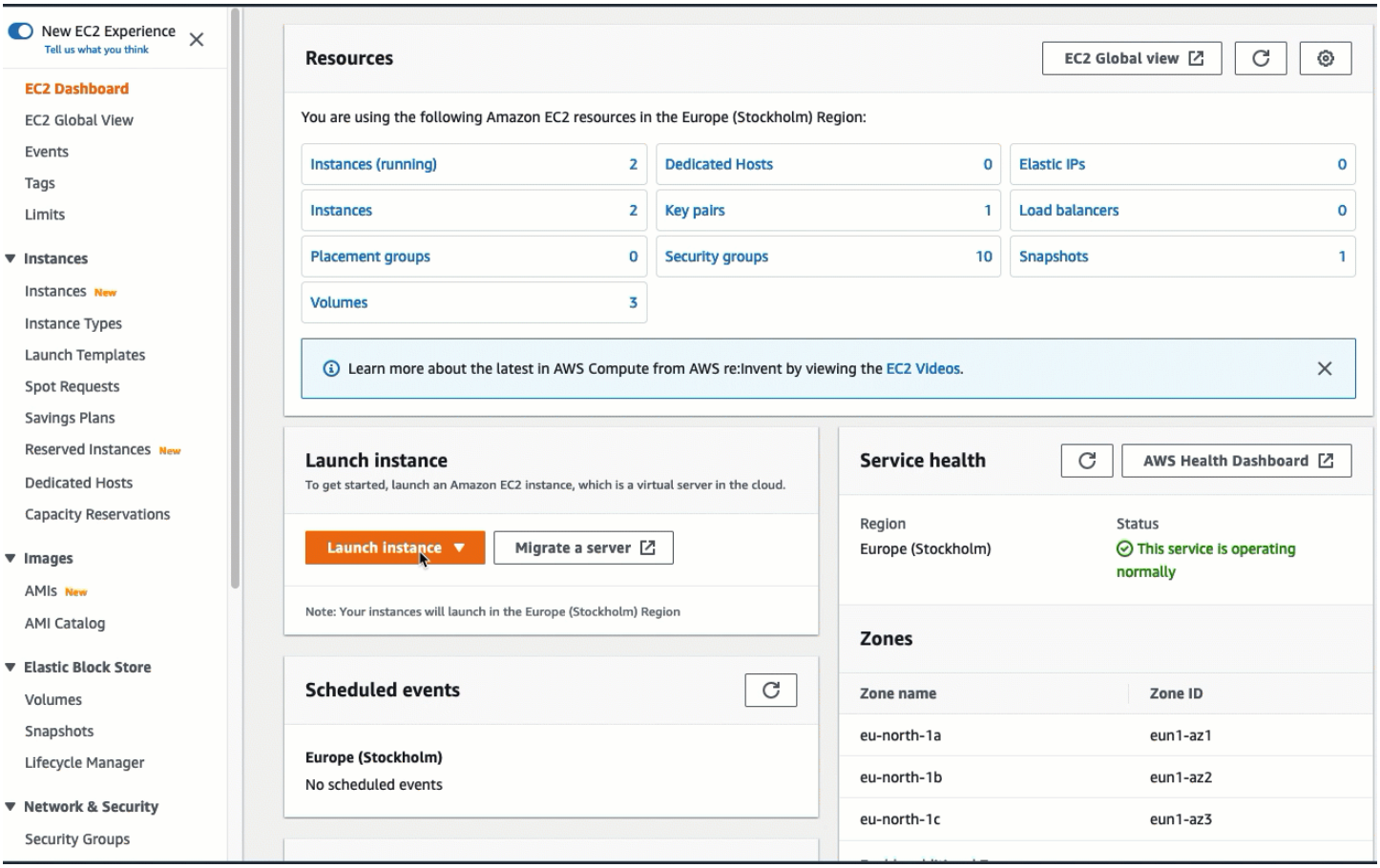
   - Allow HTTPs traffic from the internet (Autorizzare il traffico HTTPS da Internet)
   - Allow HTTP traffic from the internet (Autorizzare il traffico HTTP da Internet)

9. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza).
10. Tieni aperta la pagina di conferma. Ne avrai bisogno per eseguire l'operazione successiva, quando connetti automaticamente l'istanza al database.

    Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio dell'istanza Amazon EC2.

Per ulteriori informazioni sull'avvio di un'istanza, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

Visualizzazione di un'animazione: avvio di un'istanza EC2



Attività 3: connessione automatica dell'istanza EC2 al database RDS

L'obiettivo di questa attività è utilizzare la funzione di connessione automatica nella console EC2 per configurare automaticamente la connessione tra l'istanza EC2 e il database RDS.

Connessione automatica di un'istanza EC2 esistente a un database RDS utilizzando la console EC2

1. Nella pagina di conferma dell'avvenuto avvio dell'istanza (dovrebbe essere aperta dall'attività precedente), scegli Connect an RDS database (Connetti un database RDS).

   Se hai chiuso la pagina di conferma, segui questi passaggi:

   a. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

   b. Nel riquadro di navigazione, scegliere Instances (Istanze).

   c. Seleziona l'istanza EC2 che hai appena creato, quindi scegli Actions (Azioni), Networking (Rete), Connect RDS database (Connetti database RDS).

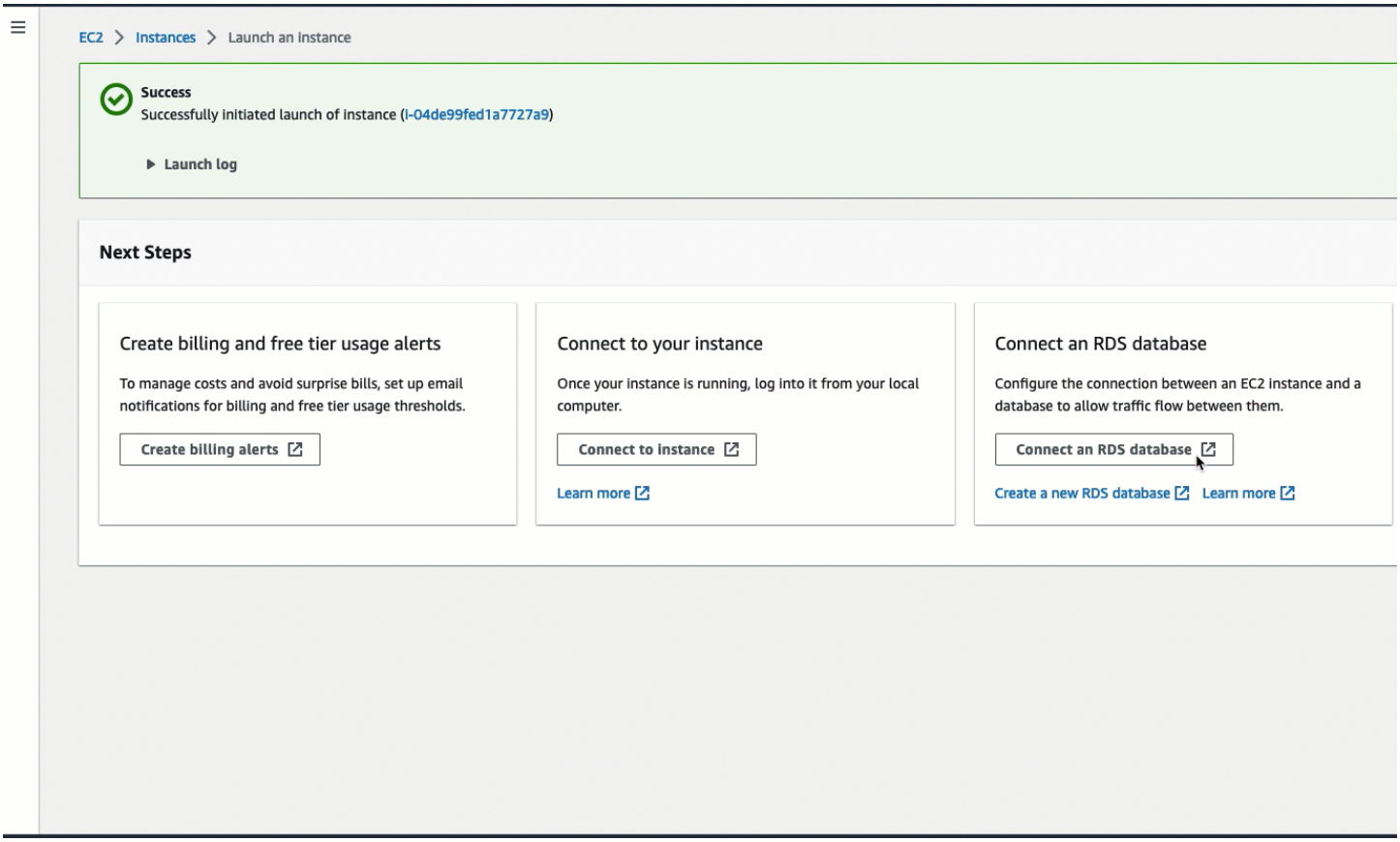
Se Connect RDS database (Connetti database RDS) non è disponibile, controlla che l'istanza EC2 sia nello stato Running (In esecuzione).

2. Per il Database role (Ruolo del database), scegli Instance (Istanza). In questo caso Instance (Istanza) si riferisce all'istanza del database.
3. Per il RDS database (Database RDS), scegli il database RDS che hai creato nell'Attività 1.

> **Note**
>
> L'istanza EC2 e il database RDS devono trovarsi nello stesso VPC per connettersi tra loro.

4. Scegli Connetti.

Visualizzazione di un'animazione: connessione automatica di un'istanza EC2 appena avviata a un database RDS



Attività 4: verifica della configurazione della connessione

L'obiettivo di questa attività è verificare che i due gruppi di sicurezza siano stati creati e assegnati all'istanza e al database.

Quando utilizzi la funzione di connessione automatica nella console per configurare la connettività, i gruppi di sicurezza vengono creati e assegnati automaticamente all'istanza e al database, come segue:

- Il gruppo di sicurezza rds-ec2-*x* viene creato e aggiunto al database RDS. Ha una regola in entrata che fa riferimento al gruppo di sicurezza ec2-rds- come origine. *x* Ciò consente al traffico proveniente dall'istanza EC2 con il gruppo di sicurezza ec2-rds-*x* di raggiungere il database RDS.
- Il gruppo di sicurezza ec2-rds-*x* viene creato e aggiunto all'istanza EC2. Ha una regola in uscita che fa riferimento al gruppo di sicurezza rds-ec2- come destinazione. *x* Ciò consente al traffico proveniente dall'istanza EC2 di raggiungere il database RDS con il gruppo di sicurezza rds-ec2-. *x*

Verifica della configurazione della connessione tramite la console

1. Aprire la console Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Nel riquadro di navigazione scegli Database.
3. Scegli il database RDS creato per questo tutorial.
4. Nella scheda Connettività e sicurezza, in Sicurezza, gruppi di sicurezza VPC , verifica che sia visualizzato un gruppo di sicurezza chiamato rds-ec2-. *x*
5. Scegli il gruppo di sicurezza rds-ec2-. *x* Si apre la schermata Gruppi di sicurezza nella console EC2.
6. Scegli il gruppo di sicurezza rds-ec2-*x* per aprirlo.
7. Selezionare la scheda Regole in entrata.
8. Verifica che esista la seguente regola del gruppo di sicurezza, come illustrato di seguito:

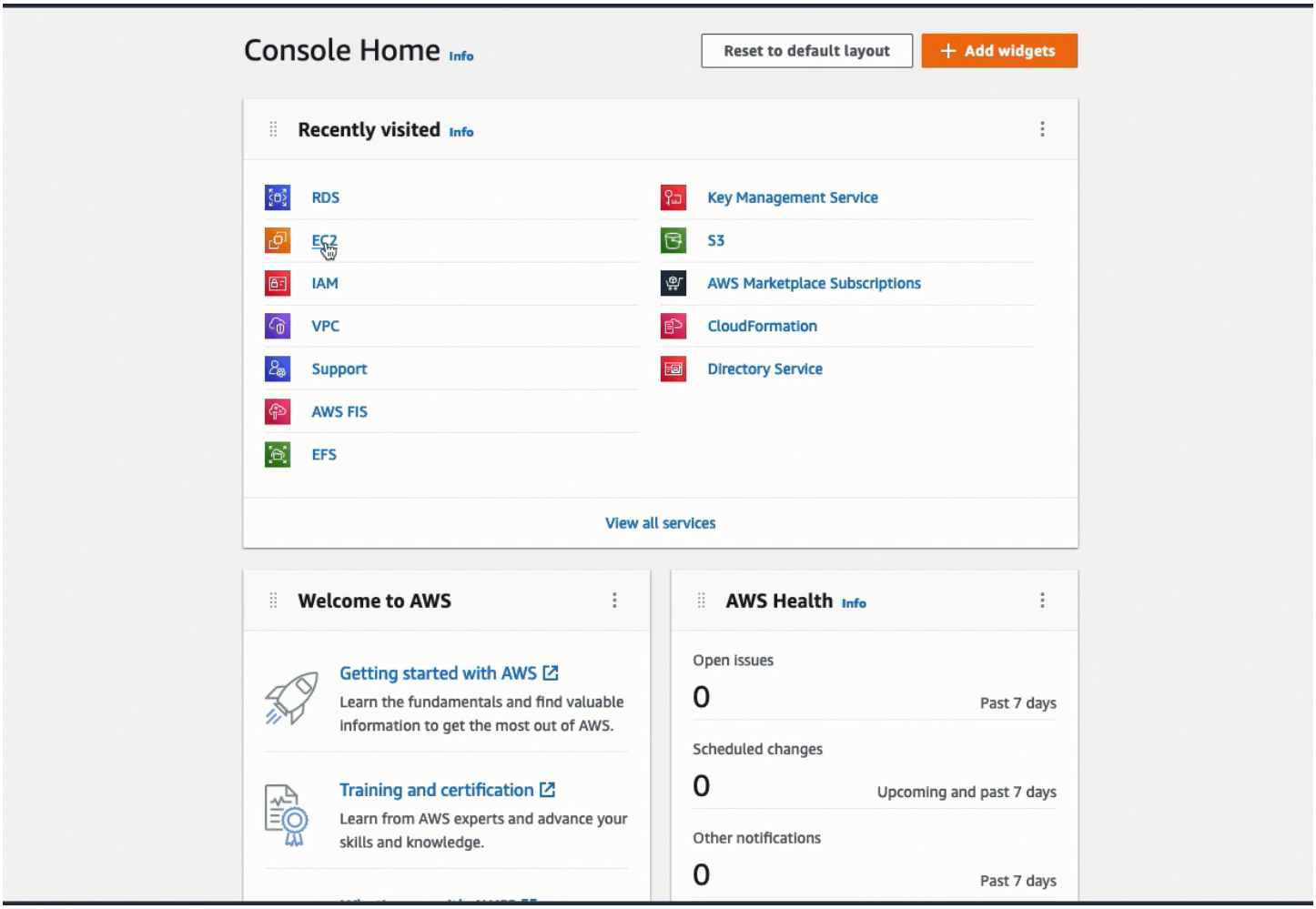
    - Tipo: MYSQL/Aurora
    - Intervallo porte: 3306
    - Fonte: ***sg-0987654321example***/ec2-rds-*x* — Questo è il gruppo di sicurezza assegnato all'istanza EC2 verificata nei passaggi precedenti.
    - Descrizione: regola per consentire le connessioni da istanze EC2 con allegato ***sg-1234567890example***

9. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
10. Nel riquadro di navigazione, scegliere Instances (Istanze).
11. Scegli l'istanza EC2 che hai selezionato per connetterti al database RDS nell'operazione precedente e scegli la scheda Security (Sicurezza).
12. In Dettagli di sicurezza, Gruppi di sicurezza, verifica che un gruppo di sicurezza chiamato ec2-rds- ***x*** sia presente nell'elenco. *x* è un numero.
13. Scegli il gruppo di *x* sicurezza ec2-rds- per aprirlo.
14. Scegli la scheda Outbound rules (Regole in uscita).
15. Verifica che esista la seguente regola del gruppo di sicurezza, come illustrato di seguito:

    - Tipo: MYSQL/Aurora
    - Intervallo porte: 3306
    - Destinazione:/rds-ec2- ***sg-1234567890example x***
    - Descrizione: Regola per consentire le connessioni a **`database-tutorial`** da qualsiasi istanza a cui è collegato questo gruppo di sicurezza

Verificando che questi gruppi di sicurezza e le regole dei gruppi di sicurezza esistano e che siano assegnati al database RDS e all'istanza EC2 come descritto in questa procedura, puoi verificare che la connessione sia stata configurata automaticamente utilizzando la funzione di connessione automatica.

Visualizzazione di un'animazione: verifica della configurazione della connessione



Hai completato l'Opzione 1 di questo tutorial. Ora puoi completare l'Opzione 2, che spiega come usare la console RDS per connettere automaticamente un'istanza EC2 a un database RDS, oppure puoi completare l'Opzione 3, che spiega come configurare manualmente i gruppi di sicurezza creati automaticamente nell'Opzione 1.

Attività 5 (Facoltativo): Pulire

> **Warning**
>
> La terminazione di un'istanza è permanente e irreversibile.
> Dopo aver terminato un'istanza, non puoi più connetterti a essa e non puoi ripristinarla. Inoltre, tutti i volumi Amazon EBS collegati e configurati per essere eliminati in caso di terminazione vengono eliminati in modo definitivo e non possono essere recuperati. Tutti i dati archiviati nei volumi di archivio dell'istanza vengono persi in modo definitivo. Per ulteriori informazioni, consulta Come funziona la terminazione delle istanze.

Prima di terminare un'istanza, assicurati di aver eseguito il backup di tutti i dati che devi mantenere dopo la terminazione sull'archivio persistente.

Ora che hai completato il tutorial, è buona norma ripulire (eliminare) tutte le risorse che non desideri più utilizzare. La pulizia AWS delle risorse impedisce al tuo account di incorrere in ulteriori addebiti.

Se hai avviato un'istanza EC2 appositamente per questo tutorial, puoi interromperla per non incorrere in alcun addebito correlato a questa.

Per interrompere un'istanza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza creata per questo tutorial, quindi scegli Stato istanza, Termina istanza.
4. Quando viene richiesta la conferma, seleziona Interrompi.

Se hai creato un database RDS appositamente per questo tutorial, puoi interromperlo per non incorrere in alcun addebito correlato a questo.

Eliminazione di un database RDS tramite la console

1. Aprire la console Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Nel pannello di navigazione, seleziona Database.
3. Seleziona il database RDS che hai creato per questo tutorial e scegli Azioni, Elimina.
4. Inserisci **`delete me`** nella casella e scegli Elimina.

Opzione 2: connessione automatica dell'istanza al database RDS tramite la console RDS

L'obiettivo dell'opzione 2 è comprendere la funzionalità di connessione automatica nella console RDS che prevede la configurazione automatica della connessione tra l'istanza EC2 e il database RDS in modo da consentire il traffico dall'istanza EC2 al database RDS. Nell'opzione 3 imparerai come configurare manualmente la connessione.

Processi

- Prima di iniziare
- Attività 1 (Facoltativo): Avvia un'istanza EC2
- Attività 2: creazione di un database RDS e connessione automatica di questo all'istanza EC2
- Attività 3: verifica della configurazione di connessione
- Attività 4 (Facoltativo): Pulire

Prima di iniziare

Per completare questo tutorial, avrai bisogno di quanto segue:

- Un'istanza EC2 nello stesso VPC del database RDS. Puoi utilizzare un'istanza EC2 esistente o seguire i passaggi illustrati nell'Attività 1 per creare una nuova istanza.
- Autorizzazioni per effettuare le seguenti operazioni:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Attività 1 (Facoltativo): Avvia un'istanza EC2

> **Note**
>
> Il fulcro di questo tutorial non è l'avvio di un'istanza. Se già disponi di un'istanza Amazon EC2 e vorresti utilizzarla in questo tutorial, puoi ignorare questa attività.

L'obiettivo di questa attività è avviare un'istanza EC2 in modo da poter completare l'Attività 2 che prevede la configurazione della connessione tra l'istanza EC2 e il database Amazon RDS. I passaggi di questa attività illustrano la configurazione dell'istanza EC2 come segue:

- nome dell'istanza: **`tutorial-instance-2`**
- AMI: Amazon Linux 2
- tipo di istanza: `t2.micro`
- Auto-assign IP pubblico: abilitato
- gruppo di sicurezza con le tre regole seguenti:
  - Consenti SSH dal tuo indirizzo IP
  - Consenti il traffico HTTPS da qualsiasi luogo
  - Consenti il traffico HTTP da qualsiasi luogo

> **Important**
>
> In un ambiente di produzione, dovrai configurare l'istanza in base alle tue esigenze specifiche.

Per avviare un'istanza EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal dashboard EC2, scegli Avvia istanza.
3. Sotto Nome e tag, per Nome inserisci un nome per identificare l'istanza. Per questo tutorial inserisci l'istanza **`tutorial-instance-2`**. Sebbene il nome dell'istanza non sia obbligatorio, quando selezioni l'istanza nella console RDS, questo ti aiuterà a identificarla facilmente.
4. Sotto Application and OS Images (Applicazioni e immagini del sistema operativo), scegli un'AMI che soddisfi le esigenze del tuo server web. Questo tutorial utilizza Amazon Linux.
5. Sotto Tipo di istanza, per Tipo di istanza, seleziona un tipo di istanza che soddisfi le esigenze del tuo server web. In questo tutorial si utilizza `t2.micro`.

   > **Note**
   >
   > A seconda di quando hai creato l'account, potresti essere aver diritto a utilizzare Amazon EC2 nell'ambito del piano gratuito.

Se hai creato la tua Account AWS prima del 15 luglio 2025 e ha meno di 12 mesi, puoi utilizzare Amazon EC2 con il piano gratuito selezionando il tipo di istanza t2.micro o il tipo di istanza t3.micro nelle regioni in cui t2.micro non è disponibile. Tieni presente che quando avvii un'istanza t3.micro, l'impostazione predefinita è la modalità Illimitata, che potrebbe comportare costi aggiuntivi in base all'utilizzo della CPU. Se un tipo di istanza può essere utilizzato nell'ambito del Piano gratuito, è etichettato come Idoneo per il Piano gratuito.
Se hai creato la tua il Account AWS 15 luglio 2025 o dopo, puoi utilizzare i tipi di istanza t3.micro , t3.small, t4g.micro, t4g.small, c7i-flex.large e m7i-flex.large per 6 mesi o fino all'esaurimento dei crediti.
Per ulteriori informazioni, consulta Vantaggi del piano gratuito prima e dopo il 15 luglio 2025.

6. Sotto Key pair (login) [Coppia di chiavi (login)], per Key pair name (Nome della coppia di chiavi) scegli la tua coppia di chiavi.
7. Sotto Network settings (Impostazioni di rete) effettua le seguenti operazioni:

   a. Per Rete e Sottorete, se non hai apportato modifiche al VPC o alle sottoreti predefiniti, puoi mantenere le impostazioni predefinite.

      Se hai apportato modifiche al tuo VPC o alle sottoreti predefiniti, controlla quanto segue:

      i. Per utilizzare la configurazione di connessione automatica, l'istanza deve trovarsi nello stesso VPC del database RDS. Per impostazione predefinita hai a disposizione un solo VPC.

      ii. Il VPC in cui stai avviando l'istanza deve avere un gateway Internet collegato ad esso in modo da poter accedere al tuo server web da Internet. Il tuo VPC predefinito viene configurato automaticamente con un gateway Internet.

      iii. Per assicurarti che la tua istanza riceva un indirizzo IP pubblico, per l'IP pubblico, verifica che l'opzione Abilita sia selezionata. Auto-assign Se è selezionato Disabilita, scegli Modifica (a destra di Impostazioni di rete), quindi, per l'IP Auto-assign pubblico, scegli Abilita.

   b. Per connettersi all'istanza tramite SSH, è necessaria una regola del gruppo di sicurezza che autorizzi il traffico SSH (Linux) o RDP (Windows) dall'indirizzo IPv4 pubblico del computer. Per impostazione predefinita, quando si avvia un'istanza, viene creato un nuovo gruppo di sicurezza con una regola che consente il traffico SSH in entrata da qualsiasi luogo.

Per assicurarti che solo il tuo indirizzo IP possa connettersi alla tua istanza, sotto Firewall (gruppi di sicurezza), dall'elenco a discesa accanto alla casella di controllo Consenti traffico SSH da, scegli Il mio IP.

c. Per consentire il traffico da Internet alla tua istanza, seleziona le caselle di controllo seguenti:

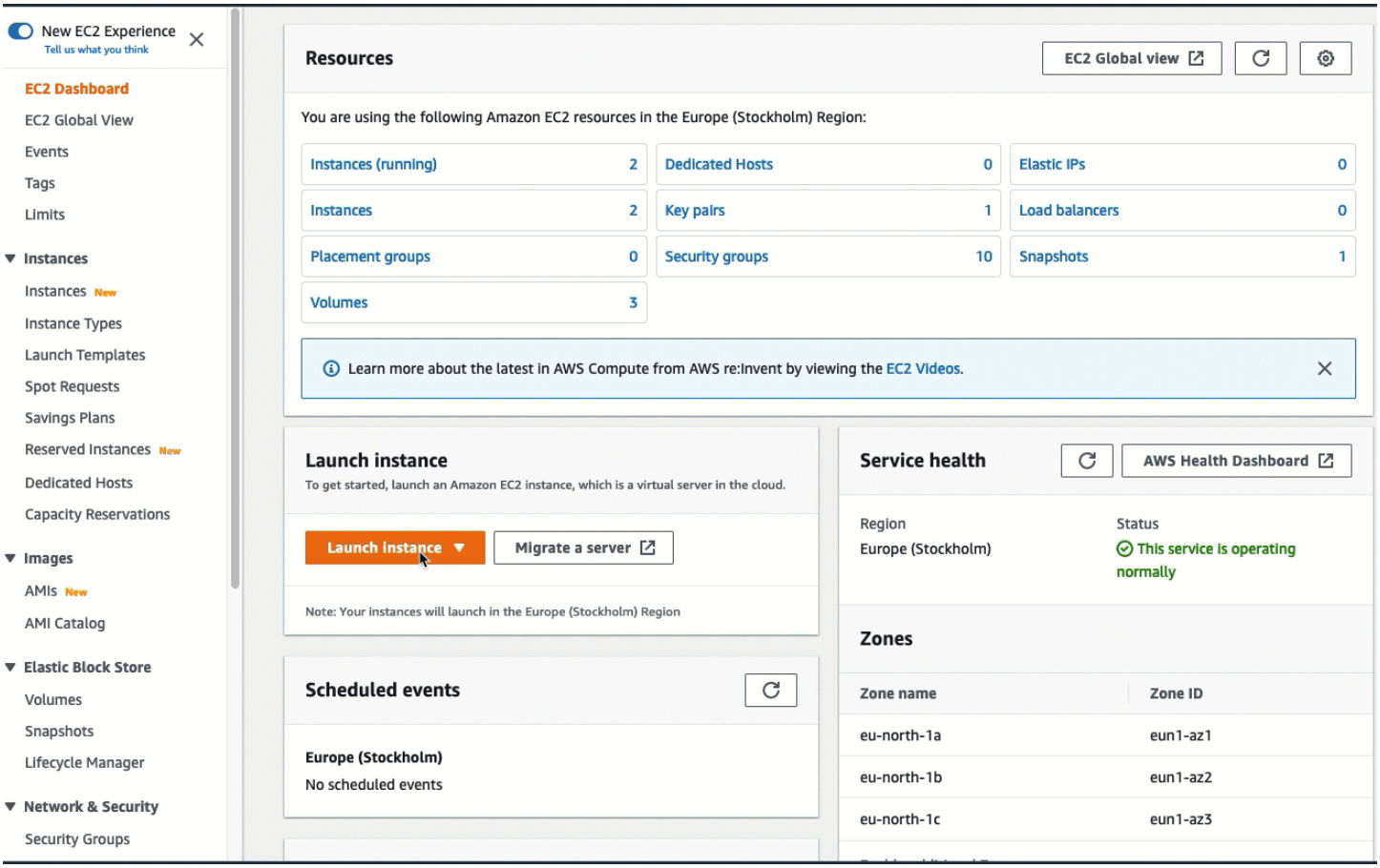
- Allow HTTPs traffic from the internet (Autorizzare il traffico HTTPS da Internet)
- Allow HTTP traffic from the internet (Autorizzare il traffico HTTP da Internet)

8. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza).
9. Scegli View Instances (Visualizza istanze) per chiudere la pagina di conferma e tornare alla console. La tua istanza sarà prima in uno stato `pending` e poi passerà allo stato `running`.

   Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio dell'istanza Amazon EC2.

Per ulteriori informazioni sull'avvio di un'istanza, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

Visualizzazione di un'animazione: avvio di un'istanza EC2



Attività 2: creazione di un database RDS e connessione automatica di questo all'istanza EC2

L'obiettivo di questa attività è creare un database RDS e usare la funzione di connessione automatica nella console RDS per configurare automaticamente la connessione tra l'istanza EC2 e il database RDS. I passaggi di questa attività illustrano la configurazione dell'istanza database come segue:

- Tipo di motore: MySQL
- Modello: livello gratuito
- DB Instance Identifier (Identificatore istanze database): **`tutorial-database`**
- DB instance class (Classe istanza database): `db.t3.micro`

> **Important**
>
> In un ambiente di produzione, dovrai configurare l'istanza in base alle tue esigenze specifiche.

Creare un database RDS e connetterlo automaticamente a un'istanza EC2

1. Aprire la console Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Dal selettore di regione (in alto a destra), scegli quella Regione AWS in cui hai creato l'istanza EC2. L'istanza EC2 e il database RDS devono trovarsi nella stessa regione.
3. Sul pannello di controllo seleziona Create database (Crea database).
4. Sotto Choose a database creation method (Seleziona metodo di creazione del database), assicurati che Standard create (Creazione standard) sia selezionato. La funzione di connessione automatica non è disponibile, se scegli Easy create (Creazione facile).
5. Sotto Engine options (Opzioni del motore) per Engine type (Tipo di motore) scegli MySQL.
6. Sotto Templates (Modelli), scegli un modello di esempio che soddisfi le tue esigenze. Per questo tutorial scegli il Free tier (Livello gratuito) in modo da creare un database RDS gratuitamente. Tuttavia, nota che il piano gratuito è disponibile solo se il tuo account è idoneo per il piano gratuito. Puoi saperne di più selezionando il link Info (Informazioni) nel campo Free tier (Livello gratuito).
7. In Settings (Impostazioni), procedere come segue:
   a. Per il DB instance identifier (Identificatore istanze database) inserire un nome per il database. Per questo tutorial, digita **`tutorial-database`**.
   b. Per il Nome utente principale, lascia il nome predefinito, che è **`admin`**.
   c. Come Master password (Password principale) inserisci una password per questo tutorial che riesci a ricordare quindi per Confirm password (Conferma password) inserisci nuovamente la password.
8. In Configurazione dell'istanza, lascia il valore predefinito per la Classe istanza database, che è db.t3.micro. Se il tuo account è idoneo per il piano gratuito, puoi utilizzare questa istanza gratuitamente. Per ulteriori informazioni, consulta Piano gratuito di AWS.
9. Sotto Connectivity (Connettività), per Compute resource (Risorsa di calcolo), scegli Connect to an EC2 compute resource (Connetti a una risorsa di calcolo EC2). Questa è la funzione di connessione automatica della console RDS.

10. Per EC2 Instance (Istanza EC2) scegli il nome dell'istanza EC2 a cui vuoi connetterti. Ai fini di questo tutorial, puoi scegliere l'istanza che hai creato nell'attività precedente, che hai denominato **`tutorial-instance`**, oppure scegliere un'altra istanza esistente. Se l'istanza non è visualizzata nell'elenco, scegli l'icona di aggiornamento a destra di Connectivity (Connettività).

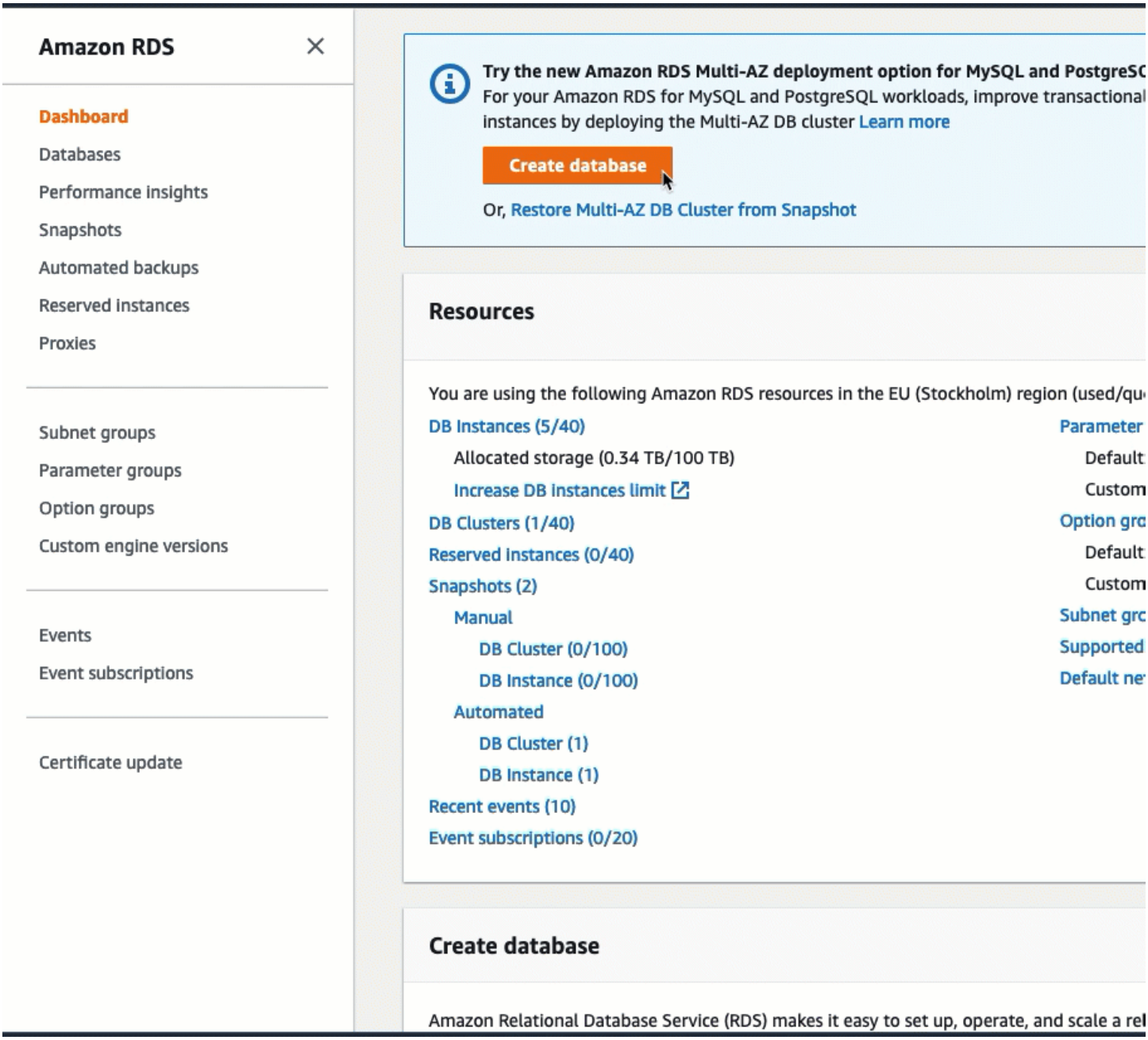
    Quando utilizzi la funzione di connessione automatica, un gruppo di sicurezza viene aggiunto a questa istanza EC2 e un altro gruppo di sicurezza viene aggiunto al database RDS. I gruppi di sicurezza sono configurati automaticamente per consentire il traffico tra l'istanza EC2 e il database RDS. Nella prossima attività, verificherai che i gruppi di sicurezza siano stati creati e assegnati all'istanza EC2 e al database RDS.

11. Scegliere Crea database.

    Nella schermata Databases (Database) lo Status (Stato) del nuovo database è Creating fino a quando il database non è pronto per l'uso. Quando lo stato diventa Available (Disponibile), puoi connetterti al database. A seconda della classe del database e della quantità di storage, possono trascorrere fino a 20 minuti prima che il nuovo database sia disponibile.

Per ulteriori informazioni, consulta Configurare la connettività di rete automatica con un'istanza EC2 nella Guida per l'utente di Amazon RDS.

Visualizzazione di un'animazione: creazione un database RDS e connessione automatica di questo a un'istanza EC2



Attività 3: verifica della configurazione di connessione

L'obiettivo di questa attività è verificare che i due gruppi di sicurezza siano stati creati e assegnati all'istanza e al database.

Quando utilizzi la funzione di connessione automatica nella console per configurare la connettività, i gruppi di sicurezza vengono creati e assegnati automaticamente all'istanza e al database, come segue:

- Il gruppo di sicurezza rds-ec2- *x* viene creato e aggiunto al database RDS. Ha una regola in entrata che fa riferimento al gruppo di sicurezza ec2-rds- come origine. *x* Ciò consente al traffico proveniente dall'istanza EC2 con il gruppo di sicurezza ec2-rds- *x* di raggiungere il database RDS.
- Il gruppo di sicurezza ec2-rds- *x* viene creato e aggiunto all'istanza EC2. Ha una regola in uscita che fa riferimento al gruppo di sicurezza rds-ec2- come destinazione. *x* Ciò consente al traffico proveniente dall'istanza EC2 di raggiungere il database RDS con il gruppo di sicurezza rds-ec2-. *x*

Verifica della configurazione della connessione tramite la console

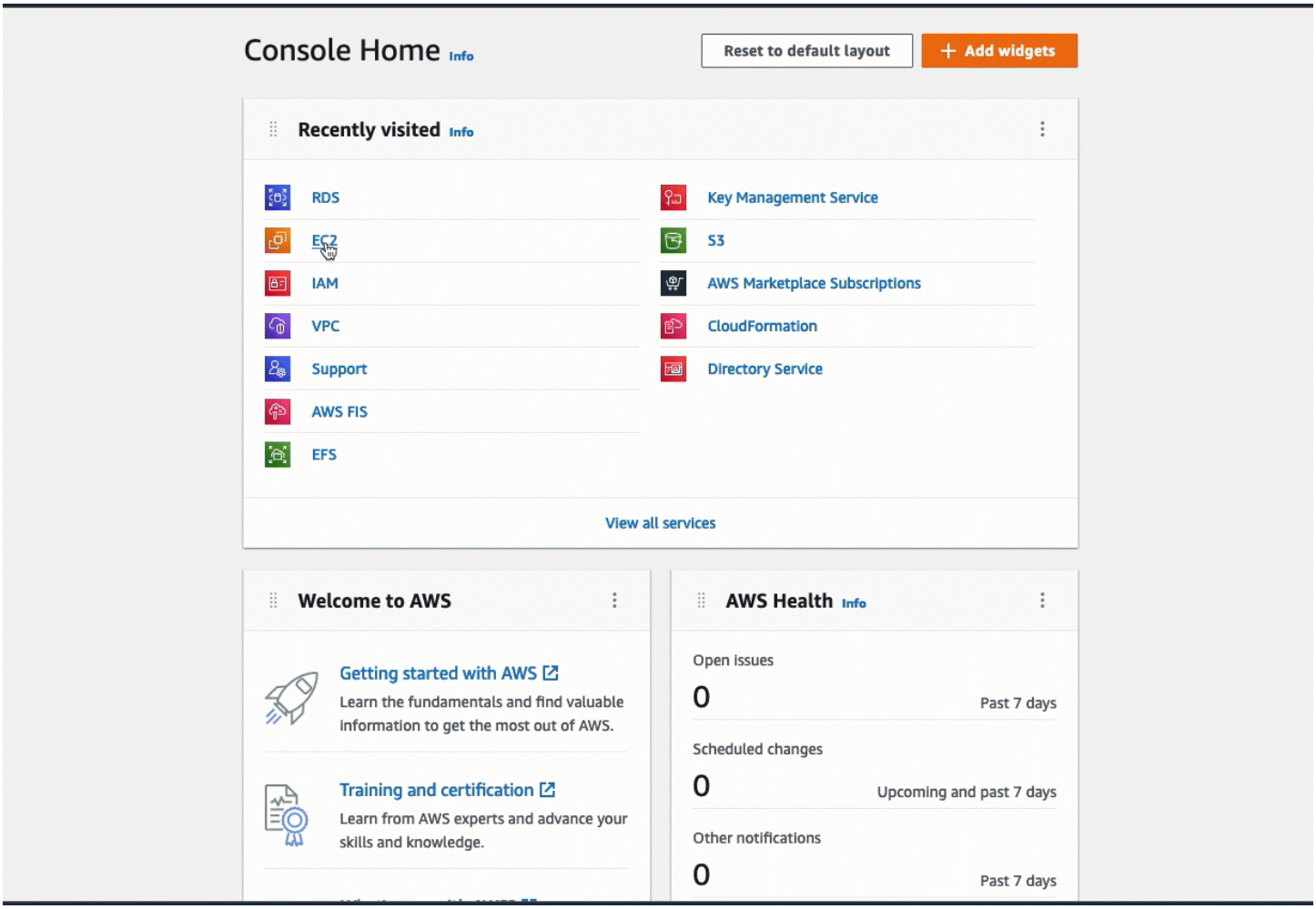
1. Aprire la console Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Nel riquadro di navigazione scegli Database.
3. Scegli il database RDS creato per questo tutorial.
4. Nella scheda Connettività e sicurezza, in Sicurezza, gruppi di sicurezza VPC , verifica che sia visualizzato un gruppo di sicurezza chiamato rds-ec2-. *x*
5. Scegli il gruppo di sicurezza rds-ec2-. *x* Si apre la schermata Gruppi di sicurezza nella console EC2.
6. Scegli il gruppo di sicurezza rds-ec2- *x* per aprirlo.
7. Selezionare la scheda Regole in entrata.
8. Verifica che esista la seguente regola del gruppo di sicurezza, come illustrato di seguito:
   - Tipo: MYSQL/Aurora
   - Intervallo porte: 3306
   - Fonte: ***sg-0987654321example***/ec2-rds- *x* — Questo è il gruppo di sicurezza assegnato all'istanza EC2 verificata nei passaggi precedenti.
   - Descrizione: regola per consentire le connessioni da istanze EC2 con allegato ***sg-1234567890example***
9. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
10. Nel riquadro di navigazione, scegliere Instances (Istanze).

11. Scegli l'istanza EC2 che hai selezionato per connetterti al database RDS nell'operazione precedente e scegli la scheda Security (Sicurezza).
12. In Dettagli di sicurezza, Gruppi di sicurezza, verifica che un gruppo di sicurezza chiamato ec2-rds- ***x*** sia presente nell'elenco. *x* è un numero.
13. Scegli il gruppo di *x* sicurezza ec2-rds- per aprirlo.
14. Scegli la scheda Outbound rules (Regole in uscita).
15. Verifica che esista la seguente regola del gruppo di sicurezza, come illustrato di seguito:

    - Tipo: MYSQL/Aurora
    - Intervallo porte: 3306
    - Destinazione:/rds-ec2- ***sg-1234567890example x***
    - Descrizione: Regola per consentire le connessioni a **`database-tutorial`** da qualsiasi istanza a cui è collegato questo gruppo di sicurezza

Verificando che questi gruppi di sicurezza e le regole dei gruppi di sicurezza esistano e che siano assegnati al database RDS e all'istanza EC2 come descritto in questa procedura, puoi verificare che la connessione sia stata configurata automaticamente utilizzando la funzione di connessione automatica.

Visualizzazione di un'animazione: verifica della configurazione della connessione



Hai completato l'Opzione 2 di questo tutorial. Ora puoi completare l'Opzione 3, che ti spiega come configurare manualmente i gruppi di sicurezza creati automaticamente nell'Opzione 2.

Attività 4 (Facoltativo): Pulire

> **Warning**
>
> La terminazione di un'istanza è permanente e irreversibile.
> Dopo aver terminato un'istanza, non puoi più connetterti a essa e non puoi ripristinarla. Inoltre, tutti i volumi Amazon EBS collegati e configurati per essere eliminati in caso di terminazione vengono eliminati in modo definitivo e non possono essere recuperati. Tutti i dati archiviati nei volumi di archivio dell'istanza vengono persi in modo definitivo. Per ulteriori informazioni, consulta Come funziona la terminazione delle istanze.

Prima di terminare un'istanza, assicurati di aver eseguito il backup di tutti i dati che devi mantenere dopo la terminazione sull'archivio persistente.

Ora che hai completato il tutorial, è buona norma ripulire (eliminare) tutte le risorse che non desideri più utilizzare. La pulizia AWS delle risorse impedisce al tuo account di incorrere in ulteriori addebiti.

Se hai avviato un'istanza EC2 appositamente per questo tutorial, puoi interromperla per non incorrere in alcun addebito correlato a questa.

Per interrompere un'istanza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza creata per questo tutorial, quindi scegli Stato istanza, Termina istanza.
4. Quando viene richiesta la conferma, seleziona Interrompi.

Se hai creato un database RDS appositamente per questo tutorial, puoi interromperlo per non incorrere in alcun addebito correlato a questo.

Eliminazione di un database RDS tramite la console

1. Aprire la console Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Nel pannello di navigazione, seleziona Database.
3. Seleziona il database RDS che hai creato per questo tutorial e scegli Azioni, Elimina.
4. Inserisci **`delete me`** nella casella e scegli Elimina.

Opzione 3: connessione manuale di un'istanza a un database RDS creando dei gruppi di sicurezza

L'obiettivo dell'Opzione 3 è imparare a configurare manualmente la connessione tra un'istanza EC2 e un database RDS riproducendo manualmente la configurazione della funzione di connessione automatica.

Processi

- Prima di iniziare

- Attività 1 (Facoltativo): Avvia un'istanza EC2
- Attività 2 (Facoltativo): Creare un database RDS
- Attività 3: connessione manuale dell'istanza EC2 al database RDS creando gruppi di sicurezza e assegnandoli alle istanze
- Attività 4 (Facoltativo): Pulire

Prima di iniziare

Per completare questo tutorial, avrai bisogno di quanto segue:

- Un'istanza EC2 nello stesso VPC del database RDS. Puoi utilizzare un'istanza EC2 esistente o seguire i passaggi illustrati nell'Attività 1 per creare una nuova istanza.
- un database RDS nello stesso VPC dell'istanza EC2. Puoi utilizzare un database RDS esistente o seguire i passaggi illustrati nell'Attività 2 per creare un nuovo database.
- Autorizzazioni per effettuare le seguenti operazioni:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Attività 1 (Facoltativo): Avvia un'istanza EC2

> **Note**
>
> Il fulcro di questo tutorial non è l'avvio di un'istanza. Se già disponi di un'istanza Amazon EC2 e vorresti utilizzarla in questo tutorial, puoi ignorare questa attività.

L'obiettivo di questa attività è creare un'istanza EC2 in modo da poter completare l'Attività 3 che prevede la configurazione della connessione tra l'istanza EC2 e il database Amazon RDS. I passaggi di questa attività illustrano la configurazione dell'istanza EC2 come segue:

- nome dell'istanza: **`tutorial-instance`**
- AMI: Amazon Linux 2
- tipo di istanza: `t2.micro`
- Auto-assign IP pubblico: abilitato
- gruppo di sicurezza con le tre regole seguenti:
  - Consenti SSH dal tuo indirizzo IP
  - Consenti il traffico HTTPS da qualsiasi luogo
  - Consenti il traffico HTTP da qualsiasi luogo

> **Important**
>
> In un ambiente di produzione, dovrai configurare l'istanza in base alle tue esigenze specifiche.

Per avviare un'istanza EC2

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal dashboard EC2, scegli Avvia istanza.
3. Sotto Nome e tag, per Nome inserisci un nome per identificare l'istanza. Per questo tutorial inserisci l'istanza **`tutorial-instance-manual-1`**. Sebbene il nome dell'istanza non sia obbligatorio, questo ti aiuterà a identificarla facilmente.

4. Sotto Applicazioni e immagini del sistema operativo, scegli un'AMI che soddisfi le esigenze del tuo server web. Questo tutorial utilizza Amazon Linux.
5. Sotto Tipo di istanza, per Tipo di istanza, seleziona un tipo di istanza che soddisfi le esigenze del tuo server web. In questo tutorial si utilizza `t2.micro`.

> **Note**
>
> A seconda di quando hai creato l'account, potresti essere aver diritto a utilizzare Amazon EC2 nell'ambito del piano gratuito.
> Se hai creato la tua Account AWS prima del 15 luglio 2025 e ha meno di 12 mesi, puoi utilizzare Amazon EC2 con il piano gratuito selezionando il tipo di istanza t2.micro o il tipo di istanza t3.micro nelle regioni in cui t2.micro non è disponibile. Tieni presente che quando avvii un'istanza t3.micro, l'impostazione predefinita è la modalità Illimitata, che potrebbe comportare costi aggiuntivi in base all'utilizzo della CPU. Se un tipo di istanza può essere utilizzato nell'ambito del Piano gratuito, è etichettato come Idoneo per il Piano gratuito.
> Se hai creato la tua il Account AWS 15 luglio 2025 o dopo, puoi utilizzare i tipi di istanza t3.micro , t3.small, t4g.micro, t4g.small, c7i-flex.large e m7i-flex.large per 6 mesi o fino all'esaurimento dei crediti.
> Per ulteriori informazioni, consulta Vantaggi del piano gratuito prima e dopo il 15 luglio 2025.

6. Sotto Key pair (login) [Coppia di chiavi (login)], per Key pair name (Nome della coppia di chiavi) scegli la tua coppia di chiavi.
7. Sotto Network settings (Impostazioni di rete) effettua le seguenti operazioni:

   a. Per Rete e Sottorete, se non hai apportato modifiche al VPC o alle sottoreti predefiniti, puoi mantenere le impostazioni predefinite.

      Se hai apportato modifiche al tuo VPC o alle sottoreti predefiniti, controlla quanto segue:

      i. L'istanza deve trovarsi nella stessa VPC del database RDS. Per impostazione predefinita hai a disposizione un solo VPC.

      ii. Il VPC in cui stai avviando l'istanza deve avere un gateway Internet collegato ad esso in modo da poter accedere al tuo server web da Internet. Il tuo VPC predefinito viene configurato automaticamente con un gateway Internet.

iii. Per assicurarti che la tua istanza riceva un indirizzo IP pubblico, per l'IP pubblico, verifica che l'opzione Abilita sia selezionata. Auto-assign Se è selezionato Disabilita, scegli Modifica (a destra di Impostazioni di rete), quindi, per l'IP Auto-assign pubblico, scegli Abilita.

b. Per connettersi all'istanza tramite SSH, è necessaria una regola del gruppo di sicurezza che autorizzi il traffico SSH (Linux) o RDP (Windows) dall'indirizzo IPv4 pubblico del computer. Per impostazione predefinita, quando si avvia un'istanza, viene creato un nuovo gruppo di sicurezza con una regola che consente il traffico SSH in entrata da qualsiasi luogo.

   Per assicurarti che solo il tuo indirizzo IP possa connettersi alla tua istanza, sotto Firewall (gruppi di sicurezza), dall'elenco a discesa accanto alla casella di controllo Consenti traffico SSH da, scegli Il mio IP.

c. Per consentire il traffico da Internet alla tua istanza, seleziona le caselle di controllo seguenti:

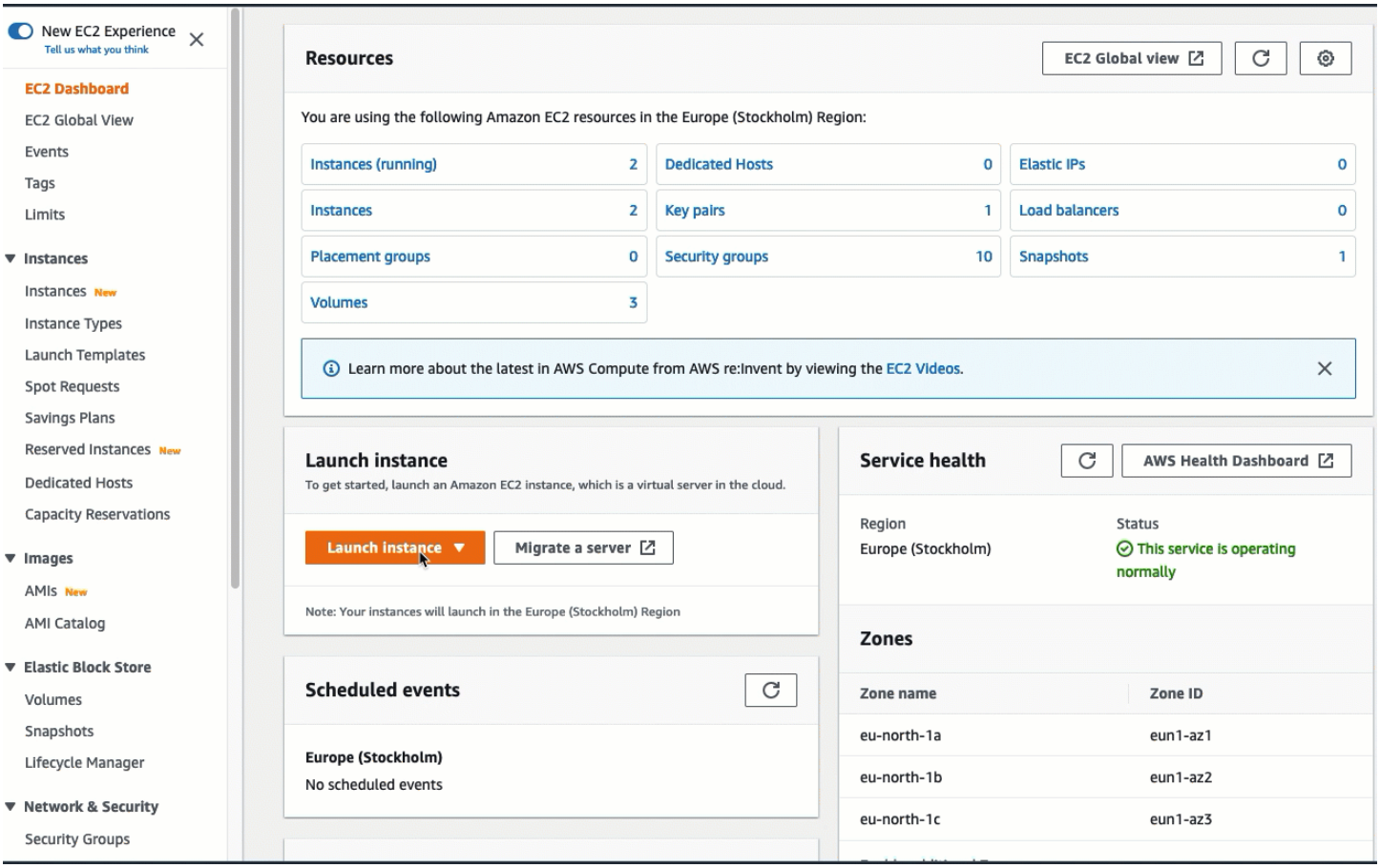
   - Allow HTTPs traffic from the internet (Autorizzare il traffico HTTPS da Internet)
   - Allow HTTP traffic from the internet (Autorizzare il traffico HTTP da Internet)

8. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza).
9. Scegli View Instances (Visualizza istanze) per chiudere la pagina di conferma e tornare alla console. La tua istanza sarà prima in uno stato `pending` e poi passerà allo stato `running`.

   Se l'istanza non riesce ad avviarsi o lo stato passa immediatamente a `terminated` anziché `running`, consultare Risoluzione dei problemi di avvio dell'istanza Amazon EC2.

Per ulteriori informazioni sull'avvio di un'istanza, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

Visualizzazione di un'animazione: avvio di un'istanza EC2



Attività 2 (Facoltativo): Creare un database RDS

> **Note**
>
> Il fulcro di questa parte del tutorial non è la creazione di un database RDS. Se già disponi di un database RDS e vorresti utilizzarlo in questo tutorial, puoi ignorare questa attività.

L'obiettivo di questa attività è creare un database RDS. Potrai utilizzare questa istanza nel corso dell'Attività 3 quando la connetti all'istanza EC2. I passaggi di questa attività illustrano la configurazione del database RDS come segue:

- Tipo di motore: MySQL
- Modello: livello gratuito
- DB Instance Identifier (Identificatore istanze database): **`tutorial-database-manual`**

- DB instance class (Classe istanza database): `db.t3.micro`

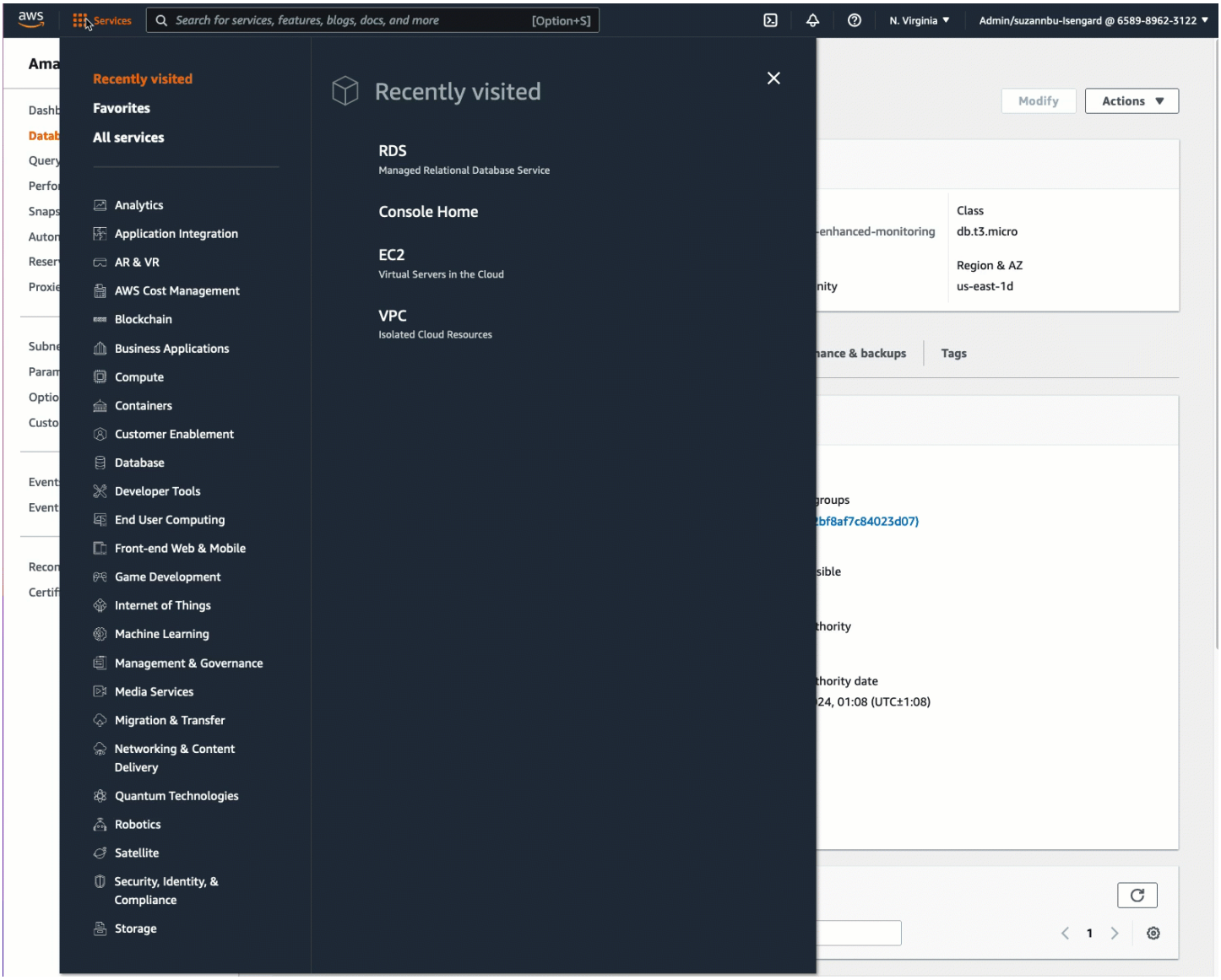
> **Important**
>
> In un ambiente di produzione, dovrai configurare l'istanza in base alle tue esigenze specifiche.

Per creare un'istanza database MySQL

1. Aprire la console Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Dal selettore di regione (in alto a destra), scegli quella Regione AWS in cui hai creato l'istanza EC2. L'istanza EC2 e l'istanza database devono trovarsi nella stessa regione.
3. Sul pannello di controllo seleziona Create database (Crea database).
4. In Choose a database creation method (Seleziona metodo di creazione del database), scegli Standard create (Creazione standard). Quando scegli questa opzione, la funzione di connessione automatica per configurare automaticamente la connessione non è disponibile.
5. Sotto Engine options (Opzioni del motore) per Engine type (Tipo di motore) scegli MySQL.
6. Per Dimensione istanza database, seleziona Piano gratuito.
7. Per il DB instance identifier (Identificatore istanze database) inserire un nome per il database RDS. Per questo tutorial, digita **`tutorial-database-manual`**.
8. Per il Nome utente principale, lascia il nome predefinito, che è **`admin`**.
9. Come Master password (Password principale) inserisci una password per questo tutorial che riesci a ricordare quindi per Confirm password (Conferma password) inserisci nuovamente la password.
10. Scegliere Crea database.

    Nella schermata Databases (Database) lo Status (Stato) dell'istanza database è Creating (Creazione in corso) fino a quando l'istanza database non è pronta per l'uso. Quando lo stato cambia in Available (Disponibile), puoi connettersi all'istanza database. A seconda della classe di istanza database e della quantità di storage, prima che la nuova istanza sia disponibile possono trascorrere fino a 20 minuti.

Visualizzazione di un'animazione: creazione di un'istanza database



Attività 3: connessione manuale dell'istanza EC2 al database RDS creando gruppi di sicurezza e assegnandoli alle istanze

L'obiettivo di questa attività è riprodurre la configurazione della connessione della funzione di connessione automatica eseguendo manualmente quanto segue: crei due nuovi gruppi di sicurezza e quindi aggiungi un gruppo di sicurezza all'istanza EC2 e uno al database RDS.

Creare due nuovi gruppi di sicurezza e assegnare uno all'istanza EC2 e uno al database RDS

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Per prima cosa crea il gruppo di sicurezza per aggiungerlo all'istanza EC2, come indicato di seguito:

   a. Fare clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.

   b. Scegliere Create Security Group (Crea gruppo di sicurezza).

   c. In Security group name (Nome di gruppo di sicurezza) inserisci un nome descrittivo per il gruppo di sicurezza. Per questo tutorial, digita **`ec2-rds-manual-configuration`**.

   d. In Description (Descrizione) inserisci una breve descrizione. Per questo tutorial, digita **`EC2 instance security group to allow EC2 instance to securely connect to RDS database`**.

   e. Scegliere Create Security Group (Crea gruppo di sicurezza). Dopo aver creato il gruppo di sicurezza del database RDS, tornerai a questo gruppo di sicurezza per aggiungere una regola in uscita.

3. Ora crea il gruppo di sicurezza da aggiungere al database RDS, come indicato di seguito:

   a. Fare clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.

   b. Scegliere Create Security Group (Crea gruppo di sicurezza).

   c. In Security group name (Nome di gruppo di sicurezza) inserisci un nome descrittivo per il gruppo di sicurezza. Per questo tutorial, digita **`rds-ec2-manual-configuration`**.

   d. In Description (Descrizione) inserisci una breve descrizione. Per questo tutorial, digita **`RDS database security group to allow EC2 instance to securely connect to RDS database`**.

   e. In Inbound rules (Regole in entrata), scegli Add rule (Aggiungi regola) ed esegui le seguenti operazioni:

      i. In Tipo, scegli MYSQL/Aurora.

      ii. Per Source (Origine), scegli il gruppo di sicurezza dell'istanza EC2 ec2-rds-manual-configuration creato nella Fase 2 di questa procedura.

   f. Scegliere Create Security Group (Crea gruppo di sicurezza).

4. Per aggiungere una regola in uscita, modifica il gruppo di sicurezza dell'istanza EC2, come indicato di seguito:

   a. Fai clic su Gruppi di sicurezza nel riquadro di navigazione.

   b. Seleziona il gruppo di sicurezza dell'istanza EC2 (che hai denominato **`ec2-rds-manual-configuration`**) e scegli la scheda Outbound rules (Regole in uscita).

c. Scegli Edit outbound rules (Modifica regole in uscita).

d. Scegli Add rule (Aggiungi regola) ed esegui le seguenti operazioni:

   i. In Tipo, scegli MYSQL/Aurora.

   ii. Per Destinazione, scegli il gruppo di sicurezza del database RDS Configurazione manuale EC2 RDS creato nella Fase 3 di questa procedura.

   iii. Scegliere Salva regole.

5. Aggiungi il gruppo di sicurezza EC2 all'istanza EC2, come indicato di seguito:

   a. Nel riquadro di navigazione, scegliere Instances (Istanze).

   b. Seleziona l'istanza EC2, quindi scegli Actions (Azioni), Security (Sicurezza), Change security groups (Cambia gruppi di sicurezza).

   c. Sotto Associated security groups (Gruppi di sicurezza associati), scegli il campo Select security groups (Seleziona gruppi di sicurezza), scegli ec2-rds-manual-configuration che hai creato in precedenza, quindi scegli Add security group (Aggiungi gruppo di sicurezza).

   d. Scegli Save (Salva).

6. Aggiungi il gruppo di sicurezza del database RDS al database RDS, come indicato di seguito:

   a. Aprire la console Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.

   b. Nel riquadro di navigazione scegli Databases (Database) quindi seleziona il database.

   c. Scegli Modifica.

   d. Sotto Connectivity (Connettività), per il Security group (Gruppo di sicurezza), scegli rds-ec2-manual-configuration che hai creato in precedenza, quindi scegli Continue (Continua).

   e. Sotto Scheduling of Modifications (Pianificazione delle modifiche) scegli Apply immediately (Applica immediatamente).

   f. Scegliere Modify DB Instance (Modifica istanza database).

   Ora hai completato i passaggi manuali che simulano i passaggi automatici che si verificano quando utilizzi la funzione di connessione automatica.

Hai completato l'Opzione 3 di questo tutorial. Se hai completato le opzioni 1, 2 e 3 e non hai più bisogno delle risorse create in questo tutorial, dovresti eliminarle per evitare di incorrere in costi inutili. Per ulteriori informazioni, consulta Attività 4 (Facoltativo): Pulire.

Attività 4 (Facoltativo): Pulire

> **Warning**
>
> La terminazione di un'istanza è permanente e irreversibile.
> Dopo aver terminato un'istanza, non puoi più connetterti a essa e non puoi ripristinarla. Inoltre, tutti i volumi Amazon EBS collegati e configurati per essere eliminati in caso di terminazione vengono eliminati in modo definitivo e non possono essere recuperati. Tutti i dati archiviati nei volumi di archivio dell'istanza vengono persi in modo definitivo. Per ulteriori informazioni, consulta Come funziona la terminazione delle istanze.
> Prima di terminare un'istanza, assicurati di aver eseguito il backup di tutti i dati che devi mantenere dopo la terminazione sull'archivio persistente.

Ora che hai completato il tutorial, è buona norma ripulire (eliminare) tutte le risorse che non desideri più utilizzare. La pulizia AWS delle risorse impedisce al tuo account di incorrere in ulteriori addebiti.

Se hai avviato un'istanza EC2 appositamente per questo tutorial, puoi interromperla per non incorrere in alcun addebito correlato a questa.

Per interrompere un'istanza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza creata per questo tutorial, quindi scegli Stato istanza, Termina istanza.
4. Quando viene richiesta la conferma, seleziona Interrompi.

Se hai creato un database RDS appositamente per questo tutorial, puoi interromperlo per non incorrere in alcun addebito correlato a questo.

Eliminazione di un database RDS tramite la console

1. Aprire la console Amazon RDS all'indirizzo https://console.aws.amazon.com/rds/.
2. Nel pannello di navigazione, seleziona Database.
3. Seleziona il database RDS che hai creato per questo tutorial e scegli Azioni, Elimina.
4. Inserisci **`delete me`** nella casella e scegli Elimina.

EC2 Fleet e parco istanze spot

Il parco istanze EC2 e il parco istanze spot sono progettati per essere strumenti utili per avviare un parco istanze di decine, centinaia o migliaia di istanze Amazon EC2 in una singola operazione. Ogni istanza in un parco istanze è configurata da un modello di avvio o da un set di parametri di avvio configurabili manualmente al momento dell'avvio.

Argomenti

- Funzionalità e vantaggi
- Qual è il metodo per parco istanze migliore da utilizzare?
- Opzioni di configurazione per il parco istanze EC2 o il parco istanze spot
- Lavorare con un parco istanze EC2
- Lavorare con un parco istanze spot
- Monitoraggio del parco istanze EC2 o del parco istanze spot
- Tutorial per parco istanze EC2
- Esempi di configurazioni di CLI per parco istanze EC2
- Configurazioni CLI di esempi per parco istanze spot
- Quote per il parco istanze EC2 e il parco istanze spot

Funzionalità e vantaggi

I parchi istanze forniscono i vantaggi e le funzionalità seguenti, consentendoti di massimizzare il risparmio sui costi e ottimizzare la disponibilità e le prestazioni durante l'esecuzione di applicazioni su più istanze EC2.

Molteplici tipi di istanze.

Un parco istanze può avviare più tipi di istanze, assicurando che non dipenda dalla disponibilità di un singolo tipo di istanza. Ciò aumenta la disponibilità complessiva delle istanze nel parco istanze.

Distribuzione di istanze tra le zone di disponibilità

Un parco istanze può essere lanciato in più zone di disponibilità, consentendoti di ridurre i costi e migliorare la disponibilità. Se il tuo parco istanze include istanze spot, il parco istanze

seleziona automaticamente le zone di disponibilità in base alle tue preferenze in termini di prezzo e interruzioni.

Molteplici opzioni di acquisto

Una flotta può lanciare più opzioni di acquisto (Spot e On-Demand Instances), consentendoti di ottimizzare i costi tramite l'utilizzo delle istanze Spot. Puoi inoltre usufruire degli sconti sulle istanze riservate e sui piani di risparmio utilizzandoli insieme alle istanze del parco On-Demand istanze.

Sostituzione automatica delle istanze spot

Se il parco istanze include istanze spot, può richiedere automaticamente la sostituzione della capacità spot se le istanze spot vengono interrotte. Grazie al ribilanciamento della capacità, un parco istanze può anche monitorare e sostituire proattivamente le istanze spot sono a un elevato rischio di interruzione.

Capacità di riserva On-Demand

Una flotta può utilizzare una riserva On-Demand di capacità per riservare On-Demand la capacità. Un parco istanze può includere anche blocchi di capacità per ML, che ti consentono di prenotare istanze GPU in una data futura per supportare i carichi di lavoro di machine learning (ML) di breve durata.

Qual è il metodo per parco istanze migliore da utilizzare?

Come best practice generale, consigliamo di lanciare flotte di Spot e On-Demand istanze con Amazon EC2 Auto Scaling perché offre funzionalità aggiuntive che puoi utilizzare per gestire il tuo parco veicoli. L'elenco delle funzionalità aggiuntive include le sostituzioni automatiche dei controlli di integrità sia per Spot che per On-Demand le istanze, controlli dello stato basati sulle applicazioni e un'integrazione con Elastic Load Balancing per garantire una distribuzione uniforme del traffico delle applicazioni verso le istanze integre. Puoi utilizzare i gruppi Auto Scaling anche quando utilizzi AWS servizi come Amazon ECS, Amazon EKS (gruppi di nodi autogestiti) e Amazon VPC Lattice. Per ulteriori informazioni, consulta Guida per l'utente di Amazon EC2 Auto Scaling.

Se non puoi usare Amazon EC2 Auto Scaling, potresti prendere in considerazione l'utilizzo di un parco istanze EC2 o un parco istanze Spot. Il parco istanze EC2 e il parco istanze spot offrono le stesse funzionalità di base. Tuttavia, il parco istanze EC2 è disponibile solo usando una riga di comando e non fornisce supporto della console. Spot Fleet fornisce supporto per console, ma utilizza un'API legacy senza investimenti pianificati.

Utilizza la tabella seguente per determinare quale metodo per parco istanze utilizzare.

Metodo per parco istanze	Quando usarlo?	Caso d'uso
Amazon EC2 Auto Scaling	• Sono necessarie più istanze con una configura zione singola o mista. • Vuoi automatizzare la gestione del ciclo di vita delle istanze.	Crea un gruppo Auto Scaling che gestisce il ciclo di vita delle istanze mantenendo il numero di istanze desiderato. Supporta il dimensionamento orizzonta le (aggiunta di più istanze) tra limiti minimi e massimi specificati.
Parco istanze EC2	• Sono necessarie più istanze con una configura zione singola o mista. • Vuoi gestire autonomam ente il ciclo di vita dell'ista nza. • Se non hai bisogno di dimensionamento automatico, ti consiglia mo di utilizzare un parco istanze EC2 di tipo `instant`.	Crea un `instant` parco di On-Demand istanze e istanze Spot in un'unica operazione, con diverse specifiche di avvio che variano in base al tipo di istanza, all'AMI, alla zona di disponibilità o alla sottorete. La strategia di allocazione delle istanze spot è per impostazi one predefinita `lowest-pr ice` per unità, ma ti consiglia mo di cambiarla in `price-cap acity-optimized` .
Spot Fleet	• Sconsigliamo vivamente di utilizzare Spot Fleet perché utilizza un'API legacy senza investimenti pianificati. • Se vuoi gestire il ciclo di vita dell'istanza, usa piuttosto il parco istanze EC2. • Se non vuoi gestire il ciclo di vita dell'istanza, usa	Usa il parco istanze spot solo se hai bisogno del supporto della console per un caso d'uso in cui utilizzeresti il parco istanze EC2.

Metodo per parco istanze	Quando usarlo?	Caso d'uso
	piuttosto un gruppo Auto Scaling.	

Opzioni di configurazione per il parco istanze EC2 o il parco istanze spot

Durante la pianificazione del parco istanze EC2 o del parco istanze spot, si consiglia di prendere in considerazione le seguenti opzioni al momento di decidere come configurare il proprio Parco istanze.

Opzione di configurazione	Domanda	Documentazione
Tipo di richiesta di parco istanze	Vuoi un parco istanze che invia una richiesta una tantum per la capacità target desiderata, o un parco istanze che mantiene la capacità target nel tempo?	Tipi di richieste del parco istanze EC2 o parco istanze Spot
Spot Instances	Prevedi di includere le istanze spot nel tuo parco istanze? Rivedi le best practice spot e usale quando pianifichi il parco istanze, così potrai effettuare il provisioning delle istanze al prezzo più basso possibile.	Best practice per spot di Amazon EC2
Limite di spesa per il parco istanze	Vuoi limitare quanto pagherai all'ora per il tuo parco istanze?	Imposta un limite di spesa per il Parco istanze EC2 o il parco istanze spot
Tipi di istanza e selezione del tipo di istanza	Vuoi specificare i tipi di istanze nel parco istanze o lasciare che Amazon EC2 selezioni i tipi di istanza che soddisfano i requisiti delle tue applicazioni?	Specifica gli attributi per la selezione del tipo di istanza per il parco del tipo per il parco istanze EC2 o il parco istanze Spot

Opzione di configurazione	Domanda	Documentazione
basata su attributi		
Ponderazione delle istanze	Vuoi assegnare dei pesi a ciascun tipo di istanza per rappresentarne la loro capacità di calcolo e le prestazioni, in modo tale che Amazon EC2 possa selezionare qualsiasi combinazione di tipi di istanza disponibile per soddisfare la capacità target desiderata?	Utilizza la ponderazione delle istanze per gestire i costi e le prestazioni del parco istanze EC2 o del parco istanze spot
Strategie di allocazione	Vuoi decidere se ottimizzare la capacità disponibile, il prezzo o i tipi di istanze da utilizzare per le istanze Spot e le istanze del tuo On-Demand parco istanze?	Utilizza le strategie di allocazione per determinare in che modo EC2 Fleet o Spot Fleet soddisfano Spot e la capacità On-Demand
Ribilanciamento della capacità	Vuoi che il parco istanze sostituisca automaticamente le istanze spot a rischio?	Utilizza il ribilanciamento della capacità nel parco istanze EC2 e nel parco istanze spot per sostituire le istanze spot a rischio
On-Demand Prenotazione della capacità	Desideri riservare la capacità per le On-Demand Istanze della tua flotta?	Usa Capacity Reservations per riservare On-Demand capacità nella flotta EC2

Opzione di configurazione	Domanda	Documentazione
Diversi tipi di prenotazione della capacità	Desideri avviare istanze su più tipi di prenotazione della capacità (prenotazioni di On-Demand capacità, blocchi di capacità per ML e prenotazioni di capacità interrompibili) utilizzando un unico gruppo di risorse per la prenotazione della capacità e, facoltativamente, ricorrere alla capacità? On-Demand	Tutorial: configura la tua flotta EC2 per avviare le istanze in più tipi di prenotazione della capacità utilizzando un gruppo di risorse per la prenotazione della capacità

Tipi di richieste del parco istanze EC2 o parco istanze Spot

> **Note**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Il tipo di richiesta per un parco istanze EC2 o un parco istanze spot determina se la richiesta è sincrona o asincrona e se si tratta di una richiesta una tantum per la capacità di destinazione target o di uno sforzo continuo per mantenere la capacità nel tempo. Quando configuri il tuo parco istanze, devi specificare il tipo di richiesta.

Il parco istanze EC2 e il parco istanze spot offrono due tipi di richieste: `request` e `maintain`. Inoltre, il parco istanze EC2 offre un terzo tipo di richiesta chiamato `instant`.

Tipi di richiesta di parco istanze

`instant` (Solo parco istanze EC2)

Se configuri il tipo di richiesta come `instant`, EC2 Fleet inserisce una richiesta una tantum sincrona per la capacità desiderata. Nella risposta API, restituisce le istanze avviate e fornisce gli errori per le istanze che non è stato possibile avviare. Per ulteriori informazioni, consulta Configurare un parco istanze EC2 di tipo instant.

`request`

Se configuri il tipo di richiesta come `request`, il parco istanze inserisce una richiesta una tantum asincrona per la capacità desiderata. Se la capacità diminuisce a causa delle interruzioni di Spot, il parco istanze non tenta di rifornire Istanze spot e non invia nemmeno richieste in pool di capacità spot alternativi se la capacità non è disponibile. Quando si crea un parco istanze spot di tipo `request` usando la console, deseleziona la casella di spunta Mantieni capacità target.

`maintain` (predefinito)

Se configuri il tipo di richiesta come `maintain`, il parco istanze effettua una richiesta asincrona per la capacità desiderata e mantiene la capacità rifornendo automaticamente le Istanze spot interrotte. Quando si crea un parco istanze spot di tipo `maintain` usando la console, seleziona la casella di spunta Mantieni capacità target.

Configurare un parco istanze EC2 di tipo instant

L'EC2 Fleet di tipo istantaneo è una richiesta una tantum sincrona che effettua un solo tentativo di avviare la capacità desiderata. La risposta dell'API restituisce le istanze avviate, insieme agli errori per quelle istanze che non è stato possibile avviare. L'utilizzo di un EC2 Fleet di tipo istantaneo comporta diversi vantaggi, descritti in questo articolo. Le configurazioni di esempio sono fornite alla fine dell'articolo.

Per i carichi di lavoro che richiedono un'API di solo avvio per avviare le istanze EC2, puoi utilizzare l'API. RunInstances Tuttavia, con RunInstances, puoi avviare solo istanze On-Demand o Istanze Spot, ma non entrambe nella stessa richiesta. Inoltre, quando si utilizzano istanze Spot RunInstances per avviare istanze Spot, la richiesta di istanza Spot è limitata a un tipo di istanza e a una zona di disponibilità. L'istanza ha come obiettivo un pool di capacità spot (un insieme di istanze inutilizzate con lo stesso tipo di istanza e zona di disponibilità). Se il pool di capacità Spot non dispone di una capacità di istanze Spot sufficiente per la richiesta, la RunInstances chiamata ha esito negativo.

Invece di RunInstances utilizzarla per avviare le istanze Spot, ti consigliamo di utilizzare l' CreateFleet API con il `type` parametro impostato su `instant` per ottenere i seguenti vantaggi:

- Avvia le istanze on demand e le istanze spot in una richiesta. Un EC2 Fleet può avviare istanze on demand, istanze spot o entrambe. La richiesta di Istanze spot viene soddisfatta se c'è capacità disponibile e il prezzo massimo all'ora specificato nella richiesta supera il prezzo Spot.
- Aumenta la disponibilità di istanze spot. Utilizzando un EC2 Fleet di tipo `instant`, puoi avviare istanze spot seguendo Best practice di istanze spot con i seguenti vantaggi:

- Best practice di istanze spot: essere flessibili riguardo tipi di istanza e zone di disponibilità.

  Vantaggio: specificando diversi tipi di istanza e zone di disponibilità, aumenti il numero di pool di capacità spot. Ciò offre al servizio Spot maggiori possibilità di trovare e allocare la capacità di calcolo Spot desiderata. Una buona regola è quella di essere flessibili su almeno 10 tipi di istanza per ogni carico di lavoro e assicurarsi che tutte le zone di disponibilità siano configurate per l'utilizzo nel VPC.

- Best practice di istanze spot: utilizzare la strategia di allocazione price-capacity-optimized..

  Vantaggio: la strategia di allocazione `price-capacity-optimized` identifica le istanze dai pool di capacità spot più disponibili, e poi effettua automaticamente il provisioning delle istanze da tali pool con il prezzo più basso. Poiché la capacità dell'istanza spot viene restituita da pool con capacità ottimale, ciò riduce la possibilità che le istanze spot vengano interrotte quando Amazon EC2 recupera la capacità.

- Accedi a un set più ampio di funzionalità. Per i carichi di lavoro che richiedono un'API solo per il lancio e in cui preferisci gestire il ciclo di vita dell'istanza anziché lasciare che EC2 Fleet lo gestisca per te, utilizza il tipo Fleet EC2 anziché l'API. `instant` RunInstances EC2 Fleet offre un set di funzionalità più ampio rispetto RunInstances a, come dimostrato negli esempi seguenti. Per tutti gli altri carichi di lavoro, è consigliabile utilizzare Amazon EC2 Auto Scaling perché fornisce un set di funzionalità più completo per un'ampia gamma di carichi di lavoro, ad esempio applicazioni supportate da ELB, carichi di lavoro containerizzati e processi di elaborazione delle code.

È possibile utilizzare EC2 Fleet di tipo instantaneo per avviare istanze in Blocchi di capacità. Per ulteriori informazioni, consulta Tutorial: Configura il tuo parco istanze EC2 per avviare istanze in Blocchi di capacità.

AWS servizi come Amazon EC2 Auto Scaling e Amazon EMR utilizzano EC2 Fleet of type Instant per avviare istanze EC2.

Prerequisiti per un EC2 Fleet di tipo istantaneo

Per i prerequisiti per la creazione di un EC2 Fleet, consulta Prerequisiti di parco istanze EC2.

Come funziona un EC2 Fleet istantaneo

Quando si utilizza un EC2 Fleet di tipo `instant`, la sequenza degli eventi è la seguente:

1. Configura: configura il tipo di richiesta come. CreateFleet`instant` Per ulteriori informazioni, consulta Creazione di un parco istanze EC2. Dopo aver effettuato la chiamata API, non puoi più modificarla.
2. Richiedere: quando effettui la chiamata API, Amazon EC2 inserisce una richiesta una tantum sincrona per la capacità desiderata.
3. Rispondere: la risposta dell'API restituisce le istanze avviate, insieme agli errori per quelle istanze che non è stato possibile avviare.
4. Descrivere: puoi descrivere il tuo EC2 Fleet, elencare le istanze associate al EC2 Fleet e visualizzare la cronologia del tuo EC2 Fleet.
5. Terminare le istanze: puoi terminare le istanze in qualsiasi momento.
6. Eliminare la richiesta del parco istanze: la richiesta del parco istanze può essere eliminata manualmente o automaticamente:
   - Manuale: Puoi eliminare la richiesta del parco istanze dopo l'avvio delle istanze.

     Un parco istanze `instant` eliminato con istanze in esecuzione non è supportato. Quando elimini un parco istanze `instant`, Amazon EC2 termina automaticamente tutte le sue istanze. Per i parchi istanze con più di 1.000 istanze, la richiesta di eliminazione potrebbe avere esito negativo. Se il tuo parco istanze ha più di 1.000 istanze, termina innanzitutto la maggior parte delle istanze manualmente, lasciandone 1.000 o meno. Poi elimina il parco istanze e le istanze rimanenti verranno terminate automaticamente.
   - Automatico: Amazon EC2 elimina la richiesta del parco istanze qualche tempo dopo che:
     - Le istanze vengono arrestate.
     - Oppure il parco istanze non riesce ad avviare alcuna istanza.

Esempi

Gli esempi seguenti mostrano come utilizzare EC2 Fleet di tipo `instant` per diversi casi d'uso. Per ulteriori informazioni sull'utilizzo dei parametri dell' CreateFleet API EC2, consulta CreateFleetAmazon EC2 API Reference.

Esempi

- Esempio 1: Avvio di istanze spot con la strategia di allocazione ottimizzata per la capacità
- Esempio 2: Avvio di una singola istanza spot con la strategia di allocazione ottimizzata per la capacità
- Esempio 3: Avvio di istanze spot utilizzando la ponderazione di istanza

- Esempio 4: Avvio di istanze spot in una singola zona di disponibilità
- Esempio 5: Avvio di istanze spot di un singolo tipo in una singola zona di disponibilità
- Esempio 6: Avvio di istanze spot solo se è possibile avviare una capacità target minima
- Esempio 7: Avvio di istanze spot solo se è possibile avviare una capacità target minima dello stesso tipo di istanza in una singola zona di disponibilità
- Esempio 8: Avvio di istanze con più modelli di avvio
- Esempio 9: Avvio di istanze spot con una base di istanze on demand
- Esempio 10: Avvio di istanze spot utilizzando una strategia di allocazione ottimizzata per la capacità con una base di istanze on demand che utilizza prenotazioni di capacità e la strategia di allocazione con priorità
- Esempio 11: avvia le istanze Spot utilizzando capacity-optimized-prioritized la strategia di allocazione
- Esempio 12: Specificare un parametro Systems Manager invece di un'ID AMI

Esempio 1: Avvio di istanze spot con la strategia di allocazione ottimizzata per la capacità

L'esempio seguente indica i parametri necessari in un parco istanze EC2 di tipo `instant`: un modello di avvio, una capacità target, un'opzione di acquisto predefinita e sostituzioni del modello di avvio.

- Il modello di avvio viene identificato dal nome e dal numero di versione.
- Le 12 sostituzioni del modello di avvio specificano 4 tipi di istanza e 3 sottoreti differenti, ognuna in una zona di disponibilità separata. Ogni combinazione di tipo di istanza e sottorete definisce un pool di capacità spot, restituendo 12 pool di capacità spot.
- La capacità obiettivo per il parco istanze è 20 istanze.
- L'opzione di acquisto predefinita è `spot`; con questa opzione, il parco istanze tenta di avviare 20 istanze spot nel pool di capacità spot con capacità ottimale per il numero di istanze che si stanno avviando.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
```

```
        "LaunchTemplateSpecification":{
           "LaunchTemplateName":"ec2-fleet-lt1",
           "Version":"$Latest"
        },
        "Overrides":[
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5d.large",
              "SubnetId":"subnet-fae8c380"
```

```
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 2: Avvio di una singola istanza spot con la strategia di allocazione ottimizzata per la capacità

Puoi avviare in modo ottimale un'istanza Spot alla volta effettuando più chiamate di tipo EC2 Fleet API`instant`, impostando il valore su 1. TotalTargetCapacity

L'esempio seguente indica i parametri necessari in un parco istanze EC2 di tipo istantaneo: un modello di avvio, una capacità target, un'opzione di acquisto predefinita e sostituzioni del modello di avvio. Il modello di avvio viene identificato dal nome e dal numero di versione. Le 12 sostituzioni del modello di avvio hanno 4 tipi di istanza e 3 sottoreti differenti, ognuna in una zona di disponibilità separata. La capacità obiettivo per il parco istanze è 1 istanza e l'opzione di acquisto predefinita è Spot, il che comporta il tentativo di avviare un'istanza spot da uno dei 12 pool di capacità spot basati sulla strategia di allocazione ottimizzata per la capacità, per avviare un'istanza spot dal pool di capacità più disponibile.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
```

```
        },
        "Overrides":[
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5d.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"m5d.large",
```

```
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 3: Avvio di istanze spot utilizzando la ponderazione di istanza

Gli esempi seguenti utilizzano la ponderazione d'istanza; questo significa che il prezzo è calcolato a ora per unità anziché a ora per istanza. Ogni configurazione di avvio elenca un tipo di istanza diverso e un peso diverso in base al numero di unità di carico di lavoro che possono essere eseguite sull'istanza, supponendo che un'unità di carico di lavoro richieda 15 GB di memoria e 4 v. CPUs Ad esempio, un m5.xlarge (4 v CPUs e 16 GB di memoria) può eseguire un'unità e ha un peso di 1, m5.2xlarge (8 v CPUs e 32 GB di memoria) può eseguire 2 unità e ha un peso di 2, e così via. La capacità obiettivo totale è impostata su 40 unità. L'opzione di acquisto predefinita è spot e la strategia di allocazione è ottimizzata per la capacità, il che si traduce in 40 m5.xlarge (40 diviso per 1), 20 m5.2xlarge (40 diviso per 2), 10 m5.4xlarge (40 diviso per 4), 5 m5.8xlarge (40 diviso per 8) o un mix dei tipi di istanza con pesi che si sommano alla capacità desiderata sulla base della strategia di allocazione ottimizzata per la capacità.

Per ulteriori informazioni, consulta Utilizza la ponderazione delle istanze per gestire i costi e le prestazioni del parco istanze EC2 o del parco istanze spot.

```
{
   "SpotOptions":{
      "AllocationStrategy":"capacity-optimized"
   },
   "LaunchTemplateConfigs":[
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
```

```
        },
        "Overrides":[
           {
              "InstanceType":"m5.xlarge",
              "SubnetId":"subnet-fae8c380",
              "WeightedCapacity":1
           },
           {
              "InstanceType":"m5.xlarge",
              "SubnetId":"subnet-e7188bab",
              "WeightedCapacity":1
           },
           {
              "InstanceType":"m5.xlarge",
              "SubnetId":"subnet-49e41922",
              "WeightedCapacity":1
           },
           {
              "InstanceType":"m5.2xlarge",
              "SubnetId":"subnet-fae8c380",
              "WeightedCapacity":2
           },
           {
              "InstanceType":"m5.2xlarge",
              "SubnetId":"subnet-e7188bab",
              "WeightedCapacity":2
           },
           {
              "InstanceType":"m5.2xlarge",
              "SubnetId":"subnet-49e41922",
              "WeightedCapacity":2
           },
           {
              "InstanceType":"m5.4xlarge",
              "SubnetId":"subnet-fae8c380",
              "WeightedCapacity":4
           },
           {
              "InstanceType":"m5.4xlarge",
              "SubnetId":"subnet-e7188bab",
              "WeightedCapacity":4
           },
           {
              "InstanceType":"m5.4xlarge",
```

```
                "SubnetId":"subnet-49e41922",
                "WeightedCapacity":4
            },
            {
                "InstanceType":"m5.8xlarge",
                "SubnetId":"subnet-fae8c380",
                "WeightedCapacity":8
            },
            {
                "InstanceType":"m5.8xlarge",
                "SubnetId":"subnet-e7188bab",
                "WeightedCapacity":8
            },
            {
                "InstanceType":"m5.8xlarge",
                "SubnetId":"subnet-49e41922",
                "WeightedCapacity":8
            }
         ]
      }
   ],
   "TargetCapacitySpecification":{
      "TotalTargetCapacity":40,
      "DefaultTargetCapacityType":"spot"
   },
   "Type":"instant"
}
```

Esempio 4: Avvio di istanze spot in una singola zona di disponibilità

È possibile configurare un parco istanze per avviare tutte le istanze in un'unica zona di disponibilità impostando le opzioni Spot su true. SingleAvailabilityZone

Le 12 sostituzioni del modello di avvio hanno tipi di istanza e sottoreti differenti, ognuna in una zona di disponibilità separata ma con la stessa capacità ponderata. La capacità obiettivo totale è di 20 istanze, l'opzione d'acquisto predefinita è spot e la strategia di allocazione spot è ottimizzata per la capacità. Il parco istanze EC2 avvia 20 istanze spot, tutte in una singola zona di disponibilità, dai pool di capacità spot con capacità ottimale, utilizzando le specifiche di avvio.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleAvailabilityZone": true
```

```
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
```

```
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 5: Avvio di istanze spot di un singolo tipo in una singola zona di disponibilità

Puoi configurare un parco istanze per avviare tutte le istanze dello stesso tipo e in un'unica zona di disponibilità impostando SpotOptions SingleInstanceType true e SingleAvailabilityZone true.

Le 12 sostituzioni del modello di avvio hanno tipi di istanza e sottoreti differenti, ognuna in una zona di disponibilità separata ma con la stessa capacità ponderata. La capacità obiettivo totale è di 20 istanze, l'opzione d'acquisto predefinita è spot, la strategia di allocazione spot è ottimizzata per la capacità. Il parco istanze EC2 avvia 20 istanze spot dello stesso tipo, tutte in una singola zona di disponibilità, dal pool di istanze spot con capacità ottimale, utilizzando le specifiche di avvio.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
```

```
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
```

```
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 6: Avvio di istanze spot solo se è possibile avviare una capacità target minima

Puoi configurare un parco istanze per avviare le istanze solo se è possibile avviare la capacità target minima impostando le opzioni Spot sulla MinTargetCapacity capacità target minima che desideri avviare insieme.

Quando si specifica MinTargetCapacity, è necessario specificare almeno uno di questi parametri: SingleInstanceType o. SingleAvailabilityZone In questo esempio, SingleInstanceType viene specificato, in modo che tutte le 20 istanze debbano utilizzare lo stesso tipo di istanza.

Le 12 sostituzioni del modello di avvio hanno tipi di istanza e sottoreti differenti, ognuna in una zona di disponibilità separata ma con la stessa capacità ponderata. La capacità obiettivo totale e la capacità obiettivo minima sono entrambe impostate su 20 istanze, l'opzione di acquisto predefinita è spot e la strategia di allocazione spot è ottimizzata per la capacità. Il parco istanze EC2 avvia 20 istanze spot dal pool di capacità spot con capacità ottimale utilizzando le sostituzioni del modello di avvio, solo se è in grado di avviare tutte e 20 le istanze contemporaneamente.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
```

```
        "LaunchTemplateSpecification":{
           "LaunchTemplateName":"ec2-fleet-lt1",
           "Version":"$Latest"
        },
        "Overrides":[
           {
              "InstanceType":"c5.4xlarge",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5.4xlarge",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5.4xlarge",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"c5d.4xlarge",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5d.4xlarge",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5d.4xlarge",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5.4xlarge",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"m5.4xlarge",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"m5.4xlarge",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5d.4xlarge",
              "SubnetId":"subnet-fae8c380"
```

```
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 7: Avvio di istanze spot solo se è possibile avviare una capacità target minima dello stesso tipo di istanza in una singola zona di disponibilità

È possibile configurare un parco istanze per avviare le istanze solo se la capacità target minima può essere avviata con un singolo tipo di istanza in un'unica zona di disponibilità impostando le opzioni MinTargetCapacity Spot sulla capacità target minima che si desidera avviare insieme alle opzioni SingleInstanceType e SingleAvailabilityZone .

Le 12 specifiche di avvio che sostituiscono il modello di avvio hanno tipi di istanza e subnet differenti, ognuna in una zona di disponibilità separata ma con la stessa capacità ponderata. La capacità target totale e la capacità target minima sono entrambe impostate su 20 istanze, l'opzione di acquisto predefinita è spot, la strategia di allocazione Spot è ottimizzata in termini di capacità, questo è vero ed è vero. SingleInstanceType SingleAvailabilityZone Il parco istanze EC2 avvia 20 istanze spot dello stesso tipo, tutte in una singola zona di disponibilità, dal pool di istanze spot con capacità ottimale, utilizzando le specifiche di avvio, solo se è possibile avviare tutte e 20 le istanze contemporaneamente.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 20
```

```
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
```

```
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 8: Avvio di istanze con più modelli di avvio

Puoi configurare un parco istanze per avviare istanze con specifiche di avvio diverse per tipi di istanza o gruppi di tipi di istanza diversi, specificando più modelli di avvio. In questo esempio vogliamo avere dimensioni del volume EBS diverse per diversi tipi di istanza e abbiamo ciò che è configurato nei modelli di avvio ec2-fleet-lt-4xl, ec2-fleet-lt-9xl e ec2-fleet-lt-18xl.

In questo esempio, stiamo utilizzando 3 diversi modelli di avvio per i 3 tipi di istanza, in base alle loro dimensioni. Le sostituzioni delle specifiche di avvio su tutti i modelli di avvio utilizzano i pesi delle istanze in base alle vCPU del tipo di istanza. La capacità obiettivo totale è di 144 unità, l'opzione d'acquisto predefinita è spot e la strategia di allocazione spot è ottimizzata per la capacità. Il parco istanze EC2 può avviare 9 c5n.4xlarge (144 diviso per 16) utilizzando il modello di avvio ec2-fleet-4xl o 4 c5n.9xlarge (144 diviso per 36) utilizzando il modello di avvio ec2-fleet-9xl o 2 c5n.18xlarge (144 diviso per 72) utilizzando il modello di avvio ec2-fleet-18xl o un mix dei tipi di istanza con pesi si sommano alla capacità desiderata, in base alla strategia di allocazione ottimizzata per la capacità.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
```

```
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-18xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":72
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-9xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":36
            },
            {
               "InstanceType":"c5n.9xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":36
```

```
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-4xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":16
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 144,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 9: Avvio di istanze spot con una base di istanze on demand

L'esempio seguente specifica la capacità target totale di 20 istanze per il parco istanze e una capacità target di 5 istanze on demand. L'opzione di acquisto predefinita è spot. Il parco istanze avvia 5 istanze on demand come indicato, ma deve avviare altre 15 istanze per soddisfare la capacità target totale. L'opzione di acquisto per la differenza è calcolata come TotalTargetCapacity — OnDemandTargetCapacity = DefaultTargetCapacityType, il che fa sì che la flotta lanci 15 istanze

Spot costituiscano uno dei 12 pool di capacità Spot in base alla strategia di allocazione ottimizzata per la capacità.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
```

```
                "InstanceType":"m5.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 10: Avvio di istanze spot utilizzando una strategia di allocazione ottimizzata per la capacità con una base di istanze on demand che utilizza prenotazioni di capacità e la strategia di allocazione con priorità

È possibile configurare una flotta in modo che utilizzi innanzitutto le prenotazioni di capacità on demand al momento del lancio di una base di istanze on demand con il tipo di capacità target predefinito come spot impostando la strategia di utilizzo per Capacity Reservations su. use-capacity-reservations-first E se più pool di istanze presentano prenotazioni di capacità inutilizzate, viene applicata la strategia di allocazione on demand scelta. In questo esempio, la strategia di allocazione on demand ha la priorità.

In questo esempio, ci sono 6 prenotazioni della capacità disponibili non utilizzate. Questa capacità è inferiore alla capacità target on demand del parco istanze di 10 istanze on demand.

L'account presenta le seguenti 6 prenotazioni della capacità inutilizzate in 2 pool. Il numero di Prenotazioni di capacità in ogni pool è indicato da AvailableInstanceCount.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

La seguente configurazione del parco istanze mostra solo le configurazioni pertinenti per questo esempio. La strategia di allocazione On-Demand ha la priorità, mentre la strategia di utilizzo per Capacity Reservations è. use-capacity-reservations-first La strategia di allocazione spot è ottimizzata per la capacità. La capacità obiettivo totale è 20, la capacità obiettivo on demand è 10 e il tipo di capacità obiettivo predefinito è spot.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "OnDemandOptions":{
       "CapacityReservationOptions": {
         "UsageStrategy": "use-capacity-reservations-first"
       },
       "AllocationStrategy":"prioritized"
    },
```

```
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 5.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 6.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 7.0
            },
            {
               "InstanceType":"m5.large",
```

```
                "SubnetId":"subnet-e7188bab",
                "Priority": 8.0
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-49e41922",
                "Priority": 9.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-fae8c380",
                "Priority": 10.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab",
                "Priority": 11.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922",
                "Priority": 12.0
            }
        ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 10,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Dopo aver creato il parco istanze istantaneo utilizzando la configurazione precedente, le seguenti 20 istanze vengono avviate per soddisfare la capacità target:

- 7 istanze on demand c5.large in us-east-1a: le istanze c5.large in us-east-1a hanno la massima priorità e sono disponibili 3 prenotazioni della capacità c5.large inutilizzate. Le prenotazioni della capacità vengono utilizzate innanzitutto per avviare 3 istanze on demand più 4 ulteriori istanza on demand che vengono avviate secondo la strategia di allocazione on demand, che in questo esempio ha la priorità.

- 3 istanze On-Demand m5.large in us-east-1a — m5.large in us-east-1a ha la priorità al secondo posto e sono disponibili 3 prenotazioni di capacità m5.large non utilizzate.
- 10 istanze spot da uno dei 12 pool di capacità spot con capacità ottimale in base alla strategia di allocazione ottimizzata per la capacità.

Dopo il lancio della flotta, puoi correre per vedere quante prenotazioni di capacità non utilizzate sono rimaste. describe-capacity-reservations In questo esempio, dovresti vedere la seguente risposta, che mostra che sono state utilizzate tutte le prenotazioni della capacità c5.large e m5.large.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "AvailableInstanceCount": 0
}
```

Esempio 11: avvia le istanze Spot utilizzando capacity-optimized-prioritized la strategia di allocazione

L'esempio seguente indica i parametri necessari in un parco istanze EC2 di tipo istantaneo: un modello di avvio, una capacità target, un'opzione di acquisto predefinita e sostituzioni del modello di avvio. Il modello di avvio viene identificato dal nome e dal numero di versione. Le 12 specifiche di avvio che sostituiscono il modello di avvio hanno 4 tipi di istanza diversi con una priorità assegnata e 3 sottoreti diverse, ognuna in una zona di disponibilità separata. La capacità target per il parco istanze è di 20 istanze e l'opzione di acquisto predefinita è spot, in base alla quale il parco istanze tenta di lanciare 20 istanze Spot da uno dei 12 pool di capacità Spot in base alla strategia di capacity-optimized-prioritized allocazione, che implementa le priorità con il massimo impegno, ma ottimizza innanzitutto la capacità.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
```

```
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 2.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 3.0
            },
```

```
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 4.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 4.0
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 12: Specificare un parametro Systems Manager invece di un'ID AMI

L'esempio seguente utilizza un modello di avvio per specificare la configurazione per le istanze nel parco istanze. In questo esempio, per `ImageId`, anziché specificare un ID AMI, all'AMI viene fatto riferimento con un parametro System Manager. All'avvio dell'istanza, il parametro Systems Manager si risolverà in un ID AMI.

In questo esempio, il parametro Systems Manager è specificato in un formato valido: `resolve:ssm:golden-ami`. Vi sono altri formati validi per il parametro Systems Manager. Per ulteriori informazioni, consulta Usare un parametro Systems Manager invece di un'ID AMI.

> **Note**
>
> Il tipo di parco istanze deve essere di tipo `instant`. Altri tipi di parco istanze non supportano la specificazione di un parametro System Manager anziché un ID AMI.

```
{
    "LaunchTemplateData": {
        "ImageId": "resolve:ssm:golden-ami",
        "InstanceType": "m5.4xlarge",
        "TagSpecifications": [{
            "ResourceType": "instance",
            "Tags": [{
                "Key": "Name",
                "Value": "webserver"
            }]
        }]
    }
}
```

Imposta un limite di spesa per il Parco istanze EC2 o il parco istanze spot

Puoi impostare un limite su quanto sei disposto a spendere all'ora nel parco istanze EC2 o nel parco istanze spot. Una volta raggiunto il limite di spesa, il parco istanze interrompe l'avvio delle istanze, anche se la capacità target non è stata raggiunta.

Esistono limiti di spesa separati per le istanze e le On-Demand istanze Spot.

Per configurare un limite di spesa per On-Demand le istanze e le istanze Spot della tua flotta EC2

Utilizza il comando create-fleet e i seguenti parametri:

- Per On-Demand le istanze: nella `OnDemandOptions` struttura, specifica il limite di spesa nel campo. `MaxTotalPrice`
- Per le istanze spot: nella struttura `SpotOptions`, specifica il limite di spesa nel campo `MaxTotalPrice`.

Per configurare un limite di spesa per On-Demand le istanze e le istanze Spot nel tuo parco istanze Spot

Puoi utilizzare la console Amazon EC2 o la AWS CLI per configurare il limite di spesa.

(Console) Quando crei il parco istanze spot, seleziona la casella di spunta Imposta il costo massimo per le istanze Spot, poi inserisci un valore per Imposta il costo massimo (all'ora). Per ulteriori informazioni, consulta la fase 6.e. in Crea una richiesta di parco istanze spot utilizzando parametri definiti.

(AWS CLI) Utilizza il comando request-spot-fleet e i seguenti parametri:

- Per On-Demand le istanze: specifica il limite di spesa nel `OnDemandMaxTotalPrice` campo.
- Per le istanze spot: specifica il limite di spesa nel campo `SpotMaxTotalPrice`.

Esempi

I seguenti esempi illustrano due scenari diversi. Nel primo esempio, il parco istanze smette di lanciare On-Demand istanze quando ha raggiunto la capacità target impostata per On-Demand Instances (). `OnDemandTargetCapacity` Nel secondo esempio, il parco istanze smette di lanciare On-Demand Istanze quando ha raggiunto l'importo massimo che sei disposto a pagare all'ora per le Istanze (). On-Demand `MaxTotalPrice`

Esempio: interrompi l'avvio delle On-Demand istanze quando viene raggiunta la capacità prevista

Data una richiesta di `m4.large` On-Demand istanze, dove:

- On-Demand Prezzo: 0,10 USD all'ora
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 1,50 USD

Il parco istanze lancia 10 On-Demand istanze perché il totale di 1,00 USD (10 istanze x 0,10 USD) non supera quello di 1,50 USD per le Istanze. `MaxTotalPrice` On-Demand

Esempio: interrompi il lancio delle istanze quando viene raggiunto il prezzo totale massimo On-Demand

Data una richiesta di `m4.large` On-Demand Istanze, in cui:

- On-Demand Prezzo: 0,10 USD all'ora
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 0,80 USD

Se la flotta raggiungesse la capacità On-Demand prevista (10 On-Demand istanze), il costo orario totale sarebbe di 1,00 USD. Si tratta di un importo superiore all'importo (0,80 USD) specificato per For Instances. `MaxTotalPrice` On-Demand Per evitare di spendere più di quanto sei disposto a pagare, il parco istanze lancia solo 8 On-Demand istanze (al di sotto della capacità On-Demand prevista) perché il lancio di più istanze supererebbe le quattro istanze. `MaxTotalPrice` On-Demand

Istanze a prestazioni espandibili

Se avvii le tue istanze spot utilizzando un tipo di istanza a prestazioni espandibili, e prevedi di utilizzare immediatamente le istanze spot a prestazioni espandibili per un breve periodo, senza alcun tempo di inattività per accumulare crediti CPU, suggeriamo di avviarla in Modalità Standard in modo da evitare costi più elevati. Se avvii le istanze spot a prestazioni espandibili in Modalità Illimitata ed espandi la capacità di CPU immediatamente, l'espansione implicherà il dispendio dei crediti in più. Se l'istanza viene utilizzata per un periodo di tempo limitato, non riesce ad accumulare crediti CPU per ripagare i crediti extra, che i vengono quindi addebitati al termine dell'istanza.

La modalità illimitata è adatta per la Istanze spot con prestazioni burstable solo se l'istanza viene eseguita per un periodo di tempo sufficiente ad accumulare i crediti CPU per l'espansione. In caso contrario, il pagamento di crediti in eccedenza rende le prestazioni Istanze spot espandibili più costose rispetto all'utilizzo di altre istanze. Per ulteriori informazioni, consulta Quando utilizzare la modalità illimitata rispetto alla CPU fissa.

I crediti di avvio hanno lo scopo di fornire un'esperienza di avvio iniziale produttiva per le istanze T2, fornendo risorse di calcolo sufficienti per configurare l'istanza. Non sono consentiti avvii ripetuti di istanze T2 per accedere a nuovi crediti di avvio. Se occorre una CPU duratura, è possibile guadagnare crediti (rimanendo inattivi per un certo periodo) utilizzando la Unlimited mode (Modalità Illimitata) per istanze spot T2 o un tipo di istanza con una CPU dedicata.

Specifica gli attributi per la selezione del tipo di istanza per il parco del tipo per il parco istanze EC2 o il parco istanze Spot

Quando si crea una flotta EC2 o una flotta Spot, è necessario specificare uno o più tipi di istanze per configurare On-Demand le istanze e le istanze Spot della flotta. In alternativa alla specifica manuale dei tipi di istanza, è possibile specificare gli attributi che un'istanza deve avere e Amazon EC2 identificherà tutti i tipi di istanza con tali attributi. Questo è noto come selezione del tipo di istanza basata su attributi. Ad esempio, puoi specificare il numero minimo e massimo di vCPU richieste per le istanze e il parco istanze avvierà le istanze utilizzando qualsiasi tipo di istanza disponibile che soddisfi i requisiti di tali vCPU.

Attribute-based La selezione del tipo di istanza è ideale per carichi di lavoro e framework che possono essere flessibili sui tipi di istanze da utilizzare, ad esempio durante l'esecuzione di container o flotte web, l'elaborazione di big data e l'implementazione di strumenti di integrazione e distribuzione continua (). CI/CD

Vantaggi

Attribute-based la selezione del tipo di istanza presenta i seguenti vantaggi:

- Usa facilmente i tipi di istanza giusti – Con un numero così elevato di tipi di istanza disponibili, trovare i tipi di istanza adatti per il proprio carico di lavoro può richiedere molto tempo. Quando si specificano gli attributi dell'istanza, i tipi di istanza avranno automaticamente gli attributi richiesti per il carico di lavoro.
- Configurazione semplificata – Per specificare manualmente più tipi di istanza per un parco istanze, è necessario creare un modello di avvio separato per ogni tipo di istanza. Tuttavia, con la selezione del tipo di istanza basata su attributi, per fornire più tipi di istanza è necessario specificare solo gli attributi dell'istanza nel modello di avvio o in una sostituzione di un modello di avvio.
- Uso automatico di nuovi tipi di istanza – Quando si specificano gli attributi di istanza anziché i tipi di istanza, il parco istanze può utilizzare tipi di istanza di nuova generazione man mano che vengono rilasciati: una configurazione del parco istanze "a prova di futuro".
- Flessibilità del tipo di istanza – Quando specifichi gli attributi dell'istanza anziché i tipi di istanza, il parco istanze può selezionare da un'ampia gamma di tipi di istanza per l'avvio di istanze spot che aderiscono alla Best practice delle istanze spot per la flessibilità dei tipi di istanza.

Argomenti

- Come funziona la selezione del tipo di istanza basata su attributi
- Protezione del prezzo
- Protezione delle prestazioni
- Considerazioni
- Creazione di un EC2 Fleet con la selezione del tipo di istanza basata su attributi
- Creazione di una serie di istanze spot con la selezione del tipo di istanza basata su attributi
- Esempi di configurazioni del parco istanze EC2 che sono valide e non valide
- Esempi di configurazioni del parco istanze spot che sono valide e non valide
- Anteprima di tipi di istanza con attributi specificati

Come funziona la selezione del tipo di istanza basata su attributi

Per utilizzare la selezione del tipo di istanza basata su attributi nella configurazione del parco istanze, è necessario sostituire l'elenco dei tipi di istanza con un elenco di attributi di istanza richiesti dalle istanze. Il parco istanze EC2 o il parco istanze spot avvierà le istanze su qualsiasi tipo di istanza disponibile con gli attributi di istanza specificati.

Argomenti

- Tipi di attributi di istanza
- Dove configurare la selezione del tipo di istanza basata su attributi
- Come il parco istanze EC2 o il parco istanze spot utilizza la selezione del tipo di istanza basata su attributi durante il provisioning di un parco istanze

Tipi di attributi di istanza

Esistono diversi attributi di istanza che è possibile specificare per esprimere i requisiti di calcolo, come ad esempio:

- Numero di vCPU – Il numero minimo e massimo di vCPU per istanza.
- Memoria: la memoria minima e massima GiBs per istanza.
- Archiviazione locale – Se utilizzare EBS o i volumi di archivio dell'istanza per l'archiviazione locale.
- Prestazioni espandibili – Se utilizzare la famiglia di istanze T, inclusi i tipi T4g, T3a, T3 e T2.

Per una descrizione di ciascun attributo e dei valori predefiniti, consulta InstanceRequirements l'API Reference di Amazon EC2.

Dove configurare la selezione del tipo di istanza basata su attributi

A seconda che utilizzi la console o il AWS CLI, puoi specificare gli attributi dell'istanza per la selezione del tipo di istanza basata sugli attributi come segue:

Nella console è possibile specificare gli attributi di istanza nei seguenti componenti di configurazione del parco istanze:

- In un modello di avvio, facendo successivamente riferimento al modello di avvio nella richiesta del parco istanze
- (Solo parco istanze spot) Nella richiesta del parco istanze

In AWS CLI, è possibile specificare gli attributi delle istanze in uno o tutti i seguenti componenti di configurazione del parco veicoli:

- In un modello di avvio, facendo successivamente riferimento al modello di avvio nella richiesta del parco istanze
- In una sostituzione del modello di avvio

  Se si desidera un mix di istanze che utilizzano AMI diverse, è possibile specificare gli attributi di istanza in più sostituzioni di modelli di avvio. Ad esempio, diversi tipi di istanza possono utilizzare x86 e Arm-based processori.
- (Solo parco istanze spot) In una specifica di avvio

Come il parco istanze EC2 o il parco istanze spot utilizza la selezione del tipo di istanza basata su attributi durante il provisioning di un parco istanze

Il parco istanze EC2 o il parco istanze spot fornisce un parco istanze nel seguente modo:

- Identifica i tipi di istanza che hanno gli attributi specificati.
- Utilizza la protezione dei prezzi per determinare quali tipi di istanza escludere.
- Determina i pool di capacità da cui prenderà in considerazione l'avvio delle istanze in base alle AWS regioni o alle zone di disponibilità con tipi di istanza corrispondenti.
- Applica la strategia di allocazione specificata per determinare da quali pool di capacità avviare le istanze.

  Notare che la selezione del tipo di istanza basata su attributi non sceglie i pool di capacità da cui effettuare il provisioning del parco istanze; questo è il compito delle strategie di allocazione.

  Se si specifica una strategia di allocazione, il parco istanze avvierà le istanze in base alla strategia di allocazione specificata.
  - Per le istanze spot, la selezione del tipo di istanza basata su attributi supporta le strategie di allocazione con ottimizzazione per prezzo e capacità, ottimizzazione per capacità e prezzo più basso. Non consigliamo la strategia di allocazione spot con prezzo più basso perché presenta il rischio di interruzione più elevato per le tue istanze spot.
  - Per On-Demand le istanze, la selezione del tipo di istanza basata sugli attributi supporta la strategia di allocazione dei prezzi più bassa.
- Se non è presente alcuna capacità per i tipi di istanza con gli attributi di istanza specificati, non è possibile avviare le istanze e il parco istanze restituisce un errore.

Protezione del prezzo

La protezione dei prezzi è una funzione che impedisce al proprio parco istanze EC2 o parco istanze spot di utilizzare tipi di istanza troppo costosi anche se si adattano agli attributi specificati. Per utilizzare la protezione del prezzo, devi impostare una soglia di prezzo. Poi, quando Amazon EC2 seleziona i tipi di istanza con i tuoi attributi, esclude i tipi di istanza con un prezzo più alto di quanto definito dalla soglia.

Il modo in cui Amazon EC2 calcola la soglia di prezzo è il seguente:

- Amazon EC2 identifica innanzitutto il tipo di istanza con il prezzo più basso tra quelle che corrispondono ai tuoi attributi.
- Poi, Amazon EC2 prende il valore (espresso in percentuale) da te specificato per il parametro di protezione del prezzo e lo moltiplica per il prezzo del tipo di istanza identificato. Il risultato è il prezzo utilizzato come soglia di prezzo.

Esistono soglie di prezzo separate per le istanze e le istanze Spot. On-Demand

Quando sia crea un parco istanze con selezione del tipo di istanza basata su attributi, la protezione dei prezzi è abilitata per impostazione predefinita. Puoi mantenere i valori predefiniti o specificarne uno personalizzato.

Puoi anche disattivare la protezione del prezzo. Per non indicare alcuna soglia di protezione del prezzo, specifica un valore percentuale elevato, come 999999.

Argomenti

- Come viene identificato il tipo di istanza con prezzo più basso
- On-Demand Protezione del prezzo delle istanze
- Protezione del prezzo dell'istanza spot
- Specifica la soglia di protezione del prezzo

Come viene identificato il tipo di istanza con prezzo più basso

Amazon EC2 determina il prezzo su cui basare la soglia di prezzo identificando il tipo di istanza con il prezzo più basso tra quelle che corrispondono ai tuoi attributi specificati. Ciò avviene come indicato di seguito:

- Per prima cosa, esamina i tipi di istanza C, M o R dell'attuale generazione che corrispondono ai tuoi attributi. Se trova corrispondenze, identifica il tipo di istanza con il prezzo più basso.
- Se non vi sono corrispondenze, esamina poi i tipi di istanza dell'attuale generazione che corrispondono ai tuoi attributi. Se trova corrispondenze, identifica il tipo di istanza con il prezzo più basso.
- Se non vi sono corrispondenze, esamina tutti i tipi di istanza della generazione precedente che corrispondono ai tuoi attributi e identifica il tipo di istanza con il prezzo più basso.

On-Demand Protezione del prezzo delle istanze

La soglia di protezione del prezzo per i tipi di On-Demand istanza è calcolata in percentuale superiore al tipo di On-Demand istanza con il prezzo più basso identificato (`OnDemandMaxPricePercentageOverLowestPrice`). Specifichi la percentuale più alta che sei disposto a pagare. Se non specifichi questo parametro, viene utilizzato un valore predefinito di `20` per calcolare una soglia di protezione del prezzo del 20% superiore al prezzo identificato.

Ad esempio, se il prezzo dell' On-Demand istanza identificato è`0.4271`, e lo specifichi`25`, la soglia di prezzo è superiore `0.4271` del 25%. Viene calcolato come indicato di seguito: `0.4271 * 1.25 = 0.533875`. Il prezzo calcolato è il massimo che sei disposto a pagare per On-Demand le istanze e, in questo esempio, Amazon EC2 escluderà tutti i tipi di On-Demand istanze che costano più di. `0.533875`

Protezione del prezzo dell'istanza spot

Per impostazione predefinita, Amazon EC2 applicherà automaticamente una protezione del prezzo ottimale dell'istanza spot per scegliere in modo coerente tra un'ampia gamma di tipi di istanza. Puoi anche impostare manualmente la protezione del prezzo. Tuttavia, lasciarlo fare ad Amazon EC2 può aumentare la probabilità che la tua capacità Spot venga soddisfatta.

Puoi specificare manualmente la protezione del prezzo utilizzando una delle seguenti opzioni. Se imposti manualmente la protezione del prezzo, ti consigliamo di usare la prima opzione.

- Una percentuale del tipo di On-Demand istanza con il prezzo più basso identificato [] `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`

  Ad esempio, se il prezzo del tipo di On-Demand istanza identificato è`0.4271`, e lo specifichi`60`, la soglia di prezzo è pari al 60% del `0.4271` prezzo. Viene calcolato come indicato di seguito: `0.4271 * 0.60 = 0.25626`. Il prezzo calcolato è il massimo che sei disposto a pagare per le

istanze spot e, in questo esempio, Amazon EC2 escluderà qualsiasi tipo di istanza spot che costa più di `0.25626`.

- Una percentuale superiore al tipo di istanza spot con prezzo più basso identificato [`SpotMaxPricePercentageOverLowestPrice`]

  Ad esempio, se il prezzo del tipo di istanza Spot identificato è `0.1808`, e tu specifichi `25`, la soglia di prezzo è superiore del 25% rispetto a `0.1808`. Viene calcolato come indicato di seguito: `0.1808 * 1.25 = 0.226`. Il prezzo calcolato è il massimo che sei disposto a pagare per le istanze spot e, in questo esempio, Amazon EC2 escluderà qualsiasi tipo di istanza spot che costa più di `0.266`. Non è consigliabile utilizzare questo parametro perché i prezzi spot possono fluttuare e quindi anche la soglia di protezione del prezzo potrebbe variare.

Specifica la soglia di protezione del prezzo

Per specificare la soglia di protezione del prezzo utilizzando AWS CLI

Durante la creazione di una flotta EC2 o Spot Fleet utilizzando il AWS CLI, configura la flotta per la selezione del tipo di istanza basata sugli attributi, quindi procedi come segue:

- Per specificare la soglia di protezione del prezzo dell' On-Demand istanza, nel file di configurazione JSON, nella `InstanceRequirements` struttura, per`OnDemandMaxPricePercentageOverLowestPrice`, inserisci la soglia di protezione del prezzo come percentuale.
- Per specificare la soglia di protezione del prezzo dell'istanza spot, nel file di configurazione JSON, nella struttura `InstanceRequirements`, specifica uno dei seguenti parametri:
  - Per `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`, inserisci la soglia di protezione del prezzo in percentuale.
  - Per `SpotMaxPricePercentageOverLowestPrice`, inserisci la soglia di protezione del prezzo in percentuale.

Per ulteriori informazioni, consulta Creazione di un EC2 Fleet con la selezione del tipo di istanza basata su attributi o Creazione di una serie di istanze spot con la selezione del tipo di istanza basata su attributi.

(Solo parco istanze spot) Per specificare la soglia di protezione del prezzo usando la console

Durante la creazione del parco istanze spot nella console, configura il parco istanze per la selezione del tipo di istanza basata su attributi ed esegui le seguenti operazioni:

- Per specificare la soglia di protezione del prezzo dell' On-Demand istanza, in Attributo aggiuntivo dell'istanza, scegli Protezione del On-demand prezzo, scegli Aggiungi attributo, quindi inserisci la soglia di protezione del prezzo come percentuale.
- Per specificare la soglia di protezione del prezzo dell'istanza spot, Attributo istanza aggiuntivo, scegli Protezione del prezzo Spot, scegli Aggiungi attributo, scegli un valore di base su cui basare il prezzo, e poi inserisci la soglia di protezione del prezzo in percentuale.

> **Note**
>
> Durante la creazione del parco istanze, se imposti `TargetCapacityUnitType` su `vcpu` o `memory-mib`, la soglia di protezione del prezzo viene applicata in base al prezzo per vCPU o per memoria, anziché al prezzo per istanza.

Protezione delle prestazioni

La protezione delle prestazioni è una funzionalità che garantisce che il parco istanze EC2 o il parco istanze spot utilizzi tipi di istanze che sono simili o superiori a un riferimento prestazionale specificato. Per utilizzare la protezione delle prestazioni, devi specificare una famiglia di istanze come riferimento di base. Le funzionalità della famiglia di istanze specificata stabiliscono il livello di prestazioni minimo accettabile. Quando Amazon EC2 seleziona i tipi di istanza per il parco istanze, considera gli attributi specificati e il riferimento delle prestazioni. I tipi di istanza che non rientrano nel riferimento prestazionale vengono automaticamente esclusi dalla selezione, anche se corrispondono agli altri attributi specificati. Ciò garantisce che tutti i tipi di istanza selezionati offrano prestazioni simili o superiori rispetto al riferimento stabilito dalla famiglia di istanze specificata. Amazon EC2 utilizza questo riferimento per guidare la selezione del tipo di istanza, ma non è garantito che i tipi di istanza selezionati superino sempre il riferimento per ogni applicazione.

Attualmente, questa funzionalità supporta solo le prestazioni della CPU come fattore prestazionale di riferimento. Le prestazioni della CPU del processore CPU della famiglia di istanze specificata fungono da riferimento delle prestazioni, garantendo che i tipi di istanza selezionati siano simili o superiori a questo riferimento. Le famiglie di istanze con gli stessi processori CPU producono gli stessi risultati di filtraggio, anche se le loro prestazioni di rete o disco sono diverse. Ad esempio, specificando `c6in` o

`c6i` come riferimento di base si otterranno risultati di filtraggio basati sulle prestazioni identici perché entrambe le famiglie di istanze utilizzano lo stesso processore CPU.

Famiglie di istanza non supportate

Le seguenti famiglie di istanze non sono supportate per la protezione delle prestazioni:

- Uso generico: Mac1 | Mac2 | | | Mac2-m1ultra | M1 Mac2-m2 Mac2-m2pro | M2 | T1
- Ottimizzato per il calcolo: C1
- Memoria ottimizzata: U-3tb1 | | U-6tb1 | U-9tb1 U-12tb1 | u-24tb1 U-18tb1 | | | | | U7i-12tb U7in-16tb U7in-24tb U7in-32tb
- Calcolo accelerato: G3 | G3s | P3dn | P4d | P5
- High-performance informatica: HPC7g

Se abiliti la protezione delle prestazioni specificando una famiglia di istanze supportata, i tipi di istanza restituiti escluderanno le famiglie di istanze non supportate di cui sopra.

Se si specifica una famiglia di istanze non supportata come valore per le prestazioni di base, l'API restituisce una risposta vuota per GetInstanceTypesFromInstanceRequirements e un'eccezione per CreateFleet,, e. RequestSpotFleet ModifyFleet ModifySpotFleetRequest

Esempio: Impostare un riferimento di prestazioni per la CPU

Nell'esempio seguente, il requisito dell'istanza è l'avvio con tipi di istanza con core CPU con prestazioni pari a quelle della famiglia di istanze `c6i`. In questo modo verranno esclusi i tipi di istanza con processori CPU meno performanti, anche se soddisfano altri requisiti di istanza specificati, come il numero di vCPU. Ad esempio, se gli attributi dell'istanza specificati includono 4 vCPU e 16 GB di memoria, un tipo di istanza con questi attributi ma con prestazioni della CPU inferiori a `c6i` verrà escluso dalla selezione.

```
"BaselinePerformanceFactors": {
        "Cpu": {
            "References": [
                {
                    "InstanceFamily": "c6i"
                }
            ]
        }
```

Considerazioni

- È possibile specificare i tipi di istanza o gli attributi di istanza in un parco istanze EC2 o un parco istanze spot, ma non entrambi nello stesso momento.

  Quando si utilizza la CLI, le sostituzioni del modello di avvio sovrascriveranno il modello di avvio. Ad esempio, se il modello di avvio contiene un tipo di istanza e la sostituzione del modello di avvio contiene attributi di istanza, le istanze identificate dagli attributi di istanza sostituiranno il tipo di istanza nel modello di avvio.
- Quando si utilizza la CLI e si specificano gli attributi di istanza come sostituzioni, non è possibile specificare pesi o priorità.
- In una configurazione di richiesta è possibile specificare un massimo di quattro strutture `InstanceRequirements`.

Creazione di un EC2 Fleet con la selezione del tipo di istanza basata su attributi

Puoi configurare un EC2 Fleet in modo da utilizzare la selezione del tipo di istanza basata su attributi. Non è possibile creare un EC2 Fleet usando la console Amazon EC2.

I parametri per la selezione del tipo di istanza basata su attributi sono specificati nella struttura `InstanceRequirements`. Quando `InstanceRequirements` è incluso nella configurazione del parco istanze, `InstanceType` e `WeightedCapacity` devono essere esclusi; non possono determinare la configurazione del parco istanze contemporaneamente agli attributi di istanza.

Negli PowerShell esempi AWS CLI e, vengono specificati i seguenti attributi:

- `VCpuCount`: un minimo di 2 vCPU e un massimo di 4 vCPU. Se non è necessario un limite massimo, puoi omettere il valore massimo.
- `MemoryMiB`: un minimo di 8 GiB di memoria e un massimo di 16 GiB. Se non è necessario un limite massimo, puoi omettere il valore massimo.

Questa configurazione identifica qualsiasi tipo di istanza con un numero di vCPU compreso fra 2 e 4 e da 8 a 16 GiB di memoria. Tuttavia, la protezione dei prezzi e la strategia di allocazione potrebbero escludere alcuni tipi di istanze quando il parco istanze EC2 alloca le istanze.

AWS CLI

Creazione di un EC2 Fleet con la selezione del tipo di istanza basata su attributi

Utilizza il comando create-fleet per creare un EC2 Fleet. Specificare la configurazione del parco istanze in un file JSON.

```
aws ec2 create-fleet \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Il file *file_name*.json dell'esempio seguente contiene i parametri che configurano un EC2 Fleet in modo da utilizzare la selezione del tipo di istanza basata su attributi.

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized"
    },
    "LaunchTemplateConfigs": [{
        "LaunchTemplateSpecification": {
            "LaunchTemplateName": "my-launch-template",
            "Version": "1"
        },
        "Overrides": [{
            "InstanceRequirements": {
                "VCpuCount": {
                    "Min": 2,
                    "Max": 4
                },
                "MemoryMiB": {
                    "Min": 8192,
                    "Max": 16384
                }
            }
        }]
    }],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

PowerShell

Creazione di un EC2 Fleet con la selezione del tipo di istanza basata su attributi

Utilizza il cmdlet New-EC2Fleet.

```
$vcpuCount = New-Object Amazon.EC2.Model.VCpuCountRangeRequest
$vcpuCount.Min = 2
$vcpuCount.Max = 4
$memoryMiB = New-Object Amazon.EC2.Model.MemoryMiBRequest
$memoryMiB.Min = 8192
$memoryMiB.Max = 16384
$instanceRequirements = New-Object Amazon.EC2.Model.InstanceRequirementsRequest
$instanceRequirements.VCpuCount = $vcpuCount
$instanceRequirements.MemoryMiB = $memoryMiB

$launchTemplateSpec = New-Object
 Amazon.EC2.Model.FleetLaunchTemplateSpecificationRequest
$launchTemplateSpec.LaunchTemplateName = "my-launch-template"
$launchTemplateSpec.Version = "1"
$override = New-Object Amazon.EC2.Model.FleetLaunchTemplateOverridesRequest
$override.InstanceRequirements = $instanceRequirements
$launchTemplateConfig = New-Object Amazon.EC2.Model.FleetLaunchTemplateConfigRequest
$launchTemplateConfig.LaunchTemplateSpecification = $launchTemplateSpec
$launchTemplateConfig.Overrides = @($override)

New-EC2Fleet `
    -SpotOptions_AllocationStrategy "price-capacity-optimized" `
    -LaunchTemplateConfig @($launchTemplateConfig) `
    -TargetCapacitySpecification_DefaultTargetCapacityType "spot" `
    -TargetCapacitySpecification_TotalTargetCapacity 20 `
    -Type "instant"
```

Creazione di una serie di istanze spot con la selezione del tipo di istanza basata su attributi

> **Important**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Puoi configurare un parco istanze per utilizzare la selezione del tipo di istanza basata su attributi.

I parametri per la selezione del tipo di istanza basata su attributi sono specificati nella struttura `InstanceRequirements`. Quando `InstanceRequirements` è incluso nella configurazione del parco istanze, `InstanceType` e `WeightedCapacity` devono essere esclusi; non possono determinare la configurazione del parco istanze contemporaneamente agli attributi di istanza.

Negli PowerShell esempi AWS CLI e, vengono specificati i seguenti attributi:

- `VCpuCount`: un minimo di 2 vCPU e un massimo di 4 vCPU. Se non è necessario un limite massimo, puoi omettere il valore massimo.
- `MemoryMiB`: un minimo di 8 GiB di memoria e un massimo di 16 GiB. Se non è necessario un limite massimo, puoi omettere il valore massimo.

Questa configurazione identifica qualsiasi tipo di istanza che hanno un numero di vCPU compreso fra 2 e 4 e da 8 a 16 GiB di memoria. Tuttavia, la protezione dei prezzi e la strategia di allocazione potrebbero escludere alcuni tipi di istanze quando il parco istanze spot alloca le istanze.

Console

Configurazione di un parco istanze spot per la selezione del tipo di istanza basata su attributi

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione selezionare Spot Requests (Richieste Spot) e scegli Request Spot Instances (Istanze spot richiesta).
3. Seguire la procedura per creare una serie di istanze spot. Per ulteriori informazioni, consulta Crea una richiesta di parco istanze spot utilizzando parametri definiti.

   Durante la creazione della serie di istanze spot, configurare il parco istanze per la selezione del tipo di istanza basata su attributi come segue:

   a. Per Instance type requirements (Requisiti per il tipo di istanza), scegliere Specify instance attributes that match your compute requirements (Specifica gli attributi di istanza che corrispondono ai requisiti di calcolo).
   b. Per vCPUs (vCPU) inserire il numero minimo e massimo desiderato di vCPU. Per non specificare alcun limite, selezionare No minimum (Nessun minimo), No maximum (Nessun massimo) o entrambe le opzioni.
   c. Per Memory (GiB) (Memoria [GiB]) inserire la quantità minima e massima di memoria desiderata. Per non specificare alcun limite, selezionare No minimum (Nessun minimo), No maximum (Nessun massimo) o entrambe le opzioni.

d. (Facoltativo) Per Additional instance attributes (Attributi istanza aggiuntivi), facoltativamente, è possibile specificare uno o più attributi per esprimere i requisiti di calcolo in modo più dettagliato. Ogni attributo aggiuntivo aggiunge ulteriori vincoli alla propria richiesta.

e. (Facoltativo) Espandere Preview matching instance types (Anteprima tipi di istanza corrispondenti) per visualizzare i tipi di istanza con gli attributi specificati.

AWS CLI

Configurazione di un parco istanze spot per la selezione del tipo di istanza basata su attributi

Utilizza il comando request-spot-fleet per creare un parco istanze spot. Specificare la configurazione del parco istanze in un file JSON.

```
aws ec2 request-spot-fleet \
    --region us-east-1 \
    --spot-fleet-request-config file://file_name.json
```

Il file *file_name*.json dell'esempio seguente contiene i parametri che configurano un parco istanze spot in modo da utilizzare la selezione del tipo di istanza basata su attributi.

```
{
    "AllocationStrategy": "priceCapacityOptimized",
    "TargetCapacity": 20,
    "Type": "request",
    "LaunchTemplateConfigs": [{
        "LaunchTemplateSpecification": {
            "LaunchTemplateName": "my-launch-template",
            "Version": "1"
        },
        "Overrides": [{
            "InstanceRequirements": {
                "VCpuCount": {
                    "Min": 2,
                    "Max": 4
                },
                "MemoryMiB": {
                    "Min": 8192,
                    "Max": 16384
                }
```

```
            }
        }]
    }]
}
```

PowerShell

Configurazione di un parco istanze spot per la selezione del tipo di istanza basata su attributi

Utilizza il cmdlet Request-EC2SpotFleet.

```
$vcpuCount = New-Object Amazon.EC2.Model.VCpuCountRange
$vcpuCount.Min = 2
$vcpuCount.Max = 4
$memoryMiB = New-Object Amazon.EC2.Model.MemoryMiB
$memoryMiB.Min = 8192
$memoryMiB.Max = 16384
$instanceRequirements = New-Object Amazon.EC2.Model.InstanceRequirements
$instanceRequirements.VCpuCount = $vcpuCount
$instanceRequirements.MemoryMiB = $memoryMiB

$launchTemplateSpec = New-Object Amazon.EC2.Model.FleetLaunchTemplateSpecification
$launchTemplateSpec.LaunchTemplateName = "my-launch-template"
$launchTemplateSpec.Version = "1"
$override = New-Object Amazon.EC2.Model.LaunchTemplateOverrides
$override.InstanceRequirements = $instanceRequirements
$launchTemplateConfig = New-Object Amazon.EC2.Model.LaunchTemplateConfig
$launchTemplateConfig.LaunchTemplateSpecification = $launchTemplateSpec
$launchTemplateConfig.Overrides = @($override)

Request-EC2SpotFleet `
    -SpotFleetRequestConfig_AllocationStrategy "PriceCapacityOptimized" `
    -SpotFleetRequestConfig_TargetCapacity 20 `
    -SpotFleetRequestConfig_Type "Request" `
    -SpotFleetRequestConfig_LaunchTemplateConfig $launchTemplateConfig
```

Esempi di configurazioni del parco istanze EC2 che sono valide e non valide

Se si utilizza il AWS CLI per creare una flotta EC2, è necessario assicurarsi che la configurazione della flotta sia valida. I seguenti esempi mostrano configurazioni valide e non valide.

Le configurazioni sono considerate non valide quando contengono quanto segue:

- Una singola struttura `Overrides` con `InstanceRequirements` e `InstanceType`
- Due strutture `Overrides`, una con `InstanceRequirements` e l'altra con `InstanceType`
- Due strutture `InstanceRequirements` con valori di attributo sovrapposti all'interno dello stesso `LaunchTemplateSpecification`

Configurazioni di esempio

- Configurazione valida: modello di avvio singolo con sostituzioni
- Configurazione valida: modello di avvio singolo con più InstanceRequirements
- Configurazione valida: due modelli di avvio, ognuno con sostituzioni
- Configurazione valida: specificati solo InstanceRequirements, nessun valore di attributo sovrapposto
- Configurazione non valida: le sostituzioni contengono e InstanceRequirements InstanceType
- Configurazione non valida: due sostituzioni contengono e InstanceRequirements InstanceType
- Configurazione non valida: valori di attributo sovrapposti

Configurazione valida: modello di avvio singolo con sostituzioni

La configurazione seguente è valida. Contiene un modello di avvio e una struttura `Overrides` contenente una struttura `InstanceRequirements`. Di seguito è riportata una spiegazione della configurazione di esempio.

```
{
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
```

```
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5000,
        "DefaultTargetCapacityType": "spot",
        "TargetCapacityUnitType": "vcpu"
        }
    }
}
```

`InstanceRequirements`

Per utilizzare la selezione dell'istanza basata su attributi, è necessario includere la struttura `InstanceRequirements` nella configurazione del parco istanze e specificare gli attributi desiderati per le istanze nel parco istanze.

Nell'esempio precedente, vengono specificati i seguenti attributi di istanza:

- `VCpuCount`: i tipi di istanza devono avere un minimo di 2 e un massimo di 8 vCPU.
- `MemoryMiB`: i tipi di istanza devono avere un massimo di 10240 MiB di memoria. Un minimo di 0 indica nessun limite minimo.
- `MemoryGiBPerVCpu`: i tipi di istanza devono avere un massimo di 10.000 MiB di memoria per vCPU. Il parametro `Min` è facoltativo. Omettendolo, non si indica alcun limite minimo.

`TargetCapacityUnitType`

Il parametro `TargetCapacityUnitType` specifica l'unità per la capacità di destinazione. Nell'esempio, la capacità di destinazione è `5000` e il tipo di unità della capacità di destinazione è `vcpu`, che insieme specificano una capacità di destinazione desiderata di 5.000 vCPU. Il parco istanze EC2 avvierà una quantità sufficiente di istanze in modo che il numero totale di vCPU nel parco istanze sia 5.000.

Configurazione valida: modello di avvio singolo con più InstanceRequirements

La configurazione seguente è valida. Contiene un modello di avvio e una struttura `Overrides` contenente due strutture `InstanceRequirements`. Gli attributi specificati in `InstanceRequirements` sono validi perché i valori non si sovrappongono; la prima struttura `InstanceRequirements` specifica un `VCpuCount` di 0-2 vCPU, mentre la seconda struttura `InstanceRequirements` specifica 4-8 vCPU.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
```

```
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configurazione valida: due modelli di avvio, ognuno con sostituzioni

La configurazione seguente è valida. Contiene due modelli di avvio, ognuno con una struttura `Overrides` contenente una struttura `InstanceRequirements`. Questa configurazione è utile per il supporto delle architetture `arm` e `x86` nello stesso parco istanze.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
```

```
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configurazione valida: specificati solo **`InstanceRequirements`**, nessun valore di attributo sovrapposto

La configurazione seguente è valida. Contiene due strutture `LaunchTemplateSpecification`, ognuna con un modello di avvio e una struttura `Overrides` contenente una struttura `InstanceRequirements`. Gli attributi specificati in `InstanceRequirements` sono validi perché i valori non si sovrappongono; la prima struttura `InstanceRequirements` specifica un `VCpuCount` di 0-2 vCPU, mentre la seconda struttura `InstanceRequirements` specifica 4-8 vCPU.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
```

```
            ]
        },
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "MyOtherLaunchTemplate",
                "Version": "1"
            },
            "Overrides": [
            {
                "InstanceRequirements": {
                    "VCpuCount": {
                        "Min": 4,
                        "Max": 8
                    },
                    "MemoryMiB": {
                        "Min": 0
                    }
                }
            }
          ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
  }
}
```

Configurazione non valida: le **sostituzioni contengono e InstanceRequirements InstanceType**

La configurazione seguente non è valida. La struttura `Overrides` include sia `InstanceRequirements` che `InstanceType`. Per le `Overrides`, è possibile specificare `InstanceRequirements` o `InstanceType`, ma non entrambi.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "MyLaunchTemplate",
                "Version": "1"
            },
```

```
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configurazione non valida: due sostituzioni contengono e **`InstanceRequirements`** **`InstanceType`**

La configurazione seguente non è valida. Le strutture `Overrides` contengono sia `InstanceRequirements` che `InstanceType`. È possibile specificare `InstanceRequirements` o `InstanceType` ma non entrambi, anche se si trovano in strutture `Overrides` differenti.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
```

```
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Configurazione non valida: valori di attributo sovrapposti

La configurazione seguente non è valida. Le due strutture `InstanceRequirements`, ognuna contenente `"VCpuCount": {"Min": 0, "Max": 2}`. I valori di questi attributi si sovrappongono, il che restituirà pool di capacità duplicati.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
```

```
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Esempi di configurazioni del parco istanze spot che sono valide e non valide

Se utilizzi il AWS CLI per creare una flotta Spot, devi assicurarti che la configurazione della tua flotta sia valida. I seguenti esempi mostrano configurazioni valide e non valide.

Le configurazioni sono considerate non valide quando contengono quanto segue:

- Una singola struttura `Overrides` con `InstanceRequirements` e `InstanceType`
- Due strutture `Overrides`, una con `InstanceRequirements` e l'altra con `InstanceType`

- Due strutture `InstanceRequirements` con valori di attributo sovrapposti all'interno dello stesso `LaunchTemplateSpecification`

Configurazioni di esempio

- Configurazione valida: modello di avvio singolo con sostituzioni
- Configurazione valida: modello di avvio singolo con più InstanceRequirements
- Configurazione valida: due modelli di avvio, ognuno con sostituzioni
- Configurazione valida: specificati solo InstanceRequirements, nessun valore di attributo sovrapposto
- Configurazione non valida: le sostituzioni contengono e InstanceRequirements InstanceType
- Configurazione non valida: due sostituzioni contengono e InstanceRequirements InstanceType
- Configurazione non valida: valori di attributo sovrapposti

Configurazione valida: modello di avvio singolo con sostituzioni

La configurazione seguente è valida. Contiene un modello di avvio e una struttura `Overrides` contenente una struttura `InstanceRequirements`. Di seguito è riportata una spiegazione della configurazione di esempio.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
```

```
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
        "TargetCapacity": 5000,
            "OnDemandTargetCapacity": 0,
            "TargetCapacityUnitType": "vcpu"
    }
}
```

`InstanceRequirements`

Per utilizzare la selezione dell'istanza basata su attributi, è necessario includere la struttura `InstanceRequirements` nella configurazione del parco istanze e specificare gli attributi desiderati per le istanze nel parco istanze.

Nell'esempio precedente, vengono specificati i seguenti attributi di istanza:

- `VCpuCount`: i tipi di istanza devono avere un minimo di 2 e un massimo di 8 vCPU.
- `MemoryMiB`: i tipi di istanza devono avere un massimo di 10240 MiB di memoria. Un minimo di 0 indica nessun limite minimo.
- `MemoryGiBPerVCpu`: i tipi di istanza devono avere un massimo di 10.000 MiB di memoria per vCPU. Il parametro `Min` è facoltativo. Omettendolo, non si indica alcun limite minimo.

`TargetCapacityUnitType`

Il parametro `TargetCapacityUnitType` specifica l'unità per la capacità di destinazione. Nell'esempio, la capacità di destinazione è `5000` e il tipo di unità della capacità di destinazione è `vcpu`, che insieme specificano una capacità di destinazione desiderata di 5.000 vCPU. La serie di istanze spot avvierà un numero sufficiente di istanze in modo che il numero totale di vCPU nel parco istanze sia di 5.000.

Configurazione valida: modello di avvio singolo con più InstanceRequirements

La configurazione seguente è valida. Contiene un modello di avvio e una struttura `Overrides` contenente due strutture `InstanceRequirements`. Gli attributi specificati in `InstanceRequirements` sono validi perché i valori non si sovrappongono; la prima struttura `InstanceRequirements` specifica un `VCpuCount` di 0-2 vCPU, mentre la seconda struttura `InstanceRequirements` specifica 4-8 vCPU.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
```

```
            ]
        }
    ],
    "TargetCapacity": 1,
    "OnDemandTargetCapacity": 0,
    "Type": "maintain"
  }
}
```

Configurazione valida: due modelli di avvio, ognuno con sostituzioni

La configurazione seguente è valida. Contiene due modelli di avvio, ognuno con una struttura `Overrides` contenente una struttura `InstanceRequirements`. Questa configurazione è utile per il supporto delle architetture `arm` e `x86` nello stesso parco istanze.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
```

```
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configurazione valida: specificati solo **`InstanceRequirements`**, nessun valore di attributo sovrapposto

La configurazione seguente è valida. Contiene due strutture `LaunchTemplateSpecification`, ognuna con un modello di avvio e una struttura `Overrides` contenente una struttura `InstanceRequirements`. Gli attributi specificati in `InstanceRequirements` sono validi perché i valori non si sovrappongono; la prima struttura `InstanceRequirements` specifica un `VCpuCount` di 0-2 vCPU, mentre la seconda struttura `InstanceRequirements` specifica 4-8 vCPU.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
```

```
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configurazione non valida: le **sostituzioni contengono e InstanceRequirements InstanceType**

La configurazione seguente non è valida. La struttura `Overrides` include sia `InstanceRequirements` che `InstanceType`. Per le `Overrides`, è possibile specificare `InstanceRequirements` o `InstanceType`, ma non entrambi.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configurazione non valida: due sostituzioni contengono e **InstanceRequirements** **InstanceType**

La configurazione seguente non è valida. Le strutture `Overrides` contengono sia `InstanceRequirements` che `InstanceType`. È possibile specificare `InstanceRequirements` o `InstanceType` ma non entrambi, anche se si trovano in strutture `Overrides` differenti.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
```

```
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Configurazione non valida: valori di attributo sovrapposti

La configurazione seguente non è valida. Le due strutture `InstanceRequirements`, ognuna contenente `"VCpuCount": {"Min": 0, "Max": 2}`. I valori di questi attributi si sovrappongono, il che restituirà pool di capacità duplicati.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
```

```
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
            }
        ]
    }
],
"TargetCapacity": 1,
"OnDemandTargetCapacity": 0,
"Type": "maintain"
}
}
```

Anteprima di tipi di istanza con attributi specificati

Puoi utilizzare il comando get-instance-types-from-instance-requirements per visualizzare in anteprima i tipi di istanza che corrispondono agli attributi specificati. Ciò è particolarmente utile per capire quali attributi specificare nella configurazione della richiesta senza avviare alcuna istanza. Si noti che il comando non considera la capacità disponibile.

Per visualizzare in anteprima un elenco di tipi di istanza specificando gli attributi utilizzando AWS CLI

1. (Facoltativo) Per generare tutti gli attributi possibili che possono essere specificati, utilizzare il comando get-instance-types-from-instance-requirements e il parametro `--generate-cli-skeleton`. Facoltativamente, è possibile indirizzare l'output a un file per salvarlo tramite `input > attributes.json`.

   ```
   aws ec2 get-instance-types-from-instance-requirements \
       --region us-east-1 \
       --generate-cli-skeleton input > attributes.json
   ```

   Output previsto

   ```
   {
       "DryRun": true,
       "ArchitectureTypes": [
           "i386"
       ],
       "VirtualizationTypes": [
   ```

```
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 0,
            "Max": 0
        },
        "MemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
```

```
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Creare un file di configurazione JSON utilizzando l'output del passaggio precedente e configurarlo come segue:

> **Note**
>
> È necessario fornire valori per `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` e `MemoryMiB`. È possibile omettere gli altri attributi, nel qual caso saranno utilizzati i valori di default.
> Per una descrizione di ciascun attributo e dei relativi valori di default, consulta get-instance-types-from-instance-requirements.

a. Per `ArchitectureTypes`, specificare uno o più tipi di architettura del processore.

b. Per `VirtualizationTypes`, specificare uno o più tipi di virtualizzazione.

c. Per `VCpuCount`, specificare il numero minimo e massimo di vCPU. Per non specificare un limite minimo, per `Min`, specificare `0`. Per non specificare alcun limite massimo, omettere il parametro `Max`.

d. Per `MemoryMiB`, specificare la quantità minima e massima di memoria in MiB. Per non specificare un limite minimo, per `Min`, specificare `0`. Per non specificare alcun limite massimo, omettere il parametro `Max`.

e. Facoltativamente, è possibile specificare uno o più altri attributi per limitare ulteriormente l'elenco di tipi di istanza restituiti.

3. Per visualizzare in anteprima i tipi di istanza con gli attributi specificati nel file JSON, utilizzare il comando get-instance-types-from-instance-requirements e specificare il nome e il percorso del file JSON utilizzando il parametro `--cli-input-json`. Facoltativamente, è possibile formattare l'output in modo che venga visualizzato in un formato tabella.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

Esempio di file *attributes.json*

In questo esempio gli attributi richiesti sono inclusi nel file JSON. Tali attributi sono `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` e `MemoryMiB`. Inoltre, è incluso anche l'attributo facoltativo `InstanceGenerations`. Tenere presente che per `MemoryMiB`, il valore `Max` può essere omesso per indicare che non c'è alcun limite.

```
{

    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
```

```
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
    }
}
```

Output di esempio

```
-----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+---------------------------------------+
||             InstanceTypes             ||
|+-------------------------------------+|
||             InstanceType              ||
|+-------------------------------------+|
||  c4.xlarge                          ||
||  c5.xlarge                          ||
||  c5a.xlarge                         ||
||  c5ad.xlarge                        ||
||  c5d.xlarge                         ||
||  c5n.xlarge                         ||
||  d2.xlarge                          ||
...
```

4. Dopo aver identificato i tipi di istanza che soddisfano le proprie esigenze, prendere nota degli attributi di istanza utilizzati in modo da poterli utilizzare durante la configurazione della richiesta del parco istanze.

Utilizza la ponderazione delle istanze per gestire i costi e le prestazioni del parco istanze EC2 o del parco istanze spot

Con la ponderazione delle istanze, assegni un peso a ciascun tipo di istanza del parco istanze EC2 o del parco istanze Spot per rappresentarne la capacità di calcolo e le prestazioni reciproche. In base ai pesi, il parco istanze può utilizzare qualsiasi combinazione dei tipi di istanza specificati, purché sia in

grado di soddisfare la capacità target desiderata. Questo può aiutarti a gestire i costi e le prestazioni del tuo parco istanze.

Il peso rappresenta le unità di capacità con cui un tipo di istanza contribuisce alla capacità target totale.

Esempio: utilizza la ponderazione delle istanze per la gestione delle prestazioni

Supponiamo che il tuo parco istanze abbia due tipi di istanza e che tu assegni un peso diverso a ciascun tipo di istanza per riflettere quante istanze ti servono per ottenere le stesse prestazioni, come indicato di seguito:

- `m5.large` – peso: 1
- `m5.2xlarge` – peso: 4

Assegnando questi pesi, stai dicendo che avresti bisogno di 4 istanze `m5.large` per ottenere le stesse prestazioni di 1 `m5.2xlarge`.

Per calcolare quante istanze di ogni tipo di istanza sono necessarie per una determinata capacità target, utilizza la formula seguente:

```
target capacity / weight = number of instances
```

Se la capacità target è di 8 unità, il parco istanze può raggiungere la capacità target con `m5.large` o `m5.2xlarge`, o con una combinazione di entrambe, come indicato di seguito:

- 8 istanze `m5.large` (capacità di 8 / peso di 1 = 8 istanze)
- 2 istanze `m5.2xlarge` (capacità di 8 / peso di 4 = 2 istanze)
- 4 `m5.large` e 1 `m5.2xlarge`

Esempio: utilizza la ponderazione delle istanze per la gestione dei costi

Per impostazione predefinita, il prezzo specificato è all'ora per istanza. Quando si utilizza la funzionalità di ponderazione di istanza, il prezzo specificato è all'ora per unità. È possibile calcolare il prezzo all'ora per unità dividendo il prezzo di un tipo di istanza per il numero di unità che essa rappresenta. Il parco istanze calcola il numero di istanze da avviare dividendo la capacità target per il peso dell'istanza. Se il risultato non è un numero intero, il parco istanze lo arrotonda al numero intero successivo, in modo che la dimensione del parco istanze non sia inferiore alla sua capacità

di destinazione. Il parco istanze può selezionare qualsiasi pool specificato nella specifica di avvio, anche se la capacità delle istanze avviate supera la capacità di destinazione richiesta.

La tabella seguente include esempi di calcoli per determinare il prezzo per unità per un parco istanze con una capacità target di 10.

Tipo di istanza	Peso dell'istanza	Capacità di destinazione	Numero di istanze avviate	Prezzo all'ora per istanza	Prezzo all'ora per unità
`r3.xlarge`	2	10	5 (10 diviso 2)	0,05 USD	0,025 USD (0,05 diviso 2)
`r3.8xlarge`	8	10	2 (10 diviso 8, risultato arrotondato)	0,10 USD	0,0125 USD (0,10 diviso 8)

Utilizzare la ponderazione d'istanza del parco istanze come segue per assegnare la capacità target desiderata nei pool con il prezzo più basso per unità al momento dell'adempimento:

1. Impostare la capacità target per il parco istanze sia nelle istanze (predefinite) sia nelle unità prescelte, come vCPU, memoria, archiviazione o throughput.
2. Impostare il prezzo per unità.
3. Per ogni specifica di avvio, indicare il peso, ovvero il numero di unità che il tipo di istanza rappresenta per la capacità di destinazione.

Esempio di ponderazione istanza

Considerare una richiesta del parco istanze con la configurazione seguente:

- Una capacità di destinazione di 24
- Una specifica di avvio con un tipo di istanza `r3.2xlarge` e un peso di 6

- Una specifica di avvio con un tipo di istanza `c3.xlarge` e un peso di 5

I pesi rappresentano il numero di unità che il tipo di istanza rappresenta per la capacità di destinazione. Se la prima specifica di avvio fornisce il prezzo più basso per unità (prezzo per `r3.2xlarge` all'ora per istanza diviso 6), il parco istanze lancerà quattro di tali istanze (24 diviso 6).

Se la seconda specifica di avvio fornisce il prezzo più basso per unità (prezzo per `c3.xlarge` all'ora per istanza diviso 5), il parco istanze lancerà cinque di tali istanze (24 diviso 5, risultato arrotondato).

Ponderazione d'istanza e strategia di allocazione

Considerare una richiesta del parco istanze con la configurazione seguente:

- Una capacità obiettivo di 30 Istanze spot
- Una specifica di avvio con un tipo di istanza `c3.2xlarge` e un peso di 8
- Una specifica di avvio con un tipo di istanza `m3.xlarge` e un peso di 8
- Una specifica di avvio con un tipo di istanza `r3.xlarge` e un peso di 8

Il parco istanze avvierà quattro istanze (30 diviso 8, risultato arrotondato). Con la strategia `diversified`, il parco istanze avvia un'istanza in ognuno dei tre pool e la quarta istanza in qualsiasi dei tre pool che fornisce il prezzo più basso per unità.

Utilizza le strategie di allocazione per determinare in che modo EC2 Fleet o Spot Fleet soddisfano Spot e la capacità On-Demand

Quando utilizzi più pool di capacità (ciascuno composto da un tipo di istanza e una zona di disponibilità) in una flotta EC2 o in una flotta Spot, puoi utilizzare una strategia di allocazione per gestire il modo in cui Amazon EC2 soddisfa il tuo Spot e On-Demand le capacità di questi pool. Le strategie di allocazione possono ottimizzare la capacità disponibile, il prezzo e i tipi di istanza da utilizzare. Esistono diverse strategie di allocazione per le istanze e le istanze Spot. On-Demand

Argomenti

- Strategie di allocazione per istanze spot
- Strategie di allocazione per le istanze On-Demand
- Scelta della strategia di allocazione spot adeguata
- Mantenimento della capacità target per le istanze Spot

- Dai priorità ai tipi di istanze in termini di capacità On-Demand

Strategie di allocazione per istanze spot

La configurazione di avvio determina tutti i possibili pool di capacità spot (tipi di istanze e zone di disponibilità) da cui il parco istanze EC2 o il parco istanze spot possono avviare istanze spot. Tuttavia, al momento del lancio delle istanze, il parco istanze utilizza la strategia di allocazione specificata per scegliere i pool specifici da tutti i pool possibili.

> **Note**
>
> (Solo istanze Linux) Se configuri l'istanza Spot per l'avvio con AMD SEV-SNP attivato, ti verrà addebitata una tariffa oraria aggiuntiva di utilizzo equivalente al 10% della tariffa On-Demand oraria per il tipo di istanza selezionato. Se la strategia di allocazione utilizza il prezzo come input, il parco istanze non include questa tariffa aggiuntiva; viene utilizzato solo il prezzo spot.

Puoi specificare una delle seguenti strategie di allocazione per le istanze Spot:

Ottimizzazione per prezzo e capacità (consigliato)

Il parco istanze identifica i pool con la massima capacità disponibile per il numero di istanze che si stanno avviando. Ciò significa che le istanze Spot vengono richieste dai pool che hanno maggiori probabilità di avere le minori possibilità di interruzione nel breve termine. Dopodiché, il parco istanze richiede istanze spot dal pool con il prezzo più basso tra questi pool.

La strategia di allocazione con ottimizzazione per prezzo e capacità è la scelta migliore per la maggior parte dei carichi di lavoro spot, come applicazioni containerizzate stateless, microservizi, applicazioni Web, processi di dati e analisi ed elaborazione in batch.

Se stai utilizzando il AWS CLI, il nome del parametro è `price-capacity-optimized` per EC2 Fleet e `priceCapacityOptimized` per Spot Fleet.

Ottimizzazione per capacità

Il parco istanze identifica i pool con la massima capacità disponibile per il numero di istanze che si stanno avviando. Ciò significa che le istanze Spot vengono richieste dai pool che hanno maggiori probabilità di avere le minori possibilità di interruzione nel breve termine.

Con Istanze spot, i prezzi cambiano lentamente nel tempo in base ai trend a lungo termine dell'offerta e della domanda, ma la capacità fluttua in tempo reale. La strategia con ottimizzazione per capacità avvia automaticamente Istanze spot nei pool più disponibili esaminando i dati di capacità in tempo reale e prevedendo quali sono le più disponibili. Questa strategia è ideale per carichi di lavoro che possono avere un costo più elevato di interruzione associato al riavvio del lavoro, ad esempio carichi di lavoro di integrazione continua (CI), rendering di immagini e media, deep learning e calcolo ad alte prestazioni (HPC), che possono avere un costo più elevato di interruzione associato al riavvio del lavoro. Offrendo la possibilità di ridurre il numero di interruzioni, la strategia con ottimizzazione per capacità può ridurre il costo complessivo del carico di lavoro.

In alternativa, puoi utilizzare la strategia di allocazione con priorità di ottimizzazione per capacità con un parametro di priorità e quindi impostare l'ordine dei tipi di istanza dalla priorità più alta alla più bassa. Puoi impostare la stessa priorità per diversi tipi di istanze. Il parco istanze ottimizzerà innanzitutto la capacità, ma rispetterà le priorità del tipo di istanza sulla base del miglior tentativo (ad esempio, se il rispetto delle priorità non influirà in modo significativo sulla capacità del parco istanze di fornire capacità ottimale). Questa è una buona opzione per i carichi di lavoro in cui è necessario ridurre al minimo la possibilità di interruzioni e la preferenza per determinati tipi di istanza è importante. Tieni presente che quando imposti la priorità per i tipi di istanze per la tua capacità Spot, la stessa priorità viene applicata anche alle On-Demand istanze se la strategia di On-Demand allocazione è impostata su prioritaria. Per il parco istanze spot, l'utilizzo delle priorità è supportato solo se il parco istanze utilizza un modello di avvio.

Se utilizzi il AWS CLI, i nomi dei parametri sono `capacity-optimized` e `capacity-optimized-prioritized` per EC2 Fleet e and per Spot Fleet. `capacityOptimized` `capacityOptimizedPrioritized`

Diversificata

I Istanze spot sono distribuiti in tutti i pool di capacità spot. Se stai usando il AWS CLI, il nome del parametro è sia `diversified` per EC2 Fleet che per Spot Fleet.

Prezzo più basso (non consigliato)

> **Warning**
>
> Non consigliamo la strategia di allocazione con prezzo più basso perché presenta il rischio di interruzione più elevato per le tue istanze spot.

Le istanze spot provengono dal pool con il prezzo più basso che ha capacità disponibile. Quando si utilizza il AWS CLI, questa è la strategia predefinita. Tuttavia, consigliamo di sostituire il valore predefinito specificando la strategia di allocazione con ottimizzazione per prezzo e capacità.

Con la strategia del prezzo più basso, se il pool con il prezzo più basso non ha capacità disponibile, le istanze spot provengono dal successivo pool con il prezzo più basso che ha capacità disponibile. Se un pool esaurisce la capacità prima di soddisfare la capacità desiderata, il parco istanze continuerà a soddisfare la richiesta attingendo dal successivo pool con il prezzo più basso. Per accertarti che la capacità desiderata sia soddisfatta, potresti ricevere istanze spot da vari pool.

Poiché questa strategia considera solo il prezzo dell'istanza e non la capacità disponibile, potrebbe comportare tassi di interruzione elevati.

La strategia di allocazione del prezzo più basso è disponibile solo quando si utilizza la AWS CLI. Il nome del parametro è `lowest-price` per il parco istanze EC2 e `lowestPrice` per il parco istanze spot.

Numero di pool da utilizzare

Il numero di pool Spot in cui allocare la capacità Spot di destinazione. Valido solo quando la strategia di allocazione è impostata sul prezzo più basso. Il parco istanze seleziona i pool spot con il prezzo più basso e alloca in modo uniforme la capacità spot obiettivo tra i pool spot specificati.

Tieni presente che il parco istanze prova a prelevare istanze spot dal numero di pool specificati sulla base del massimo sforzo. Se un pool esaurisce la capacità spot prima di soddisfare la capacità obiettivo, il parco istanze continuerà a soddisfare la tua richiesta attingendo al pool con il prezzo più basso successivo. Per garantire che la capacità di destinazione sia soddisfatta, è possibile ricevere istanze spot da un numero di pool maggiore di quello specificato. Analogamente, se la maggior parte dei pool non dispone di capacità spot, è possibile ricevere la capacità di destinazione completa da un numero di pool inferiore a quello specificato.

Questo parametro è disponibile solo quando si specifica la strategia di allocazione del prezzo più basso e solo quando si utilizza la AWS CLI. Il nome del parametro è `InstancePoolsToUseCount` sia per il parco istanze EC2 sia per il parco istanze spot.

Strategie di allocazione per le istanze On-Demand

La configurazione di avvio determina tutti i possibili pool di capacità (tipi di istanze e zone di disponibilità) da cui EC2 Fleet o Spot Fleet possono avviare le istanze. On-Demand Tuttavia, al

momento del lancio delle istanze, il parco istanze utilizza la strategia di allocazione specificata per scegliere i pool specifici da tutti i pool possibili.

È possibile specificare una delle seguenti strategie di allocazione per le istanze: On-Demand

Prezzo più basso

Le On-Demand istanze provengono dal pool con il prezzo più basso con capacità disponibile. Questa è la strategia predefinita.

Se il pool con il prezzo più basso non dispone di capacità disponibile, le On-Demand istanze provengono dal successivo pool con il prezzo più basso con capacità disponibile.

Se un pool esaurisce la capacità prima di soddisfare la capacità desiderata, il parco istanze continuerà a soddisfare la richiesta attingendo dal successivo pool con il prezzo più basso. Per garantire che la capacità desiderata sia soddisfatta, potresti ricevere On-Demand istanze da diversi pool.

Prioritaria

Il parco istanze utilizza la priorità che hai assegnato a ogni sostituzione del modello di avvio, avviando tipi di istanza prima nell'ordine per la priorità più alta. Questa strategia non può essere utilizzata con la selezione del tipo di istanza basata su attributi. Per un esempio di come utilizzare questa strategia di allocazione, consulta Dai priorità ai tipi di istanze in termini di capacità On-Demand.

Scelta della strategia di allocazione spot adeguata

Puoi ottimizzare il tuo parco istanze in base al tuo caso d'uso scegliendo la strategia di allocazione spot appropriata.

Equilibrio tra prezzo più basso e capacità disponibile

Per bilanciare i compromessi tra i pool di capacità spot con il prezzo più basso e i pool di capacità spot con la massima capacità disponibile, ti consigliamo di utilizzare la strategia di allocazione con ottimizzazione per prezzo e capacità. Questa strategia decide a quali pool richiedere le istanze spot tenendo conto sia del prezzo dei pool sia della capacità di istanze spot disponibile in tali pool. Ciò significa che le istanze Spot vengono richieste dai pool con maggiori probabilità di interruzione nel breve termine, tenendo comunque conto del prezzo.

Se il tuo parco istanze esegue carichi di lavoro resilienti e stateless, tra cui applicazioni containerizzate, microservizi, applicazioni Web, processi di dati e analisi ed elaborazione in batch, utilizza la strategia di allocazione con ottimizzazione per prezzo e capacità per risparmiare sui costi e disporre di una capacità ottimale.

Se il parco istanze esegue carichi di lavoro che possono avere un costo più elevato di interruzione associato al riavvio del lavoro, ti consigliamo implementare i checkpoint affinché le applicazioni possano riavviarsi da quel punto in caso di interruzione. Utilizzando i checkpoint, la strategia di allocazione con ottimizzazione per prezzo e capacità è una buona scelta per questi carichi di lavoro perché alloca la capacità dai pool con il prezzo più basso che offrono anche una bassa frequenza di interruzione delle istanze spot.

Per configurazioni JSON di esempio che utilizzano la strategia di allocazione con ottimizzazione per prezzo e capacità, consulta quanto segue:

- Parco istanze EC2 – Esempio 10: avvio di istanze spot in un parco istanze ottimizzato per prezzo e capacità
- Parco istanze spot – Esempio 11: avvio di istanze Spot in un prezzo CapacityOptimized parco istanze

Quando i carichi di lavoro hanno un costo di interruzione elevato

Facoltativamente, è possibile utilizzare la strategia con ottimizzazione per capacità se si eseguono carichi di lavoro che utilizzano tipi di istanze con prezzi simili o in cui il costo dell'interruzione è così significativo che qualsiasi risparmio sui costi è inadeguato rispetto a un aumento marginale delle interruzioni. Questa strategia alloca la capacità dai pool di capacità spot con maggiore disponibilità che offrono una possibilità minore di interruzioni, il che può ridurre il costo complessivo del carico di lavoro.

Quando è necessario ridurre al minimo la possibilità di interruzione ma la preferenza per determinati tipi di istanza è importante, puoi esprimere le priorità dei pool utilizzando la strategia di allocazione con priorità ottimizzata per capacità e quindi impostare l'ordine dei tipi di istanza da utilizzare dalla priorità più alta alla più bassa.

Tieni presente che quando stabilisci le priorità per l'ottimizzazione della capacità, le stesse priorità vengono applicate anche alle On-Demand istanze se la strategia di On-Demand allocazione è impostata su priorità. Inoltre, per il parco istanze spot, l'utilizzo delle priorità è supportato solo se il parco istanze utilizza un modello di avvio.

Per configurazioni JSON di esempio che utilizzano la strategia di allocazione con ottimizzazione per capacità, consulta quanto segue:

- Parco istanze EC2 – Esempio 8: Avviare le istanze spot in un parco istanze ottimizzato per la capacità
- Parco istanze spot – Esempio 9: Avvia le istanze spot in un parco istanze ottimizzato per la capacità

Per configurazioni JSON di esempio che utilizzano la strategia di allocazione con priorità ottimizzata per capacità, consulta quanto segue:

- Parco istanze EC2 – Esempio 9: Avviare le istanze spot in un parco istanze ottimizzato per la capacità con priorità
- Parco istanze spot – Esempio 10: Avviare le istanze spot in un parco istanze ottimizzato per la capacità con priorità

Quando il carico di lavoro è flessibile in termini di tempo e la capacità disponibile non è un fattore rilevante

Se il parco istanze è piccolo o viene eseguito per un breve periodo di tempo, puoi utilizzare la strategia con ottimizzazione per prezzo e capacità per massimizzare i risparmi sui costi pur tenendo conto della capacità disponibile.

Quando il parco istanze è grande o viene eseguito per un lungo periodo di tempo

Se il parco istanze è grande o funziona per un lungo periodo di tempo, puoi aumentare la disponibilità del parco istanze distribuendo la Istanze spot tra più pool utilizzando la strategia diversificata. Ad esempio, se il parco istanze specifica 10 pool e una capacità target pari a 100 istanze, il parco istanze avvia 10 istanze spot in ogni pool. Se il prezzo Spot per un pool supera il prezzo massimo per tale pool, solo il 10% del parco istanze ne è interessato. L'utilizzo di questa strategia rende inoltre il parco istanze meno sensibile agli aumenti del prezzo Spot in ogni pool unico nel tempo. Con la strategia diversificata, il parco istanze Spot non inserisce le istanze Spot in nessun pool con un prezzo Spot uguale o superiore al prezzo. On-Demand

Mantenimento della capacità target per le istanze Spot

Dopo che le istanze spot sono terminate a causa di una modifica del prezzo di Spot o della capacità disponibile di un pool di capacità spot, un parco istanze di tipo `maintain` avvia il istanze spot di

sostituzione. La strategia di allocazione determina i pool da cui vengono avviate le istanze sostitutive, come segue:

- Se la strategia di allocazione è ottimizzata per prezzo e capacità, il parco istanze avvia le istanze sostitutive nei pool che hanno la massima capacità disponibile di istanze spot tenendo in considerazione e identificando anche i pool con il prezzo più basso con una capacità disponibile elevata.
- Se la strategia di allocazione è ottimizzata per capacità, il parco istanze avvia le istanze sostitutive nei pool che hanno la massima capacità disponibile di istanze spot.
- Se la strategia di allocazione è diversificata, il parco istanze distribuisce le Istanze spot sostitutive nei pool rimanenti.

Dai priorità ai tipi di istanze in termini di capacità On-Demand

Quando una flotta EC2 o una flotta Spot tenta di soddisfare la tua On-Demand capacità, per impostazione predefinita avvia prima il tipo di istanza con il prezzo più basso. Se la strategia di On-Demand allocazione è impostata su una priorità, la flotta utilizza la priorità per determinare quale tipo di istanza utilizzare per primo per soddisfare la capacità. On-Demand La priorità è assegnata alla sostituzione del modello di avvio e la priorità più alta viene lanciata per prima.

Esempio: assegnare priorità ai tipi di istanza

Ad esempio, hai configurato tre sostituzioni dei modelli di avvio, ognuna con un tipo di istanza diversa.

Il On-Demand prezzo per i tipi di istanza varia. Di seguito sono riportati i tipi di istanza utilizzati in questo esempio, elencati in ordine di prezzo, a partire dal tipo di istanza più economico:

- `m4.large`: meno costosa
- `m5.large`
- `m5a.large`

Se non si utilizza la priorità per determinare l'ordine, il parco istanze soddisfa la On-Demand capacità partendo dal tipo di istanza meno costoso.

Tuttavia, poniamo che tu non abbia utilizzato le istanze riservate `m5.large` che vuoi utilizzare per prime. È possibile impostare la priorità di sostituzione del modello di avvio in modo che i tipi di istanze vengano utilizzati nell'ordine di priorità, come segue:

- `m5.large`: priorità 1
- `m4.large`: priorità 2
- `m5a.large`: priorità 3

Utilizza il ribilanciamento della capacità nel parco istanze EC2 e nel parco istanze spot per sostituire le istanze spot a rischio

Con il ribilanciamento della capacità, il parco istanze EC2 o il parco istanze spot possono mantenere la capacità spot desiderata sostituendo in modo proattivo le istanze spot a rischio di interruzione. Quando un'istanza Spot è a rischio elevato di interruzione, Amazon EC2 invia un suggerimento di ribilanciamento. Se il ribilanciamento della capacità è abilitato, il suggerimento di ribilanciamento innesca l'avvio di una nuova istanza Spot prima che l'istanza a rischio venga interrotta.

Il ribilanciamento della capacità consente di mantenere la disponibilità del carico di lavoro aumentando proattivamente il parco istanze con nuove istanze spot prima che le istanze in esecuzione vengano interrotte da Amazon EC2.

Per configurare il parco istanze EC2 per usare il ribilanciamento della capacità per avviare un'istanza spot sostitutiva

Utilizza il comando create-fleet e i parametri pertinenti nella struttura `MaintenanceStrategies`. Per una configurazione JSON di esempio, consulta Esempio 7: Configurare il ribilanciamento della capacità per avviare la sostituzione delle istanze spot.

Per configurare il parco istanze spot per usare il ribilanciamento della capacità per avviare un'istanza spot sostitutiva

Puoi utilizzare la console Amazon EC2 o la AWS CLI per configurare il ribilanciamento della capacità.

(Console) Quando si crea il parco istanze spot, seleziona la casella di spunta Ribilanciamento capacità. Per ulteriori informazioni, consulta la fase 6.d in Crea una richiesta di parco istanze spot utilizzando parametri definiti.

(AWS CLI) Utilizza il comando request-spot-fleet e i parametri pertinenti nella struttura `SpotMaintenanceStrategies`. Per una configurazione JSON di esempio, consulta Esempio 8: Configura il ribilanciamento della capacità per avviare la sostituzione delle istanze spot.

Argomenti

- Limitazioni

- Opzioni di configurazione
- Considerazioni

Limitazioni

- Il ribilanciamento della capacità è disponibile solo per i parchi istanza di tipo `maintain`.
- Quando il parco istanze è in esecuzione, non è possibile modificare l'impostazione di ribilanciamento della capacità. Per modificare l'impostazione di ribilanciamento capacità, è necessario eliminare il parco istanze e crearne uno nuovo.

Opzioni di configurazione

`ReplacementStrategy` per il parco istanze EC2 e il parco istanze spot supporta i due seguenti valori:

`launch-before-terminate`

Amazon EC2 termina le istanze spot che ricevono una notifica di ribilanciamento dopo avere avviato le nuove istanze spot sostitutive. Se si specifica `launch-before-terminate`, occorre specificare un valore anche per `termination-delay`. Dopo l'avvio delle nuove istanze sostitutive, Amazon EC2 attende la durata di `termination-delay`, quindi termina le vecchie istanze. Per `termination-delay`, il minimo è 120 secondi (2 minuti) e il massimo è di 7200 secondi (2 ore).

Consigliamo di utilizzare `launch-before-terminate` solo se è possibile prevedere il tempo necessario per il completamento delle procedure di arresto dell'istanza. Ciò garantirà che le vecchie istanze vengano terminate solo dopo il completamento delle procedure di arresto. Tenere presente che Amazon EC2 può interrompere le vecchie istanze con un avviso di due minuti prima di `termination-delay`.

Consigliamo vivamente di non utilizzare la strategia di allocazione `lowest-price` (parco istanze EC2) o `lowestPrice` (parco istanze spot) insieme a `launch-before-terminate` per evitare di avere istanze spot sostitutive che presentano anche un rischio elevato di interruzione.

`launch`

Amazon EC2 avvia le istanze spot sostitutive quando viene emessa una notifica di ribilanciamento per le istanze spot esistenti. Amazon EC2 non termina le istanze che ricevono una notifica di

ribilanciamento. È possibile terminare le vecchie istanze o lasciarle in esecuzione. Saranno addebitati i costi per entrambe le istanze durante la loro esecuzione.

Considerazioni

Se si configura un parco istanze EC2 o un parco istanze spot per il ribilanciamento della capacità, è necessario considerare quanto segue:

Fornisci il maggior numero possibile di pool di capacità spot nella richiesta

Configura il parco istanze per usare molteplici tipi di istanza e zone di disponibilità. Ciò fornisce la flessibilità necessaria per avviare Istanze spot in vari pool di capacità spot. Per ulteriori informazioni, consulta Essere flessibili riguardo tipi di istanza e zone di disponibilità.

Evitare un rischio elevato di interruzione delle istanze spot sostitutive

Per evitare un rischio elevato di interruzione, consigliamo la strategia di allocazione `capacity-optimized` o `capacity-optimized-prioritized`. Queste strategie garantiscono che le Spot Instances (Istanze spot) sostitutive vengano avviate nei pool di capacità spot ottimali per cui è meno probabile che vengano interrotte nel prossimo futuro. Per ulteriori informazioni, consulta Utilizzo della strategia di allocazione ottimizzata per prezzo e capacità.

Se si utilizza la strategia di allocazione `lowest-price`, le istanze spot sostitutive possono comportare un elevato rischio di interruzione. Questo perché Amazon EC2 avvierà sempre le istanze nel pool con capacità disponibile al prezzo più basso in quel momento, anche se è probabile che le istanze spot sostitutive vengano interrotte subito dopo l'avvio.

Amazon EC2 avvierà una nuova istanza solo se la disponibilità è uguale o migliore

Uno degli obiettivi del ribilanciamento della capacità è migliorare la disponibilità di un'istanza spot. Se un'istanza spot esistente riceve una raccomandazione di ribilanciamento, Amazon EC2 avvierà una nuova istanza solo se la nuova istanza fornisce una disponibilità uguale o migliore rispetto all'istanza esistente. Se il rischio di interruzione di una nuova istanza è peggiore di quello dell'istanza esistente, Amazon EC2 non avvierà una nuova istanza. Tuttavia, Amazon EC2 continuerà a valutare i pool di capacità spot e avvierà una nuova istanza se la disponibilità migliorerà.

È possibile che l'istanza esistente venga interrotta senza che Amazon EC2 avvii in modo proattivo una nuova istanza. In questo caso, Amazon EC2 tenterà di avviare una nuova istanza indipendentemente dal fatto che la nuova istanza presenti un rischio elevato di interruzione.

Il ribilanciamento della capacità non aumenta il tasso di interruzione dell'istanza Spot

Quando si abilita il ribilanciamento della capacità, non aumenta il tasso di interruzione dell'istanza spot (il numero di istanze Spot che vengono recuperate quando Amazon EC2 ha bisogno di capacità). Tuttavia, se il ribilanciamento della capacità rileva che un'istanza è a rischio di interruzione, Amazon EC2 tenterà immediatamente di avviare una nuova istanza. Il risultato è che potrebbero essere sostituite più istanze di quelle che sarebbero state sostituite se avessi aspettato che Amazon EC2 avviasse una nuova istanza dopo l'interruzione di quella a rischio.

Sebbene sia possibile sostituire più istanze mediante l'abilitazione del ribilanciamento delle capacità, è meglio prendersi più tempo per agire prima che le istanze vengano interrotte. Con un Avviso di interruzione dell'istanza Spot, in genere hai solo fino a due minuti per interrompere l'istanza. Con il ribilanciamento della capacità che avvia una nuova istanza in anticipo, offri ai processi esistenti maggiori possibilità di completamento sull'istanza a rischio, puoi avviare le procedure di chiusura dell'istanza e impedire la pianificazione di nuovi lavori sull'istanza a rischio. Puoi anche iniziare a preparare l'istanza appena avviata per assumere il controllo dell'applicazione. Con la sostituzione proattiva offerta dal ribilanciamento della capacità, puoi beneficiare di una continuità regolare.

Come esempio teorico per dimostrare i rischi e i benefici dell'utilizzo del ribilanciamento della capacità, osserviamo il seguente scenario:

- 14:00: viene ricevuto un suggerimento di ribilanciamento per l'istanza A e Amazon EC2 inizia immediatamente a tentare di avviare un'istanza sostitutiva B, dandoti il tempo di iniziare le procedure di arresto.*
- 14:30: viene ricevuto un suggerimento di ribilanciamento per l'istanza B, sostituita dall'istanza C dandoti il tempo di iniziare le procedure di arresto.*
- 14:32 — Se Capacity Rebalancing non fosse abilitato e se un avviso di interruzione dell'istanza Spot fosse stato ricevuto alle 14:32 PM per l'istanza A, avresti avuto a disposizione solo due minuti per intervenire, ma avresti avuto tempo fino a quest'ora. Instance-A

* Se `launch-before-terminate` è specificato, Amazon EC2 terminerà l'istanza a rischio dopo che l'istanza sostitutiva sarà online.

Amazon EC2 può avviare nuove Istanze spot sostitutive fino a quando la capacità soddisfatta non è il doppio della capacità obiettivo

Quando un parco istanze è configurato per il ribilanciamento della capacità, il parco istanze tenta di avviare una nuova istanza spot sostitutiva per ogni istanza spot che riceve un suggerimento

di ribilanciamento. Dopo che un'istanza spot riceve un suggerimento di ribilanciamento, non viene più conteggiata come parte della capacità evasa. A seconda della strategia di sostituzione, Amazon EC2 termina l'istanza dopo un ritardo di terminazione preconfigurato o la lascia in esecuzione. In questo modo è possibile eseguire operazioni di ribilanciamento sull'istanza.

Se il parco istanze raggiunge il doppio della capacità target, smette di lanciare nuove istanze sostitutive anche se le istanze sostitutive stesse ricevono una raccomandazione di ribilanciamento.

Ad esempio, se crei un parco istanze con una capacità target di 100 istanze spot. Tutte le istanze spot ricevono un suggerimento di ribilanciamento, cosicché Amazon EC2 avvia 100 istanze spot sostitutive. In questo modo il numero di istanze spot evase sale a 200, che è il doppio della capacità target. Alcune istanze sostitutive ricevono una raccomandazione di ribilanciamento, ma non vengono più avviate istanze sostitutive perché il parco istanze non può superare il doppio della capacità target.

Tenere presente che tutte le istanze vengono addebitate mentre sono in esecuzione.

Si consiglia di configurare il parco istanze in modo che termini le istanze spot che ricevono un suggerimento di ribilanciamento

Se si configura il parco istanze per il ribilanciamento della capacità, si consiglia di scegliere `launch-before-terminate` con un ritardo di terminazione appropriato solo se è possibile prevedere il tempo necessario per il completamento delle procedure di arresto dell'istanza. Ciò garantirà che le vecchie istanze vengano terminate solo dopo il completamento delle procedure di arresto.

Se si decide di terminare autonomamente le istanze suggerite per il ribilanciamento, si consiglia di monitorare il segnale di suggerimento del ribilanciamento ricevuto dalle istanze spot nel parco istanze. Monitorando il segnale, puoi eseguire rapidamente le operazioni di ribilanciamento sulle istanze interessate prima che Amazon EC2 le interrompa; poi potrai terminarle manualmente. Se non si terminano le istanze, verranno addebitati i relativi costi fintantoché sono in esecuzione. Amazon EC2 non termina automaticamente le istanze che ricevono un suggerimento di ribilanciamento.

Puoi configurare le notifiche utilizzando Amazon o i metadati dell'istanza. EventBridge Per ulteriori informazioni, consulta Monitorare i segnali di raccomandazione di ribilanciamento.

Il parco istanze non conteggia le istanze che ricevono una raccomandazione di ribilanciamento quando calcola la capacità evasa durante il dimensionamento orizzontale o verticale

Se il parco istanze è configurato per il ribilanciamento della capacità e si modifica la capacità di destinazione per l'aumento o la diminuzione, il parco istanze non conteggia le istanze contrassegnate per il ribilanciamento come parte della capacità evasa, come indicato di seguito:

- Riduzione orizzontale: se riduci la capacità obiettivo desiderata, Amazon EC2 termina le istanze che non sono contrassegnate per il ribilanciamento fino a quando non viene raggiunta la capacità desiderata. Le istanze contrassegnate per il ribilanciamento non vengono conteggiate per la capacità evasa.

  Ad esempio, crei un parco istanze con una capacità target di 100 istanze spot. 10 istanze ricevono un suggerimento di ribilanciamento, quindi Amazon EC2 avvia 10 nuove istanze sostitutive, con una capacità soddisfatta di 110 istanze. Riduci quindi la capacità obiettivo a 50 (riduzione orizzontale), ma la capacità soddisfatta è in realtà di 60 istanze, perché le 10 istanze contrassegnate per il ribilanciamento non vengono terminate da Amazon EC2. È necessario terminare manualmente queste istanze oppure lasciarle in esecuzione.
- Aumento orizzontale: se aumenti la capacità desiderata obiettivo, Amazon EC2 avvia nuove istanze fino al raggiungimento della capacità desiderata. Le istanze contrassegnate per il ribilanciamento non vengono conteggiate per la capacità evasa.

  Ad esempio, crei un Parco istanze con una capacità target di 100 istanze spot. 10 istanze ricevono un suggerimento di ribilanciamento, quindi il parco istanze avvia 10 nuove istanze sostitutive, con una capacità evasa di 110 istanze. Si aumenta quindi la capacità target a 200 (dimensionamento orizzontale), ma la capacità evasa effettiva è di 210 istanze, perché le 10 istanze contrassegnate per il ribilanciamento non vengono conteggiate dal parco istanze come parte della capacità target. È necessario terminare manualmente queste istanze oppure lasciarle in esecuzione.

Usa Capacity Reservations per riservare On-Demand capacità nella flotta EC2

Con On-Demand Capacity Reservations, puoi riservare la capacità di calcolo per le tue On-Demand istanze in una determinata zona di disponibilità per qualsiasi durata. È possibile configurare un parco istanze EC2 in modo da utilizzare prima le prenotazioni di capacità all'avvio delle istanze. On-Demand

On-Demand Le prenotazioni di capacità sono disponibili solo per la flotta EC2 con il tipo di richiesta impostato su. `instant`

Le prenotazioni delle capacità sono configurate come `open` o `targeted`. EC2 Fleet può avviare On-Demand le istanze in una delle due versioni `open` o in `targeted` Capacity Reservations, come segue:

- Se una prenotazione di capacità è`open`, On-Demand le istanze con attributi corrispondenti vengono eseguite automaticamente nella capacità riservata.
- Se una prenotazione di capacità lo è`targeted`, On-Demand le istanze devono specificatamente impostarla per essere eseguita nella capacità riservata. Ciò è utile per utilizzare una specifica prenotazione della capacità o per controllare quando utilizzare specifiche prenotazioni della capacità.

Se utilizzi le prenotazioni `targeted` di capacità nella tua flotta EC2, deve esserci un numero sufficiente di prenotazioni di capacità per raggiungere la On-Demand capacità prevista, altrimenti il lancio non riesce. Per evitare un errore di avvio, aggiungere invece le prenotazioni della capacità `targeted` a un gruppo di risorse e quindi prendere come obiettivo il gruppo di risorse. Il gruppo di risorse non deve disporre di un numero sufficiente di riserve di capacità; se esaurisce le riserve di capacità prima che la On-Demand capacità target sia raggiunta, la flotta può portare la capacità target rimanente alla capacità normale. On-Demand

Per utilizzare le prenotazioni della capacità con il parco istanze EC2

1. Configurare il parco istanze come tipo `instant`. Non è possibile utilizzare le prenotazioni della capacità per parchi istanze di altri tipi.
2. Configurare la strategia di utilizzo per le prenotazioni della capacità come `use-capacity-reservations-first`.
3. Nel modello di avvio, per Capacity reservation (Prenotazione della capacità) scegliere Open (Aperta) o Target by group (Obiettivo per gruppo). Se si sceglie Target by group (Definisci obiettivo in base al gruppo), specificare l'ID gruppo di risorsa della prenotazione della capacità.

Quando il parco tenta di raggiungere la On-Demand capacità, se rileva che più pool di istanze hanno prenotazioni di capacità corrispondenti inutilizzate, determina i pool in cui avviare On-Demand le istanze in base alla strategia di On-Demand allocazione (o). `lowest-price` `prioritized`

Risorse correlate

- Per esempi CLI su come configurare un parco veicoli per utilizzare le prenotazioni di capacità per soddisfare la On-Demand capacità, consultaEsempi di configurazioni di CLI per parco istanze EC2, in particolare, gli esempi da 5 a 7.
- Per un tutorial che illustra le fasi per creare prenotazioni della capacità, utilizzarle nel parco istanze e visualizzare quante prenotazioni della capacità sono rimaste, consulta Tutorial: configura la flotta EC2 per avviare On-Demand istanze utilizzando prenotazioni di capacità mirate
- Puoi anche configurare una flotta EC2 per avviare istanze su più tipi di prenotazione della capacità (prenotazioni di capacità, blocchi di On-Demand capacità per ML e prenotazioni di capacità interrompibili) utilizzando un unico gruppo di risorse per la prenotazione della capacità e, facoltativamente, ricorrere alla capacità. On-Demand Per fare ciò, usa `ReservedCapacityOptions` con il set to. `DefaultTargetCapacityType` `reserved-capacity` Per un tutorial, vedere Tutorial: configura la tua flotta EC2 per avviare le istanze in più tipi di prenotazione della capacità utilizzando un gruppo di risorse per la prenotazione della capacità.
- Per informazioni sulla configurazione di Capacity Reservations, consulta Riserva la capacità di calcolo con EC2 On-Demand Capacity Reservations e le Domande frequenti sulle prenotazioni On-Demand di capacità.

Lavorare con un parco istanze EC2

Per iniziare a utilizzare un parco istanze EC2, crea una richiesta che includa la capacità target totale, la capacità, la On-Demand capacità Spot e un modello di avvio che specifichi la configurazione per le istanze del parco istanze. Facoltativamente, puoi specificare parametri aggiuntivi o lasciare che il parco istanze utilizzi i valori predefiniti. Puoi anche etichettare la richiesta del parco istanze e le relative istanze e volumi, quando crei il parco istanze.

Il parco istanze avvia On-Demand le istanze quando c'è capacità disponibile e le istanze Spot quando il prezzo massimo supera il prezzo Spot e la capacità è disponibile.

Dopo il lancio della flotta, puoi descrivere la richiesta del parco veicoli, le istanze del parco veicoli e gli eventuali eventi del parco veicoli. Se necessario, puoi anche assegnare tag aggiuntivi.

Se è necessario modificare i parametri del parco istanze, come la capacità target totale, è possibile modificare il parco istanze, a condizione che sia configurato per mantenere la capacità. Non puoi modificare la capacità target di una richiesta una tantum dopo che è stata inviata.

La richiesta di parco istanze rimane attiva fino a quando non scade o fino a quando non viene eliminata. Quando elimini la richiesta del parco istanze, puoi interrompere le istanze o lasciarle in esecuzione. Se scegli di lasciarle in esecuzione, le On-Demand istanze restano attive finché non le chiudi, mentre le istanze Spot vengono interrotte o finché non sei tu a terminarle.

Argomenti

- Stati della richiesta parco istanze EC2
- Prerequisiti di parco istanze EC2
- Creazione di un parco istanze EC2
- Applicare un tag a una richiesta nuova o esistente per un parco istanze EC2 e alle istanze e ai volumi che avvia
- Descrivi un EC2 Fleet, le relative istanze e gli eventi
- Come modificare un parco istanze EC2
- Eliminazione di una richiesta del parco istanze EC2 e delle istanze nel parco istanze

Stati della richiesta parco istanze EC2

Una richiesta del parco istanze EC2 può essere uno dei diversi stati, ciascuno dei quali indica una fase diversa del ciclo di vita della richiesta e della relativa gestione delle istanze.

Una richiesta parco istanze EC2 può avere uno dei seguenti stati:

`submitted`

La richiesta parco istanze EC2 è in fase di valutazione ed Amazon EC2 si sta preparando ad avviare il numero previsto di istanze. Se una richiesta supera il limite del parco istanze, viene eliminata immediatamente.

`active`

La richiesta parco istanze EC2 è stata convalidata ed Amazon EC2 sta tentando di mantenere il numero previsto di istanze in esecuzione. La richiesta rimane in questo stato finché non viene modificata o eliminata.

`modifying`

La richiesta parco istanze EC2 è in fase di modifica. La richiesta rimane in questo stato finché la modifica non viene completamente elaborata o la richiesta non viene eliminata. È possibile

modificare solo un tipo di parco istanze `maintain`. Questo stato non si applica ad altri tipi di richieste.

`deleted_running`

La richiesta parco istanze EC2 viene eliminata e non avvia istanze spot aggiuntive. Le sue istanze esistenti continuano a essere eseguite finché non vengono interrotte o terminate manualmente. La richiesta rimane in questo stato finché tutte le istanze non vengono interrotte o terminate. Solo un parco istanze EC2 del tipo `maintain` o `request` può avere istanze in esecuzione dopo l'eliminazione della richiesta del parco istanze EC2. Un parco istanze `instant` eliminato con istanze in esecuzione non è supportato. Questo stato non si applica ai parchi istanze `instant`.

`deleted_terminating`

La richiesta del parco istanze EC2 viene eliminata e le sue istanze vengono terminate. La richiesta rimane in questo stato finché tutte le istanze non vengono terminate.

`deleted`

Il parco istanze EC2 viene eliminato e non ha istanze in esecuzione. La richiesta viene eliminata due giorni dopo e le sue istanze vengono terminate.

Prerequisiti di parco istanze EC2

Per creare un parco istanze EC2, devono esserci i prerequisiti seguenti:

- Modello di avvio
- Service-linked ruolo per la flotta EC2
- Concessione dell'accesso alle chiavi gestite dal cliente per l'uso con le AMI crittografate e gli snapshot EBS
- Autorizzazioni del parco istanze EC2 per gli utenti

Modello di avvio

Un modello di avvio specifica le informazioni di configurazione riguardo alle istanze da avviare, come il tipo di istanza e la zona di disponibilità. Per ulteriori informazioni sui modelli di avvio, consulta Archivia i parametri di avvio dell'istanza nei modelli di avvio di Amazon EC2.

Service-linked ruolo per la flotta EC2

Il ruolo `AWSServiceRoleForEC2Fleet` concede al parco istanze EC2 l'autorizzazione per richiedere, avviare e terminare le istanze, e applicarvi tag per tuo conto. Amazon EC2 utilizza questo ruolo collegato ai servizi per completare le operazioni seguenti:

- `ec2:RunInstances` – Avviare istanze.
- `ec2:RequestSpotInstances` – Richiesta Istanze spot.
- `ec2:TerminateInstances` – Terminare istanze
- `ec2:DescribeImages` – Descrivere Amazon Machine Image (AMI) per le istanze.
- `ec2:DescribeInstanceStatus` – Descrivere lo stato delle istanze.
- `ec2:DescribeSubnets` – Descrivere le sottoreti per le istanze.
- `ec2:CreateTags` – Aggiungere tag a parco istanze EC2, istanze e volumi.

Assicurati che questo ruolo esista prima di utilizzare AWS CLI o un'API per creare una flotta EC2.

> **Note**
>
> Un parco istanze EC2 `instant` non richiede questo ruolo.

Per creare il ruolo, utilizzare la console IAM nel modo seguente.

Per creare il AWSServiceRoleForEC2Fleet ruolo per EC2 Fleet

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. Nella pagina Seleziona un'entità attendibile, esegui le operazioni seguenti:
   a. Per Tipo di entità attendibile, scegli Servizio AWS .
   b. In Caso d'uso, per Servizio o caso d'uso, scegli EC2 – Parco istanze.

      > **Tip**
      >
      > Assicurati di scegliere EC2 – Parco istanze. Se scegli EC2, il caso d'uso EC2 – Parco istanze non appare nell'elenco dei casi d'uso. Lo use case EC2 - Fleet

creerà automaticamente una policy con le autorizzazioni IAM richieste e suggerirà AWSServiceRoleForEC2Fleet come nome del ruolo.

c. Scegli Next (Successivo).

5. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo).
6. Nella pagina Nomina, rivedi e crea scegli Crea ruolo.

Se non hai più bisogno di usare EC2 Fleet, ti consigliamo di eliminare il ruolo. AWSServiceRoleForEC2Fleet Dopo che questo ruolo è stato eliminato dal proprio account, è possibile creare di nuovo il ruolo se si crea un altro parco istanze.

Per ulteriori informazioni, consulta Service-linked i ruoli nella IAM User Guide.

Concessione dell'accesso alle chiavi gestite dal cliente per l'uso con le AMI crittografate e gli snapshot EBS

Se specifichi un'AMI crittografata o uno snapshot Amazon EBS crittografato nella tua flotta EC2 e utilizzi una AWS KMS chiave per la crittografia, devi concedere al AWSServiceRoleForEC2Fleet ruolo l'autorizzazione a utilizzare la chiave gestita dal cliente in modo che Amazon EC2 possa avviare istanze per tuo conto. Per farlo, occorre aggiungere una concessione alla chiave gestita dal cliente, come mostrato nella procedura seguente.

Nel processo di assegnazione delle autorizzazioni, le concessioni rappresentano un'alternativa alle policy delle chiavi. Per ulteriori informazioni, consulta Utilizzo delle concessioni e Utilizzo delle policy delle chiavi in AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .

Per concedere al AWSServiceRoleForEC2Fleet ruolo le autorizzazioni per l'utilizzo della chiave gestita dal cliente

- Utilizza il comando create-grant per aggiungere una concessione alla chiave gestita dal cliente e per specificare il principale (il ruolo AWSServiceRoleForEC2Fleet collegato al servizio) a cui è concessa l'autorizzazione per eseguire le operazioni consentite dalla concessione. La chiave gestita dal cliente è specificata dal parametro `key-id` e dall'ARN della chiave gestita dal cliente. L'entità principale è specificata dal `grantee-principal` parametro e dall'ARN del ruolo collegato al servizio. AWSServiceRoleForEC2Fleet

```
aws kms create-grant \
    --region us-east-1 \
```

```
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Autorizzazioni del parco istanze EC2 per gli utenti

Se gli utenti creano o gestiscono un parco istanze EC2, assicurati di concedere loro le autorizzazioni richieste.

Per creare una policy per il parco istanze EC2

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Policy.
3. Scegli Create Policy (Crea policy).
4. Nella pagina Create policy (Crea policy), selezionare la scheda JSON, sostituire il testo con il seguente, quindi selezionare Review policy (Rivedi policy).

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
              "iam:ListRoles",
              "iam:PassRole",
              "iam:ListInstanceProfiles"
            ],
            "Resource":"arn:aws:iam::123456789012:role/DevTeam*"
```

```
        }
    ]
}
```

`ec2:*` concede a un utente l'autorizzazione per chiamare tutte le operazioni API Amazon EC2. Per limitare l'utente a specifiche operazioni API Amazon EC2, è necessario invece indicare tali azioni.

L'utente deve avere l'autorizzazione per chiamare l'operazione `iam:ListRoles` per enumerare i ruoli IAM esistenti, l'operazione `iam:PassRole` per specificare il ruolo del parco istanze EC2 e l'operazione `iam:ListInstanceProfiles` per enumerare i profili dell'istanza esistenti.

(Facoltativo) Per consentire a un utente di creare ruoli o profili dell'istanza utilizzando la console IAM, devi inoltre aggiungere le operazioni seguenti alla policy:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

5. Nella pagina Review policy (Rivedi policy), immettere un nome policy e una descrizione, poi selezionare Create policy (Crea policy).
6. Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

   - 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 Create a role for a third-party identity provider (federation) della Guida per l'utente IAM.

   - Utenti IAM:

     - Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina Create a role for an IAM user della Guida per l'utente IAM.

- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente IAM.

Creazione di un parco istanze EC2

Per creare un EC2 Fleet, definisci la configurazione del parco istanze in un file JSON e fai riferimento al file con il comando create-fleet della . Nel file JSON, devi specificare la capacità di destinazione totale per la flotta, le capacità target separate per le istanze Spot e le istanze e un modello di avvio che definisca la configurazione per On-Demand le istanze del parco, ad esempio un'AMI, un tipo di istanza, una sottorete o una zona di disponibilità e uno o più gruppi di sicurezza. Puoi facoltativamente specificare configurazioni aggiuntive, come i parametri per sovrascrivere la configurazione del modello di lancio, le strategie di allocazione per la selezione delle On-Demand istanze Spot e delle istanze dai pool di capacità EC2 e l'importo massimo che sei disposto a pagare per la flotta. Per ulteriori informazioni, consulta Opzioni di configurazione per il parco istanze EC2 o il parco istanze spot.

Il parco istanze EC2 avvia On-Demand le istanze quando la capacità è disponibile e le istanze Spot quando il prezzo massimo supera il prezzo Spot e la capacità è disponibile.

Se il parco istanze include istanze spot ed è di tipo `maintain`, Amazon EC2 tenterà di mantenere la capacità target del parco istanze quando le istanze spot vengono interrotte.

Limitazioni di EC2 Fleet

Le limitazioni seguenti riguardano EC2 Fleet:

- La creazione di un parco istanze EC2 è disponibile solo tramite l'API Amazon EC2, la AWS CLI, gli SDK AWS e CloudFormation.
- Una richiesta EC2 Fleet non può estendersi a più regioni. AWS È necessario creare un EC2 Fleet separato per ciascuna regione.
- Una richiesta di EC2 Fleet non può comprendere sottoreti diverse della stessa zona di disponibilità.

Creazione di un parco istanze EC2

Per avviare un parco istanze utilizzando il parco istanze EC2, devi solo specificare i seguenti parametri nella richiesta del parco istanze, e il parco istanze utilizzerà i valori predefiniti per gli altri parametri:

- `LaunchTemplateId` o `LaunchTemplateName` – Specifica il modello di avvio da utilizzare (che contiene i parametri per le istanze da avviare, come il tipo di istanza e la zona di disponibilità)
- `TotalTargetCapacity`: specifica la capacità di destinazione totale per il parco istanze
- `DefaultTargetCapacityType`— Specifica se l'opzione di acquisto predefinita è o Spot On-Demand

Per sostituire i parametri specificati nel modello di avvio, puoi specificare una o più sostituzioni. Ciascuna sostituzione può variare a seconda del tipo di istanza, della zona di disponibilità, della sottorete e del prezzo massimo e può includere una capacità ponderata diversa. In alternativa alla specifica di un tipo di istanza, è possibile specificare gli attributi che un'istanza deve avere e Amazon EC2 identificherà tutti i tipi di istanza con tali attributi. Per ulteriori informazioni, consulta Specifica gli attributi per la selezione del tipo di istanza per il parco del tipo per il parco istanze EC2 o il parco istanze Spot.

Per le flotte di tipo EC2`instant`, puoi anche sovrascrivere i seguenti parametri del modello di avvio:

- `IamInstanceProfile`— Il profilo dell'istanza IAM da associare alle istanze. Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.
- `KeyName`— Il nome della coppia di chiavi da utilizzare per le istanze. Per ulteriori informazioni, consulta Coppie di chiavi Amazon EC2 e istanze Amazon EC2.
- `MetadataOptions`— La configurazione del servizio di metadati delle istanze per le istanze. Per ulteriori informazioni, consulta Utilizzo del servizio di metadati di istanza per accedere ai metadati dell'istanza.

Per il parco istanze EC2 di tipo`instant`, puoi specificare un parametro Systems Manager anziché l'ID dell'AMI. Puoi specificare il parametro Systems Manager nella sostituzione o nel modello di avvio. Per ulteriori informazioni, consulta Usare un parametro Systems Manager invece di un'ID AMI.

Per le flotte EC2 di tipo`instant`, puoi anche specificare i dati utente a livello di specifica del modello di avvio utilizzando il parametro. `LaunchTemplateSpecificationUserData` Con questo parametro, puoi fornire dati utente con codifica base64 senza includerli nel modello di avvio stesso. I dati utente non devono superare i 16 KB prima della codifica base64.

Puoi specificare i parametri del parco istanze in un file JSON. Per informazioni su tutti i possibili parametri che è possibile specificare, consulta Visualizza tutte le opzioni di configurazione del parco istanze EC2.

Per gli esempi di configurazione del parco istanze, consulta Esempi di configurazioni di CLI per parco istanze EC2.

Al momento non è disponibile il supporto per la console per la creazione di un parco istanze EC2.

Per creare un parco istanze EC2

Utilizza il comando create-fleet per creare un parco istanze e specifica il file JSON che contiene i parametri di configurazione del parco istanze.

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Di seguito è riportato l'output di esempio per un parco istanze del tipo `request` o `maintain`.

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

Di seguito è riportato l'output di esempio per un parco istanze del tipo `instant` che ha avviato la capacità target.

La risposta include l'ID della zona di disponibilità, il nome della zona di disponibilità e l'ID della sottorete per ogni set di istanze avviate.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
```

```
        "i-9876543210abcdef9"
      ],
      "InstanceType": "c5.large",
      "Platform": null,
      "AvailabilityZoneId": "use1-az1",
      "AvailabilityZone": "us-east-1a",
      "SubnetId": "subnet-0123456789abcdefEXAMPLE"
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-5678901234abcdef0",
        "i-5432109876abcdef9"
      ],
      "AvailabilityZoneId": "use1-az1",
      "AvailabilityZone": "us-east-1a",
      "SubnetId": "subnet-0123456789abcdefEXAMPLE"
    }
  ]
}
```

Di seguito è riportato l'output di esempio per un parco istanze del tipo `instant` che ha avviato parte della capacità target con errori per le istanze che non erano state avviate.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
```

```
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientInstanceCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ]
  ]
}
```

Di seguito è riportato l'output di esempio per un parco istanze del tipo `instant` che non ha avviato istanze.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
```

```
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": []
}
```

Crea un parco istanze EC2 che sostituisca le istanze spot non integre

parco istanze EC2 controlla lo stato delle istanze nel parco istanze ogni due minuti. Lo stato di un'istanza è `healthy` o `unhealthy`.

parco istanze EC2 determina lo stato di un'istanza utilizzando i controlli dello stato forniti da Amazon EC2. Un'istanza viene determinata come `unhealthy` quando lo stato del controllo dello stato dell'istanza o del controllo dello stato del sistema è `impaired` per tre controlli dello stato di integrità consecutivi. Per ulteriori informazioni, consulta Verifiche dello stato delle istanze Amazon EC2.

È possibile configurare il parco istanze per sostituire le Istanze spot non integre. Dopo l'impostazione di `ReplaceUnhealthyInstances` su `true`, l'istanza spot viene sostituita quando viene segnalata come `unhealthy`. Durante la sostituzione di un'istanza spot non integra, il parco istanze può scendere al di sotto della sua capacità obiettivo.

Requisiti

- La sostituzione del controllo dello stato è supportata solo per Parchi istanze EC2 che mantengono una capacità target (parchi istanza del tipo `maintain`) e non con parchi istanza del tipo `request` o `instant`.
- La sostituzione del controllo dello stato è supportata solo per Istanze spot. Questa funzionalità non è supportata per On-Demand le istanze.
- È possibile configurare EC2 Fleet per sostituire le istanze non integre solo al momento della sua creazione.
- Gli utenti possono utilizzare la sostituzione del controllo dell'integrità solo se hanno l'autorizzazione a chiamare l'operazione `ec2:DescribeInstanceStatus`.

Per configurare un parco istanze EC2 per sostituire un Istanze spot non integro

1. Utilizza le informazioni per creare un parco istanze EC2 in Creazione di un parco istanze EC2.
2. Per configurare il parco istanze per sostituire Istanze spot non integre, nel file JSON, per `ReplaceUnhealthyInstances` specifica `true`.

Visualizza tutte le opzioni di configurazione del parco istanze EC2

Per visualizzare l'elenco completo dei parametri di configurazione del parco istanze EC2, è possibile generare un file JSON. Per una descrizione di ciascun parametro, consulta create-fleet.

Per generare un file JSON con tutti i parametri del parco istanze EC2 possibili

Utilizzare il comando create-fleet (AWS CLI) e il parametro `--generate-cli-skeleton` per generare un file JSON del parco istanze EC2 e indirizzare l'output in un file per salvarlo.

```
aws ec2 create-fleet \
    --generate-cli-skeleton input > ec2createfleet.json
```

Di seguito è riportato un output di esempio.

```
{
    "DryRun": true,
    "ClientToken": "",
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
```

```
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch"
            }
        },
        "InstanceInterruptionBehavior": "hibernate",
        "InstancePoolsToUseCount": 0,
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        },
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "",
                "LaunchTemplateName": "",
                "Version": ""
            },
            "Overrides": [
                {
                    "InstanceType": "r5.metal",
                    "MaxPrice": "",
                    "SubnetId": "",
                    "AvailabilityZone": "",
                    "WeightedCapacity": 0.0,
                    "Priority": 0.0,
                    "Placement": {
                        "AvailabilityZone": "",
                        "Affinity": "",
                        "GroupName": "",
                        "PartitionNumber": 0,
                        "HostId": "",
```

```
                    "Tenancy": "dedicated",
                    "SpreadDomain": "",
                    "HostResourceGroupArn": ""
                },
                "InstanceRequirements": {
                    "VCpuCount": {
                        "Min": 0,
                        "Max": 0
                    },
                    "MemoryMiB": {
                        "Min": 0,
                        "Max": 0
                    },
                    "CpuManufacturers": [
                        "amd"
                    ],
                    "MemoryGiBPerVCpu": {
                        "Min": 0.0,
                        "Max": 0.0
                    },
                    "ExcludedInstanceTypes": [
                        ""
                    ],
                    "InstanceGenerations": [
                        "previous"
                    ],
                    "SpotMaxPricePercentageOverLowestPrice": 0,
                    "OnDemandMaxPricePercentageOverLowestPrice": 0,
                    "BareMetal": "included",
                    "BurstablePerformance": "required",
                    "RequireHibernateSupport": true,
                    "NetworkInterfaceCount": {
                        "Min": 0,
                        "Max": 0
                    },
                    "LocalStorage": "excluded",
                    "LocalStorageTypes": [
                        "ssd"
                    ],
                    "TotalLocalStorageGB": {
                        "Min": 0.0,
                        "Max": 0.0
                    },
                    "BaselineEbsBandwidthMbps": {
```

```
                        "Min": 0,
                        "Max": 0
                    },
                    "AcceleratorTypes": [
                        "inference"
                    ],
                    "AcceleratorCount": {
                        "Min": 0,
                        "Max": 0
                    },
                    "AcceleratorManufacturers": [
                        "amd"
                    ],
                    "AcceleratorNames": [
                        "a100"
                    ],
                    "AcceleratorTotalMemoryMiB": {
                        "Min": 0,
                        "Max": 0
                    }
                }
            }
        ]
    }
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 0,
    "OnDemandTargetCapacity": 0,
    "SpotTargetCapacity": 0,
    "DefaultTargetCapacityType": "on-demand",
    "TargetCapacityUnitType": "memory-mib"
},
"TerminateInstancesWithExpiration": true,
"Type": "instant",
"ValidFrom": "1970-01-01T00:00:00",
"ValidUntil": "1970-01-01T00:00:00",
"ReplaceUnhealthyInstances": true,
"TagSpecifications": [
    {
        "ResourceType": "fleet",
        "Tags": [
            {
                "Key": "",
                "Value": ""
```

```
                }
            ]
        }
    ],
    "Context": ""
}
```

Applicare un tag a una richiesta nuova o esistente per un parco istanze EC2 e alle istanze e ai volumi che avvia

Per categorizzare e gestire le richieste del parco istanze EC2 e le istanze e i volumi che avvia, puoi contrassegnarle con tag contenenti metadati personalizzati. È possibile assegnare un tag a una richiesta parco istanze EC2 alla sua creazione o successivamente. Allo stesso modo, puoi assegnare un tag alle istanze e ai volumi quando vengono lanciati dal parco istanze o in un secondo momento.

Quando si applica un tag a una richiesta del parco istanze, alle istanze e ai volumi che vengono avviati dal parco istanze non vengono automaticamente applicati tag. È necessario applicare esplicitamente tag alle istanze e ai volumi avviati dal parco istanze. Puoi scegliere di assegnare tag solo alla richiesta del parco veicoli, o solo alle istanze lanciate dal parco veicoli, o solo ai volumi collegati alle istanze lanciate dal parco istanze, o solo alle interfacce di rete create dal parco veicoli, o a tutte.

> **Note**
>
> Per i tipi di `instant` parco veicoli, puoi contrassegnare i volumi collegati alle On-Demand istanze e alle istanze Spot. Puoi anche etichettare le interfacce di rete per `instant` i tipi di parco veicoli. Per `request` i `maintain` nostri tipi di flotta, puoi contrassegnare solo i volumi collegati alle On-Demand istanze.

Per ulteriori informazioni sul funzionamento dei tag, consultare Tagging delle risorse Amazon EC2..

Prerequisito

Concedi all'utente l'autorizzazione per taggare le risorse. Per ulteriori informazioni, consulta Esempio: aggiunta di tag alle risorse.

Per concedere a un utente l'autorizzazione per taggare le risorse

Creare una policy IAM che include quanto segue:

- L'operazione `ec2:CreateTags`. Ciò concede all'utente l'autorizzazione per creare tag.
- L'operazione `ec2:CreateFleet`. Ciò concede all'utente l'autorizzazione per creare una richiesta parco istanze EC2.
- Per `Resource`, si consiglia di specificare `"*"`. Ciò consente agli utenti di taggare tutti i tipi di risorse.

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- 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 Create a role for a third-party identity provider (federation) della Guida per l'utente IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina Create a role for an IAM user della Guida per l'utente IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente IAM.

Per applicare tag a una nuova richiesta parco istanze EC2

Per assegnare un tag a una richiesta parco istanze EC2 durante la sua creazione, specificare la coppia chiave-valore nel file JSON utilizzato per creare il parco istanze. Il valore di `ResourceType` deve essere `fleet`. Indicando un altro valore, la richiesta per il parco istanze fallisce.

Per applicare tag a istanze e volumi avviati da un parco istanze EC2

Per applicare tag alle istanze e ai volumi quando vengono avviate dal parco istanze, specificare i tag nel modello di lancio a cui fa riferimento la richiesta nel parco istanze EC2.

> **Note**
>
> Non è possibile applicare tag ai volumi collegati a Istanze spot che vengono avviati da un tipo di parco istanze `request` o `maintain`.

Per applicare tag a una richiesta di parco istanze EC2, un'istanza e un volume esistenti

Utilizzare il comando create-tags per aggiungere un tag alle risorse esistenti.

```
aws ec2 create-tags \
    --resources fleet-12a34b55-67cd-8ef9-
ba9b-9208dEXAMPLE i-1234567890abcdef0 vol-1234567890EXAMPLE \
    --tags Key=purpose,Value=test
```

Descrivi un EC2 Fleet, le relative istanze e gli eventi

Puoi descrivere la configurazione del tuo parco istanze EC2, le istanze nel tuo parco istanze EC2 e la cronologia degli eventi del tuo parco istanze EC2.

Processi

- Descrivere il parco istanze EC2
- Descrivi tutte le istanze nel tuo EC2 Fleet
- Descrivi la cronologia degli eventi per il parco istanze EC2

Descrivere il parco istanze EC2

AWS CLI

Per descrivere il tuo EC2 Fleet

Utilizza il comando describe-fleets.

```
aws ec2 describe-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Di seguito è riportato un output di esempio.

```
{
```

```
    "Fleets": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2022-02-09T03:35:52+00:00",
            "FleetId": "fleet-364457cd-3a7a-4ed9-83d0-7b63e51bb1b7",
            "FleetState": "active",
            "ExcessCapacityTerminationPolicy": "termination",
            "FulfilledCapacity": 2.0,
            "FulfilledOnDemandCapacity": 0.0,
            "LaunchTemplateConfigs": [
                {
                    "LaunchTemplateSpecification": {
                        "LaunchTemplateName": "my-launch-template",
                        "Version": "$Latest"
                    }
                }
            ],
            "TargetCapacitySpecification": {
                "TotalTargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "SpotTargetCapacity": 2,
                "DefaultTargetCapacityType": "spot"
            },
            "TerminateInstancesWithExpiration": false,
            "Type": "maintain",
            "ReplaceUnhealthyInstances": false,
            "SpotOptions": {
                "AllocationStrategy": "capacity-optimized",
                "InstanceInterruptionBehavior": "terminate"
            },
            "OnDemandOptions": {
                "AllocationStrategy": "lowestPrice"
            }
        }
    ]
}
```

PowerShell

Per descrivere il tuo EC2 Fleet

Utilizza il cmdlet Get-EC2FleetList.

```
Get-EC2FleetList `
```

```
    -FleetId fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Descrivi tutte le istanze nel tuo EC2 Fleet

L'elenco delle istanze in esecuzione riportato viene aggiornato periodicamente e potrebbe essere obsoleto.

AWS CLI

Per descrivere le istanze per l'EC2 Fleet specificato

Utilizza il comando describe-fleet-instances.

```
aws ec2 describe-fleet-instances \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Di seguito è riportato un output di esempio.

```
{
    "ActiveInstances": [
        {
            "InstanceId": "i-09cd595998cb3765e",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-86k84j6p"
        },
        {
            "InstanceId": "i-09cf95167ca219f17",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-dvxi7fsm"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

PowerShell

Per descrivere le istanze per l'EC2 Fleet specificato

Utilizza il cmdlet Get-EC2FleetInstanceList.

```
Get-EC2FleetInstanceList `
    -FleetId fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Descrivi la cronologia degli eventi per il parco istanze EC2

Per ulteriori informazioni sugli eventi nella cronologia degli eventi, consulta Tipi di eventi Parco istanze EC2

AWS CLI

Per descrivere gli eventi per l'EC2 Fleet specificato

Utilizza il comando describe-fleet-history.

```
aws ec2 describe-fleet-history \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2020-06-01T00:00:00Z
```

Di seguito è riportato un output di esempio.

```
{
    "HistoryRecords": [
        {
            "EventInformation": {
                "EventSubType": "submitted"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:05.000Z"
        },
        {
            "EventInformation": {
                "EventSubType": "active"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:15.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "t2.small, ami-07c8bc5c1ce9598c3, ...",
                "EventSubType": "progress"
            },
```

```
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-083a1c446e66085d2"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-090db02406cc3c2d6"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
    "LastEvaluatedTime": "1970-01-01T00:00:00.000Z",
    "StartTime": "2020-06-01T00:00:00.000Z"
}
```

PowerShell

Per descrivere gli eventi per l'EC2 Fleet specificato

Utilizza il cmdlet Get-EC2FleetHistory.

```
Get-EC2FleetHistory `
    -FleetId fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE `
    -UtcStartTime 2020-06-01T00:00:00Z
```

Come modificare un parco istanze EC2

Puoi modificare la capacità target totale, la capacità Spot e la On-Demand capacità di una flotta EC2. Puoi anche modificare se l'esecuzione delle istanze deve terminare quando la nuova capacità target totale scende al di sotto della dimensione attuale del parco istanze.

Considerazioni

Quando si modifica un parco istanze EC2, si consideri quanto segue:

- Tipo di parco istanze – È possibile modificare solo un parco istanze EC2 di tipo `maintain`. Non è possibile modificare un parco istanze EC2 di tipo `request` o `instant`.
- Parametri del parco istanze – È possibile modificare i parametri seguenti di un parco istanze EC2:
  - `target-capacity-specification` – Consente di aumentare o diminuire la capacità target per:
    - `TotalTargetCapacity`
    - `OnDemandTargetCapacity`
    - `SpotTargetCapacity`
  - `excess-capacity-termination-policy` – Indica se l'esecuzione delle istanze deve terminare quando la capacità target totale del parco istanze EC2 scende al di sotto della dimensione attuale del parco istanze. I valori validi sono:
    - `no-termination`
    - `termination`
- Comportamento del parco istanze in caso di aumento della capacità totale target: quando si aumenta la capacità target totale, il parco istanze EC2 avvia le istanze aggiuntive in base all'opzione di acquisto delle istanze specificata per`DefaultTargetCapacityType`, che è On-Demand Istanze o Istanze Spot, e in base alla strategia di allocazione specificata. ???
- Comportamento del parco istanze quando si diminuisce la capacità target spot – Quando si diminuisce la capacità target spot, il parco istanze EC2 elimina qualsiasi richiesta aperta che supera la nuova capacità di destinazione. È possibile richiedere che il parco istanze termini le istanze spot finché la dimensione del parco istanze non raggiunge la nuova capacità obiettivo. Quando un parco istanze EC2 termina un'istanza spot a seguito della diminuzione della capacità obiettivo, l'istanza riceve un avviso di interruzione dell'istanza spot.

  Le istanze vengono selezionate per la terminazione in base alla strategia di allocazione:
  - `capacity-optimized`: termina le istanze dai pool con la minore capacità disponibile.
  - `price-capacity-optimized`: utilizza una combinazione di prezzo e capacità disponibile: termina le istanze dai pool con la minore capacità disponibile e che sono più costose tra questi pool.
  - `diversified`: termina le istanze in tutti i pool.
  - `lowest-price`: termina le istanze dai pool più costosi.

In alternativa, puoi richiedere che l'EC2 Fleet mantenga il parco istanze alla sua dimensione attuale, ma che non sostituisca le istanze spot che vengono interrotte o tutte le istanze che vengono terminate manualmente.

- Stato del parco istanze – È possibile modificare un parco istanze EC2 che risulta nello stato `submitted` o `active`. Quando si modifica un parco istanze, esso acquisisce lo stato `modifying`.

Comandi per modificare un parco istanze EC2

AWS CLI

Per modificare la capacità target totale di un parco istanze EC2

Utilizza il comando modify-fleet.

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=20
```

Se diminuisci la capacità target, ma desideri mantenere il parco istanze alla dimensione attuale, puoi modificare l'esempio precedente come segue.

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=10 \
    --excess-capacity-termination-policy no-termination
```

PowerShell

Per modificare la capacità target totale di un parco istanze EC2

Utilizza il cmdlet Edit-EC2Fleet.

```
Edit-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacitySpecification_TotalTargetCapacity 20
```

Se diminuisci la capacità target, ma desideri mantenere il parco istanze alla dimensione attuale, puoi modificare l'esempio precedente come segue.

```
Edit-EC2Fleet `
```

```
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacitySpecification_TotalTargetCapacity 20 `
    -ExcessCapacityTerminationPolicy "NoTermination"
```

Eliminazione di una richiesta del parco istanze EC2 e delle istanze nel parco istanze

Se una richiesta del parco istanze EC2 non è più necessaria, puoi eliminarla. Dopo aver eliminato una richiesta di parco istanze, tutte le richieste Spot associate al parco istanze vengono eliminate, in modo che nessuna istanza spot nuova venga avviata per tale parco.

Quando si elimina una richiesta del parco istanze EC2, devi specificare se si desidera terminare tutte le relative istanze. Queste includono sia le istanze che le istanze Spot. On-Demand Per i parchi istanze `instant`, il parco istanze EC2 deve interrompere le istanze in cui il parco istanze viene eliminato. Un parco istanze `instant` eliminato con istanze in esecuzione non è supportato.

> **Warning**
>
> La terminazione di un'istanza è permanente e irreversibile.
> Dopo aver terminato un'istanza, non puoi più connetterti a essa e non puoi ripristinarla. Inoltre, tutti i volumi Amazon EBS collegati e configurati per essere eliminati in caso di terminazione vengono eliminati in modo definitivo e non possono essere recuperati. Tutti i dati archiviati nei volumi di archivio dell'istanza vengono persi in modo definitivo. Per ulteriori informazioni, consulta Come funziona la terminazione delle istanze.
> Prima di terminare un'istanza, assicurati di aver eseguito il backup di tutti i dati che devi mantenere dopo la terminazione sull'archivio persistente.

Se specifichi che le istanze devono essere terminate quando elimini la richiesta del parco istanze, quest'ultima acquisisce lo stato `deleted_terminating`. Altrimenti, esso acquisisce lo stato `deleted_running` e l'esecuzione delle istanze continua finché esse non vengono interrotte o terminate manualmente.

Restrizioni

- È possibile eliminare fino a 25 parchi istanze di tipo `instant` in una singola operazione.
- È possibile eliminare fino a 100 parchi istanze di tipo `maintain` o `request` in una singola operazione.

- È possibile eliminare fino a 125 parchi istanze in una singola operazione, a condizione che non si superi la quota per ciascun tipo di parco istanze, come specificato sopra.
- Se si supera il numero di parchi specificato da eliminare, non viene eliminato alcun parco istanze.
- Un parco istanze `instant` eliminato con istanze in esecuzione non è supportato. Quando elimini un parco istanze `instant`, Amazon EC2 termina automaticamente tutte le sue istanze. Per i parchi istanze `instant` con più di 1.000 istanze, la richiesta di eliminazione potrebbe avere esito negativo. Se il tuo parco istanze ha più di 1.000 istanze, termina innanzitutto la maggior parte delle istanze manualmente, lasciandone 1.000 o meno. Poi elimina il parco istanze e le istanze rimanenti verranno terminate automaticamente.

AWS CLI

Per eliminare una richiesta dell'EC2 Fleet e terminare le relative istanze

Utilizza il comando delete-fleets con l'opzione `--terminate-instances`.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Di seguito è riportato un output di esempio.

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
            "PreviousFleetState": "active",
            "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
        }
    ]
}
```

Per eliminare una richiesta dell'EC2 Fleet senza terminare le relative istanze

Modifica l'esempio precedente utilizzando invece l'opzione `--no-terminate-instances`. `--no-terminate-instances` non è supportato per i parchi istanze `instant`.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
```

```
    --no-terminate-instances
```

Di seguito è riportato un output di esempio.

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_running",
            "PreviousFleetState": "active",
            "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafa4c6b7dcEXAMPLE"
        }
    ]
}
```

PowerShell

Per eliminare una richiesta dell'EC2 Fleet e terminare le relative istanze

Utilizza il Remove-EC2Fleet cmdlet con il parametro. `-TerminateInstance`

```
Remove-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $true
```

Per eliminare una richiesta dell'EC2 Fleet senza terminare le relative istanze

Modifica l'esempio precedente cambiando il valore del parametro `-TerminateInstance`.

```
Remove-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $false
```

Risoluzione dei problemi di eliminazione di un parco istanze

Se una richiesta dell'EC2 Fleet non viene eliminata, `UnsuccessfulFleetDeletions` nell'output restituisce l'ID della richiesta dell'EC2 Fleet, un codice di errore e un messaggio di errore.

I codici di errore sono:

- `ExceededInstantFleetNumForDeletion`

- `fleetIdDoesNotExist`
- `fleetIdMalformed`
- `fleetNotInDeletableState`
- `NoTerminateInstancesNotSupported`
- `UnauthorizedOperation`
- `unexpectedError`

Risoluzione dei problemi di **`ExceededInstantFleetNumForDeletion`**

Se si tenta di eliminare più di 25 parchi istanze `instant` in una singola richiesta, viene restituito l'errore `ExceededInstantFleetNumForDeletion`. Di seguito è riportato l'output di esempio per questo errore.

```
{
    "UnsuccessfulFleetDeletions": [
     {
          "FleetId": " fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
          "Error": {
                 "Message": "Can't delete more than 25 instant fleets in a single
 request.",
                 "Code": "ExceededInstantFleetNumForDeletion"
           }
     },
     {
           "FleetId": "fleet-9a941b23-0286-5bf4-2430-03a029a07e31",
           "Error": {
                 "Message": "Can't delete more than 25 instant fleets in a single
 request.",
                 "Code": "ExceededInstantFleetNumForDeletion"
            }
     }
     .
     .
     .
     ],
     "SuccessfulFleetDeletions": []
}
```

Risoluzione dei problemi di **`NoTerminateInstancesNotSupported`**

Se si specifica che le istanze di un parco istanze `instant` non devono essere terminate quando si elimina il parco istanze, viene restituito l'errore `NoTerminateInstancesNotSupported`. `--no-terminate-instances` non è supportato per i parchi istanze `instant`. Di seguito è riportato l'output di esempio per questo errore.

```
{
      "UnsuccessfulFleetDeletions": [
            {
                  "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
                  "Error": {
                         "Message": "NoTerminateInstances option is not supported for
 instant fleet",
                         "Code": "NoTerminateInstancesNotSupported"
                   }
            }
       ],
       "SuccessfulFleetDeletions": []
}
```

Risoluzione dei problemi di **`UnauthorizedOperation`**

Se non si dispone dell'autorizzazione per terminare le istanze, viene restituito l'errore `UnauthorizedOperation` quando si elimina un parco istanze che deve terminare le relative istanze. Di seguito è riportata la risposta di errore.

```
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not
 authorized to perform this
operation. Encoded authorization failure message: VvuncIxj7Z_CPGNYXWqnuFV-
YjByeAU66Q9752NtQ-I3-qnDLWs6JLFd
KnSMMiq5s6cGqjjPtEDpsnGHzzyHasFHOaRYJpaDVravoW25azn6KNkUQQlFwhJyujt2dtNCdduJfrqcFYAjlEiRMkfDHt7
BHturzDK6A560Y2nDSUiMmAB1y9UNtqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVHbY9JhLvGypLcMUjtJ76
VPiU5v2s-
UgZ7h0p2yth6ysUdhlONg6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-
EMhekLFZeJLr
DtYOpYcEl4_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1PxODZuqWHs23YXWVywzgnLtHeRf2o4lUhGBw17mXsS07k7
PT9vrHtQiILor5VVTsjSPWg7edj__1rsnXhwPSu8gI48ZLRGrPQqFq0RmKO_QIE8N8s6NWzCK4yoX-9gDcheurOGpkprPIC
</Message></Error></Errors><RequestID>89b1215c-7814-40ae-a8db-41761f43f2b0</
RequestID></Response>
```

Per risolvere l'errore, è necessario aggiungere l'operazione `ec2:TerminateInstances` alla policy IAM, come illustrato nell'esempio seguente.

Lavorare con un parco istanze spot

> **Important**
>
> Sconsigliamo vivamente di utilizzare Spot Fleet perché utilizza un'API legacy senza investimenti pianificati. Se desideri gestire il ciclo di vita dell'istanza, utilizza invece EC2 Fleet. Se non desideri gestire il ciclo di vita dell'istanza, utilizza invece un gruppo Auto Scaling. Usa Spot Fleet solo se hai bisogno del supporto da console per un caso d'uso in cui utilizzeresti EC2 Fleet. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Per iniziare a utilizzare una flotta Spot, crea una richiesta che includa la capacità totale di destinazione per le istanze Spot, una On-Demand parte opzionale, e specifica manualmente un'AMI e una coppia di chiavi oppure specifica un modello di avvio che includa la configurazione per le istanze del parco istanze. Facoltativamente, puoi specificare parametri aggiuntivi o lasciare che il parco istanze utilizzi i valori predefiniti. Puoi anche etichettare la richiesta del parco istanze e le relative istanze e volumi, quando crei il parco istanze.

Il parco istanze avvia On-Demand le istanze quando c'è capacità disponibile e le istanze Spot quando il prezzo massimo supera il prezzo Spot e la capacità è disponibile.

Dopo il lancio della flotta, puoi descrivere la richiesta del parco veicoli, le istanze del parco veicoli e gli eventuali eventi del parco veicoli. Se necessario, puoi anche assegnare tag aggiuntivi.

Se è necessario modificare i parametri del parco istanze, come la capacità target totale, è possibile modificare il parco istanze, a condizione che sia configurato per mantenere la capacità. Non puoi modificare la capacità target di una richiesta una tantum dopo che è stata inviata.

La richiesta di parco istanze rimane attiva fino a quando non scade o fino a quando non viene annullata (eliminata). Quando annulli la richiesta del parco istanze, puoi interrompere le istanze o lasciarle in esecuzione. Se scegli di lasciarle in esecuzione, le On-Demand istanze restano attive finché non le chiudi, mentre le istanze Spot vengono interrotte o finché non sei tu a terminarle.

Argomenti

- Stati della richiesta di parco istanze spot
- Autorizzazioni del parco istanze spot
- Creazione di un parco istanze Spot

- Applicare un tag a una richiesta nuova o esistente per un parco istanze spot e alle istanze e ai volumi che avvia
- Descrivi una richiesta del parco istanze spot, le relative istanze e la cronologia degli eventi
- Modificare una richiesta di parco istanze spot
- Annullare (eliminare) una richiesta di parco istanze spot
- Informazioni sulla scalabilità automatica per il parco istanze spot

Stati della richiesta di parco istanze spot

> **Important**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Una richiesta del parco istanze spot può essere uno dei diversi stati, ciascuno dei quali indica una fase diversa del ciclo di vita della richiesta e della relativa gestione delle istanze.

Una richiesta di parco istanze spot può avere uno dei seguenti stati:

`submitted`

La richiesta del parco istanze spot è in fase di valutazione e Amazon EC2 si sta preparando ad avviare il numero previsto di istanze. Se la tua richiesta supera le quote del parco istanze spot, viene annullata immediatamente.

`active`

Il parco istanze spot è stata convalidato e Amazon EC2 sta tentando di mantenere il numero previsto di istanze spot in esecuzione. La richiesta rimane in questo stato finché non viene modificata o annullata.

`modifying`

La richiesta del parco istanze spot è in fase di modifica. La richiesta rimane in questo stato finché la modifica non viene completamente elaborata o la richiesta non viene annullata. È possibile modificare solo un tipo di parco istanze `maintain`. Questo stato non si applica al tipo di parco istanze `request` una tantum.

`cancelled_running`

Il parco istanze spot viene annullato (eliminato) e non avvia istanze spot aggiuntive. Le sue istanze esistenti continuano a essere eseguite finché non vengono interrotte o terminate manualmente. La richiesta rimane in questo stato finché tutte le istanze non vengono interrotte o terminate.

`cancelled_terminating`

Il parco istanze spot viene annnullato (eliminato) e le sue istanze vengono terminate. La richiesta rimane in questo stato finché tutte le istanze non vengono terminate.

`cancelled`

Il parco istanze spot viene annullato (eliminato) e non contiene istanze in esecuzione. La richiesta viene eliminata due giorni dopo e le sue istanze vengono terminate.

Autorizzazioni del parco istanze spot

> **Important**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Se gli utenti IAM creano o gestiscono una serie di istanze spot, occorre concedere loro le autorizzazioni richieste.

Se utilizzi la console Amazon EC2 per creare una serie di istanze spot, viene creato un ruolo collegato ai due servizi denominato `AWSServiceRoleForEC2SpotFleet` e `AWSServiceRoleForEC2Spot` e un ruolo denominato `aws-ec2-spot-fleet-tagging-role` che concede al serie di istanze spot le autorizzazioni per richiedere, avviare, terminare e assegnare tag alle risorse per tuo conto. Se utilizzi AWS CLI o un'API, devi assicurarti che questi ruoli esistano.

Utilizzare le istruzioni seguenti per concedere le autorizzazioni necessarie e creare i ruoli.

Autorizzazioni e ruoli

- Concessione di autorizzazioni a un utente per la serie di istanze spot
- Service-linked ruolo per Spot Fleet

- Service-linked ruolo per le istanze Spot
- Ruolo IAM per l'assegnazione di tag a un parco istanze spot

Concessione di autorizzazioni a un utente per la serie di istanze spot

Se gli utenti creano o gestiscono una serie di istanze spot, assicurati di concedere loro le autorizzazioni richieste.

Per creare una policy per la serie di istanze spot

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, selezionare Policies (Policy), quindi Create policy (Crea policy).
3. Nella pagina Crea policy scegliere JSON e sostituire il testo con il seguente.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:CreateTags",
                "ec2:RequestSpotFleet",
                "ec2:ModifySpotFleetRequest",
                "ec2:CancelSpotFleetRequests",
                "ec2:DescribeSpotFleetRequests",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeSpotFleetRequestHistory"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
            "Resource": "*"
        }
    ]
}
```

La policy di esempio precedente concede a un utente le autorizzazioni richieste dalla maggior parte dei casi d'uso della serie di istanze spot. Per limitare l'utente a operazioni API specifiche, specificare solo tali operazioni API.

EC2 e API IAM obbligatorie

Le API seguenti devono essere incluse nella policy:

- `ec2:RunInstances` - Obbligatorio per avviare istanze in una serie di istanze spot
- `ec2:CreateTags` - Obbligatorio per applicare tag alla richiesta della serie di istanze spot, alle istanze o ai volumi
- `iam:PassRole` - Obbligatorio per specificare il ruolo della serie di istanze spot
- `iam:CreateServiceLinkedRole` - Obbligatorio per creare il ruolo collegato ai servizi
- `iam:ListRoles` - Obbligatorio per enumerare i ruoli IAM esistenti
- `iam:ListInstanceProfiles` - Obbligatorio per enumerare i profili delle istanze esistenti

> **Important**
>
> Se specifichi un ruolo per il profilo dell'istanza IAM nella specifica di avvio o nel modello di avvio, devi concedere all'utente l'autorizzazione per passare il ruolo al servizio. A tale scopo, nella policy IAM includere "`arn:aws:iam::*:role/`*`IamInstanceProfile-role`*" come risorsa per l'operazione `iam:PassRole`. Per maggiori informazioni, consulta Concessione a un utente delle autorizzazioni per passare un ruolo a un AWS servizio nella IAM User Guide.

API della serie di istanze spot

Aggiungere le operazioni API del parco istanze spot seguenti alla policy, se necessario:

- `ec2:RequestSpotFleet`
- `ec2:ModifySpotFleetRequest`
- `ec2:CancelSpotFleetRequests`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequestHistory`

API IAM opzionali

(Facoltativo) Per consentire a un utente di creare ruoli o profili delle istanze utilizzando la console IAM, è anche necessario aggiungere le operazioni seguenti alla policy:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

4. Scegliere Review policy (Esamina policy).
5. Nella pagina Review policy (Rivedi policy), immettere un nome policy e una descrizione, poi selezionare Create policy (Crea policy).
6. Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

   - 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 Create a role for a third-party identity provider (federation) della Guida per l'utente IAM.

   - Utenti IAM:

- Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina Create a role for an IAM user della Guida per l'utente IAM.
- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente IAM.

Service-linked ruolo per Spot Fleet

Amazon EC2 utilizza ruoli collegati ai servizi per le autorizzazioni di cui ha bisogno per eseguire chiamate ad altri servizi AWS per tuo conto. Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a un AWS servizio. Service-linked i ruoli forniscono un modo sicuro per delegare le autorizzazioni ai AWS servizi perché solo il servizio collegato può assumere un ruolo collegato al servizio. Per ulteriori informazioni, consulta Service-linked i ruoli nella IAM User Guide.

Amazon EC2 utilizza il ruolo collegato al servizio denominato AWSServiceRoleForEC2Spot Fleet per avviare e gestire le istanze per tuo conto.

> **Important**
>
> Se specifichi un'AMI crittografata o uno snapshot Amazon EBS crittografato nella tua flotta Spot, devi concedere al ruolo Fleet l'autorizzazione a utilizzare la AWSServiceRoleForEC2Spot CMK in modo che Amazon EC2 possa avviare istanze per tuo conto. Per ulteriori informazioni, consulta Concessione dell'accesso alle CMK per l'uso con le AMI crittografate e gli snapshot EBS.

Autorizzazioni concesse da AWSServiceRoleForEC2SpotFleet

Il ruolo AWSServiceRoleForEC2Spot Fleet concede a Spot Fleet l'autorizzazione a richiedere, avviare, terminare ed etichettare le istanze per tuo conto. Amazon EC2 utilizza questo ruolo collegato ai servizi per completare le operazioni seguenti:

- `ec2:RequestSpotInstances` – Richiesta di Istanze spot
- `ec2:RunInstances` - Avviare istanze
- `ec2:TerminateInstances` - Terminare istanze
- `ec2:DescribeImages` - Descrivere le immagini Amazon Machine (AMI) per le istanze
- `ec2:DescribeInstanceStatus` - Monitorare lo stato delle istanze.

- `ec2:DescribeSubnets` - Descrivere le sottoreti per le istanze
- `ec2:CreateTags` - Aggiungere tag alla richiesta della serie di istanze spot, alle istanze e ai volumi
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer` - Aggiungere le istanze specificate al load balancer specificato
- `elasticloadbalancing:RegisterTargets` - Registrare le destinazioni specificate nel gruppo di destinazioni specificato

Creazione del ruolo collegato ai servizi

In gran parte dei casi, non è necessario creare manualmente un ruolo collegato ai servizi. Amazon EC2 crea il ruolo collegato al servizio AWSServiceRoleForEC2Spot Fleet la prima volta che crei uno Spot Fleet utilizzando la console.

Se avevi una richiesta Spot Fleet attiva prima di ottobre 2017, quando Amazon EC2 ha iniziato a supportare questo ruolo collegato al servizio, Amazon EC2 ha creato il ruolo Fleet nel tuo account. AWSServiceRoleForEC2Spot AWS Per ulteriori informazioni, consulta A new role appeared in my AWS account nella IAM User Guide.

Se utilizzi AWS CLI o un'API per creare una Spot Fleet, devi prima assicurarti che questo ruolo esista.

Per creare il AWSServiceRoleForEC2SpotFleet ruolo per Spot Fleet utilizzando la console

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. Nella pagina Seleziona un'entità attendibile, esegui le operazioni seguenti:
   a. Per Tipo di entità attendibile, scegli Servizio AWS .
   b. In Caso d'uso, per Servizio o caso d'uso, scegli EC2.
   c. In Caso d'uso, scegli EC2 – Parco istanze spot.

> **Note**
>
> Lo use case EC2 - Spot Fleet creerà automaticamente una policy con le autorizzazioni IAM richieste e suggerirà AWSEC2SpotFleetServiceRolePolicy come nome del ruolo.

d. Scegli Next (Successivo).

5. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo).
6. Nella pagina Nomina, rivedi e crea scegli Crea ruolo.

Per creare il AWSServiceRoleForEC2SpotFleet ruolo per Spot Fleet utilizzando AWS CLI

Utilizzare il comando create-service-linked-role come segue.

```
aws iam create-service-linked-role --aws-service-name spotfleet.amazonaws.com
```

Se non hai più bisogno di usare Spot Fleet, ti consigliamo di eliminare il ruolo AWSServiceRoleForEC2Spot Fleet. Dopo che questo ruolo è stato eliminato dall'account, Amazon EC2 creerà di nuovo il ruolo se viene richiesto un parco istanze spot utilizzando la console. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Concessione dell'accesso alle CMK per l'uso con le AMI crittografate e gli snapshot EBS

Se specifichi un'AMI crittografata o un'istantanea Amazon EBS crittografata nella tua richiesta Spot Fleet e utilizzi una chiave gestita dal cliente per la crittografia, devi concedere al ruolo AWSServiceRoleForEC2Spot Fleet l'autorizzazione a utilizzare la CMK in modo che Amazon EC2 possa avviare istanze per tuo conto. Per farlo, occorre aggiungere una concessione alla chiave CMK, come mostrato nella procedura seguente.

Nel processo di assegnazione delle autorizzazioni, le concessioni rappresentano un'alternativa alle policy delle chiavi. Per ulteriori informazioni, consulta Utilizzo delle concessioni e Utilizzo delle policy delle chiavi in AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .

Per concedere al AWSServiceRoleForEC2SpotFleet ruolo le autorizzazioni per l'utilizzo del CMK

- Usa il comando create-grant per aggiungere una concessione al CMK e per specificare il principale (il ruolo collegato al servizio AWSServiceRoleForEC2Spot Fleet) a cui viene

concessa l'autorizzazione per eseguire le operazioni consentite dalla concessione. La CMK è specificata dal parametro `key-id` e dal relativo ARN. L'entità principale è specificata dal `grantee-principal` parametro e dall'ARN del ruolo collegato al servizio Fleet. AWSServiceRoleForEC2Spot

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
spotfleet.amazonaws.com/AWSServiceRoleForEC2SpotFleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Service-linked ruolo per le istanze Spot

Amazon EC2 utilizza il ruolo collegato al servizio denominato AWSServiceRoleForEC2Spot per avviare e gestire le istanze Spot per tuo conto. Per ulteriori informazioni, consulta Service-linked ruolo per le richieste di istanza Spot.

Ruolo IAM per l'assegnazione di tag a un parco istanze spot

Il ruolo IAM `aws-ec2-spot-fleet-tagging-role` concede l'autorizzazione al serie di istanze spot per assegnare tag alla richiesta, alle istanze e ai volumi della serie di istanze spot. Per ulteriori informazioni, consulta Applicare un tag a una richiesta nuova o esistente per un parco istanze spot e alle istanze e ai volumi che avvia.

Important

Se scegli di applicare tag alle istanze nel parco istanze e scegli anche di mantenere la capacità obiettivo (la richiesta della serie di istanze spot è di tipo `maintain`), le differenze nelle autorizzazioni impostate per l'utente e il `IamFleetRole` potrebbero generare un comportamento incoerente nell'assegnazione di tag alle istanze nel parco istanze. Se l'autorizzazione `IamFleetRole` `CreateTags` non include, alcune delle istanze lanciate dal parco istanze potrebbero non essere taggate. Mentre stiamo lavorando per risolvere questa incoerenza, per garantire che tutte le istanze lanciate dal parco istanze siano taggate, si consiglia di utilizzare il ruolo `aws-ec2-spot-fleet-tagging-role` per `IamFleetRole`. In alternativa, per utilizzare un ruolo esistente, collega la

`AmazonEC2SpotFleetTaggingRole` AWS Managed Policy al ruolo esistente. In caso contrario, è necessario aggiungere manualmente l'autorizzazione `CreateTags` alla policy esistente.

Per creare il ruolo IAM per l'assegnazione di tag a un parco istanze spot

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. Nella pagina Select trusted entity (Seleziona entità attendibile) in Trusted entity type (Tipo di entità attendibile), scegli AWS service (Servizio).
5. In Use case (Caso d'uso), da Use cases for other AWS services (Casi d'uso per altri servizi), scegli EC2, quindi scegli EC2 - Spot Fleet Tagging (EC2 - Assegnazione di tag per la serie di istanze spot).
6. Scegli Next (Successivo).
7. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo).
8. Nella pagina Name, review, and create (Nome, revisione e creazione), per Role name (Nome ruolo) inserisci un nome per il ruolo (ad esempio **`aws-ec2-spot-fleet-tagging-role`**).
9. Rivedi le informazioni presenti nella pagina, quindi scegli Create role (Crea ruolo).

Cross-service vice prevenzione confusa

Il problema confused deputy è un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità maggiormente privilegiata a eseguire l'azione. Consigliamo di utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` nelle policy di attendibilità `aws-ec2-spot-fleet-tagging-role` per limitare le autorizzazioni con cui la serie di istanze spot fornisce un altro servizio alla risorsa.

Per aggiungere le chiavi di SourceAccount condizione aws: SourceArn e aws: alla policy di fiducia aws-ec2-spot-fleet-tagging-role

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, seleziona Ruoli.

3. Individuare la policy `aws-ec2-spot-fleet-tagging-role` creata in precedenza e scegliere il collegamento (non la casella di spunta).
4. In Summary (Riepilogo), scegliere la scheda Trust relationships (Relazioni di attendibilità), quindi scegliere Edit trust policy (Modifica policy di attendibilità).
5. Nell'istruzione JSON, aggiungere un elemento `Condition` contenente le proprie chiavi di contesto delle condizioni globali `aws:SourceAccount` e `aws:SourceArn` per prevenire il problema del "deputy confused", come segue:

```
"Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/
sfr-*"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
```

> **Note**
>
> Se si utilizzano entrambe le chiavi di contesto delle condizioni globali e il valore `aws:SourceArn` contiene l'ID account, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` devono utilizzare lo stesso ID account quando viene utilizzato nella stessa dichiarazione di policy.

La policy di attendibilità finale sarà la seguente:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "spotfleet.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
```

```
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-
request/sfr-*"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
    }
  }
}
```

6. Scegli Aggiorna policy.

La tabella seguente fornisce valori potenziali affinché `aws:SourceArn` limiti l'ambito di `aws-ec2-spot-fleet-tagging-role` secondo diversi gradi di specificità.

Operazione API	Servizio chiamato	Scope	**aws:SourceArn**
RequestSpotFleet	AWS STS (`AssumeRole`)	Limita la capacità di `AssumeRole` in `aws-ec2-spot-fleet-tagging-role` per spot-fleet-requests nell'account specificato.	`arn:aws:ec2:*: 123456789012 :spot-fleet-request/sfr-*`
RequestSpotFleet	AWS STS (`AssumeRole`)	Limita la capacità di `AssumeRole` in `aws-ec2-spot-fleet-tagging-role` per spot-fleet-requests nell'account specificato e nella regione specificata. Questo ruolo non sarà utilizzabile in altre regioni.	`arn:aws:ec2: us-east-1 :123456789012 :spot-fleet-request/sfr-*`

Operazione API	Servizio chiamato	Scope	**aws:SourceArn**
RequestSpotFleet	AWS STS (AssumeRole)	Limita la capacità di AssumeRole in aws-ec2-spot-fleet-tagging-role alle sole operazioni che interessano il parco istanze sfr-11111111-1111-1111-1111-111111111111. Questo ruolo potrebbe non essere utilizzabile per altre serie di istanze spot. Inoltre, questo ruolo non può essere utilizzato per avviare nuove serie di istanze spot tramite il comando request-spot-fleet.	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*11111111-1111-1111-1111-111111111111*

Creazione di un parco istanze Spot

> **Important**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Utilizzando il Console di gestione AWS, puoi creare rapidamente una richiesta Spot Fleet scegliendo solo un AMI e la capacità target totale desiderata. Amazon EC2 configurerà un parco istanze più appropriato alle tue esigenze e segue le best practice Spot. In alternativa, puoi modificare le impostazioni predefinite che preferisci.

Se desideri includere le On-Demand istanze nel tuo parco istanze, devi specificare un modello di lancio nella richiesta e specificare la On-Demand capacità desiderata.

Il parco istanze avvia On-Demand le istanze quando la capacità è disponibile e le istanze Spot quando il prezzo massimo supera il prezzo Spot e la capacità è disponibile.

Se il parco istanze include istanze spot ed è di tipo `maintain`, Amazon EC2 tenterà di mantenere la capacità target del parco istanze quando le istanze spot vengono interrotte.

Autorizzazioni richieste

Per ulteriori informazioni, consulta the section called "Autorizzazioni del parco istanze spot".

Processi

- Crea rapidamente una richiesta di parco istanze spot
- Crea una richiesta di parco istanze spot utilizzando parametri definiti
- Crea un parco istanze spot che sostituisca le istanze spot non integre

Crea rapidamente una richiesta di parco istanze spot

Per creare rapidamente una richiesta di parco istanze spot usando la console Amazon EC2, segui la procedura descritta di seguito.

Per creare una richiesta di parco istanze spot utilizzando le impostazioni consigliate

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Se è la prima volta che viene utilizzato lo Spot, verrà visualizzata una pagina di benvenuto; selezionare Get started (Inizia). Altrimenti, scegli Crea richiesta del parco istanze spot.
4. Sotto Launch parameters (Parametri di avvio), scegliere Manually configure launch parameters (Configura manualmente i parametri di avvio).
5. Per AMI, scegliere un'AMI.
6. Sotto Target capacity (Capacità di destinazione), per Total target capacity (Capacità di destinazione totale), specificare il numero di unità da richiedere. Per il tipo di unità, è possibile scegliere Istanze, vCPU oppure Memoria (GiB).
7. Per La tua richiesta immediata per il parco istanze, controlla la configurazione del tuo parco istanze e scegli Launch (Avvia).

Crea una richiesta di parco istanze spot utilizzando parametri definiti

È possibile creare un parco istanze spot utilizzando i parametri che si definiscono.

Console

Per creare una richiesta di parco istanze spot utilizzando parametri definiti

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Se è la prima volta che viene utilizzato lo Spot, verrà visualizzata una pagina di benvenuto; selezionare Get started (Inizia). Altrimenti, scegli Crea richiesta del parco istanze spot.
4. Per i parametri di avvio, puoi configurare manualmente i parametri di avvio oppure utilizzare un modello di avvio, come indicato di seguito:

   a. [Configurazione manuale] Per definire i parametri di avvio nella console Amazon EC2, scegli Configura manualmente i parametri di avvio, poi procedi come indicato di seguito:

      i. Per l'AMI, scegli una delle AMI di base fornite da AWS, oppure scegli Cerca AMI per utilizzare un'AMI della nostra community di utenti Marketplace AWS, della o di una tua.

      > **Note**
      >
      > Se un'AMI specificata nei parametri di avvio viene disabilità o la sua registrazione viene annullata, non è possibile avviare nuove istanze dall'AMI. Per i parchi istanze che sono impostati per mantenere la capacità target, tale capacità non verrà mantenuta.

      ii. (Facoltativo) Per Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente o crearne una nuova.

      [Coppia di chiavi esistente] Scegliere la coppia di chiavi.

      [Nuova coppia di chiavi] Scegli Crea nuova coppia di chiavi per accedere alla pagina Coppie di chiavi. Una volta terminato, tornare alla pagina Spot Requests (Richieste Spot) e aggiornare l'elenco.

      iii. (Facoltativo) Espandere Additional launch parameters (Parametri di avvio aggiuntivi) ed effettuare le seguenti operazioni.

A. (Facoltativo) Per abilitare l'ottimizzazione di Amazon EBS EBS-optimized, seleziona le istanze Launch EBS-optimized.

B. (Facoltativo) Per aggiungere archiviazione a livello di blocchi temporaneo per le istanze, per Instance store, scegliere Attach at launch (Collega all'avvio).

C. (Facoltativo) Per aggiungere archiviazione, scegli Add new volume (Aggiungi nuovo volume) e specifica volumi di archivio istanza aggiuntivi o volumi Amazon EBS, a seconda del tipo di istanza.

D. (Facoltativo) Per impostazione predefinita, per le proprie istanze è attivo il monitoraggio base. Per abilitare il monitoraggio dettagliato, per Monitoraggio, seleziona Abilita monitoraggio CloudWatch dettagliato.

E. (Facoltativo) Per eseguire un'istanza spot dedicata, per Tenancy selezionare Dedicated - run a dedicated instance (Dedicata: esegui un'istanza dedicata).

F. (Facoltativo) Per Security groups (Gruppi di sicurezza), scegliere uno o più gruppi di sicurezza o crearne uno nuovo.

   [Gruppo di sicurezza esistente] Scegliere uno o più gruppi di sicurezza.

   [Nuovo gruppo di sicurezza] Scegliere Create new security group (Crea nuovo gruppo di sicurezza) per accedere alla pagina Security Groups (Gruppi di sicurezza). Una volta terminato, tornare alla pagina Spot Requests (Richieste Spot) e aggiornare l'elenco.

G. (Facoltativo) Per rendere le tue istanze raggiungibili da Internet, per l'IP pubblico Auto-assign IPv4, scegli Abilita.

H. (Facoltativo) Per avviare le Istanze spot con un ruolo IAM, selezionare il ruolo per IAM instance profile (Profilo dell'istanza IAM).

I. (Facoltativo) Per eseguire uno script di avvio, copiarlo su User data (Dati utente).

J. (Facoltativo) Per aggiungere un tag, scegliere Create tag (Crea tag) e inserire la chiave e il valore per il tag, quindi scegliere Create (Crea). Ripetere per ogni tag.

   Per ogni tag, per assegnare alle richieste di istanze e serie di istanze spot lo stesso tag, assicurarsi che siano selezionati sia Instance (Istanza) che Fleet (parco istanze). Per assegnare tag solo alle istanze avviate dal parco istanze,

deseleziona Fleet (parco istanze). Per assegnare tag solo alla richiesta della serie di istanze spot, deselezionare Instances (Istanze).

b. [Modello di avvio] Per utilizzare una configurazione creata in un modello di avvio, scegli Usa un modello di avvio e per Modello di avvio, scegli un modello di avvio.

> **Note**
>
> Se desideri aumentare la On-Demand capacità del tuo parco Spot, devi specificare un modello di lancio.

5. Per Additional request details (Dettagli richiesta aggiuntivi), procedere come segue:

   a. Esaminare i dettagli aggiuntivi della richiesta. Per apportare modifiche, deselezionare Apply defaults (Applica impostazioni predefinite).

   b. (Facoltativo) Per IAM fleet role (Ruolo parco istanze IAM), è possibile utilizzare il ruolo predefinito o scegliere un ruolo diverso. Per utilizzare il ruolo predefinito dopo aver modificato il ruolo, scegliere Use default role (Usa ruolo predefinito).

   c. (Facoltativo) Per creare una richiesta valida soltanto per un periodo di tempo specifico, modificare Request valid from (Richiesta valida da) e Request valid until (Richiesta valida fino a).

   d. (Facoltativo) Per impostazione predefinita, Amazon EC2 termina le istanze quando la richiesta del parco istanze spot scade. Per tenerle in esecuzione dopo la scadenza della richiesta, deselezionare Terminate the instances when the request expires (Termina istanze alla scadenza della richiesta).

   e. (Facoltativo) Per registrare le proprie Istanze Spot con un load balancer, selezionare Receive traffic from one or more load balancers (Ricevi traffico da uno o più load balancer) e scegliere uno o più Classic Load Balancer o gruppi di destinazione.

6. In Target capacity (Capacità target), effettuare le operazioni seguenti:

   a. Per Total target capacity (Capacità di destinazione totale), specificare il numero di unità da richiedere. Per il tipo di unità, è possibile scegliere Instances (Istanze), vCPU oppure Memory (MiB) (Memoria (MiB)). Per specificare una capacità target pari a 0 per aggiungere la capacità in un secondo momento, devi prima selezionare Mantieni capacità target.

b. (Facoltativo) Per Includi capacità On-Demand base, specifica il numero di On-Demand unità da richiedere. Il numero deve essere inferiore alla Capacità obiettivo totale. Amazon EC2 calcola la differenza e la assegna alle unità Spot da richiedere.

> **Important**
>
> Per specificare la On-Demand capacità opzionale, devi prima scegliere un modello di avvio.

c. (Facoltativo) Per impostazione predefinita, Amazon EC2 termina le istanze spot quando esse vengono interrotte. Per mantenere la capacità target, selezionare Maintain target capacity (Mantieni capacità target). È quindi possibile specificare che Amazon EC2 termini, arresti o iberni le istanze spot quando vengono interrotte. Per procedere in questo senso, selezionare l'opzione corrispondente da Interruption behavior (Comportamento di interruzione).

> **Note**
>
> Se un'AMI specificata nei parametri di avvio viene disabilità o la sua registrazione viene annullata, non è possibile avviare nuove istanze dall'AMI. In questo caso, per i parchi istanze che sono impostati per mantenere la capacità target, tale capacità non verrà mantenuta.

d. (Facoltativo) Per consentire alla serie di istanze spot di avviare un'istanza spot sostitutiva quando viene emessa una notifica di ribilanciamento dell'istanza per un'istanza spot esistente nel parco istanze, selezionare Capacity rebalance (Ribilanciamento capacità), quindi scegliere una strategia di sostituzione istanze. Se scegli Avviare prima di terminare, specificare il ritardo (in secondi) prima che Amazon EC2 termini le vecchie istanze. Per ulteriori informazioni, consulta Utilizza il ribilanciamento della capacità nel parco istanze EC2 e nel parco istanze spot per sostituire le istanze spot a rischio.

e. (Facoltativo) Per controllare l'importo che paghi all'ora per tutte le istanze spot del parco istanze, seleziona Set maximum cost for Spot Instances (Imposta il costo massimo per le istanze spot) e quindi inserisci l'importo totale massimo che sei disposto a pagare all'ora. Quando viene raggiunto l'importo totale massimo, il parco istanze spot interrompe l'avvio di istanze spot, anche se non è stata raggiunta la capacità obiettivo. Per ulteriori informazioni, consulta Imposta un limite di spesa per il Parco istanze EC2 o il parco istanze spot.

7. In Network (Rete), procedere come segue:

   a. (Facoltativo) Per Rete, scegliere un VPC esistente o crearne uno nuovo.

      [VPC esistente] Scegliere il VPC.

      [VPC nuovo] Scegliere Create new VPC (Crea nuovo VPC) per accedere alla console Amazon VPC. Una volta terminato, torna in questa schermata e aggiorna l'elenco.

   b. (Facoltativo) Per Zona di disponibilità, lascia che Amazon EC2 scelga le zone di disponibilità per le istanze spot oppure specifica una o più zone di disponibilità.

      Se si ha più di una sottorete in una zona di disponibilità, scegliere la sottorete appropriata da Subnet (Sottorete). Per aggiungere sottoreti, scegliere Create new subnet (Crea nuova sottorete) per accedere alla console Amazon VPC. Una volta terminato, torna in questa schermata e aggiorna l'elenco.

8. Per Instance type requirements (Requisiti per il tipo di istanza), puoi specificare gli attributi dell'istanza e consentire ad Amazon EC2 di identificare i tipi di istanza ottimali con questi attributi, oppure puoi specificare un elenco di istanze. Per ulteriori informazioni, consulta Specifica gli attributi per la selezione del tipo di istanza per il parco del tipo per il parco istanze EC2 o il parco istanze Spot.

   a. Se si sceglie Specify instance attributes that match your compute requirements (Specifica gli attributi di istanza che corrispondono ai requisiti di calcolo), specificare gli attributi di istanza nel modo seguente:

      i. Per vCPUs (vCPU) inserire il numero minimo e massimo desiderato di vCPU. Per non specificare alcun limite, selezionare Nessun minimo, Nessun massimo o entrambe le opzioni.

      ii. Per Memory (GiB) (Memoria [GiB]) inserire la quantità minima e massima di memoria desiderata. Per non specificare alcun limite, selezionare Nessun minimo, Nessun massimo o entrambe le opzioni.

      iii. (Facoltativo) Per Attributi istanza aggiuntivi, facoltativamente, è possibile specificare uno o più attributi per esprimere i requisiti di calcolo in modo più dettagliato. Ogni attributo aggiuntivo aggiunge ulteriori vincoli alla tua richiesta. È possibile omettere gli attributi aggiuntivi, nel qual caso saranno utilizzati i valori di default. Per una descrizione di ciascun attributo e dei relativi valori predefiniti, consulta get-spot-placement-scores.

iv. (Facoltativo) Per visualizzare i tipi di istanza con gli attributi specificati, espandere Preview matching instance types (Anteprima tipi di istanza corrispondenti). Per escludere i tipi di istanza utilizzati nella richiesta, selezionare le istanze e quindi scegliere Exclude selected instance types (Escludi tipi di istanze selezionati).

b. Se si sceglie Manually select instance types (Seleziona manualmente i tipi di istanza), la serie di istanze spot fornisce un elenco di tipi di istanza di default. Per selezionare più tipi di istanza, scegliere Add instance types (Aggiungi tipi di istanza), selezionare i tipi di istanza da utilizzare nella tua richiesta e scegliere Select (Seleziona). Per eliminare i tipi di istanza, selezionarli e scegliere Delete (Elimina).

9. Per Strategia di allocazione, scegli una strategia di allocazione Spot e una strategia di On-Demand allocazione che soddisfi le tue esigenze. Per ulteriori informazioni, consulta Utilizza le strategie di allocazione per determinare in che modo EC2 Fleet o Spot Fleet soddisfano Spot e la capacità On-Demand.
10. Per Your fleet request at a glance (La tua richiesta immediata per il parco istanze), rivedere la configurazione del parco istanze e, se necessario, apportare eventuali modifiche.
11. (Facoltativo) Per scaricare una copia della configurazione di avvio da utilizzare con AWS CLI, scegli JSON config.
12. Quando è tutto pronto per l'avvio del parco istanze spot, scegli Avvia.

    Il tipo di richiesta della serie di istanze spot è `fleet`. Quando la richiesta viene soddisfatta, vengono aggiunte delle richieste di tipo `instance`, che hanno come condizione `active` e come stato `fulfilled`.

AWS CLI

Per creare una richiesta di parco istanze spot

Utilizzare il comando request-spot-fleet.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Per i file di configurazione di esempio, consultare Configurazioni CLI di esempi per parco istanze spot.

PowerShell

Per creare una richiesta di parco istanze spot

Utilizza il cmdlet Request-EC2SpotFleet. L'esempio seguente avvia le istanze spot in un parco istanze ottimizzato per la capacità.

```
Request-EC2SpotFleet `
    -SpotFleetRequestConfig_TargetCapacity 50 `
    -SpotFleetRequestConfig_AllocationStrategy "CapacityOptimized" `
    -SpotFleetRequestConfig_IamFleetRole "arn:aws:iam::123456789012:role/my-spot-
fleet-role" `
    -SpotFleetRequestConfig_LaunchTemplateConfig @($launchConfig)
```

Definisci la configurazione di avvio nel modo seguente, impostando il modello di avvio e sovrascrivendo le proprietà necessarie. Per gli esempi di configurazione, consulta Configurazioni CLI di esempi per parco istanze spot.

```
$lcSpec = Amazon.EC2.Model.FleetLaunchTemplateSpecification
# To do - Set FleetLaunchTemplateSpecification properties
$lcOverrides = New-Object Amazon.EC2.Model.LaunchTemplateOverrides
# To do - Set LaunchTemplateOverrides properties
$launchConfig = New-Object Amazon.EC2.Model.LaunchTemplateConfig
$launchConfig.LaunchTemplateSpecification $lcSpec
$launchConfig.Overrides @($lcOverrides)
```

Crea un parco istanze spot che sostituisca le istanze spot non integre

Il parco istanze spot controlla lo stato di integrità delle istanze nel parco istanze ogni due minuti. Lo stato di un'istanza è `healthy` o `unhealthy`.

Il parco istanze spot determina lo stato di integrità un'istanza utilizzando i controlli dello stato forniti da Amazon EC2. Un'istanza viene determinata come `unhealthy` quando lo stato del controllo dello stato dell'istanza o del controllo dello stato del sistema è `impaired` per tre controlli di integrità consecutivi. Per ulteriori informazioni, consulta Verifiche dello stato delle istanze Amazon EC2.

È possibile configurare il parco istanze per sostituire le Istanze spot non integre. Dopo avere abilitato la sostituzione del controllo di integrità, un'istanza spot viene sostituita quando viene segnalata come `unhealthy`. Durante la sostituzione di un'istanza spot non integra, il parco istanze può scendere al di sotto della sua capacità obiettivo.

Requisiti

- La sostituzione del controllo dello stato è supportata solo per i Parchi istanze spot che mantengono una capacità target (parchi istanza del tipo `maintain`) e non per i Parchi istanze spot una tantum (ossia del tipo `request`).
- La sostituzione del controllo dello stato è supportata solo per Istanze spot. Questa funzionalità non è supportata per On-Demand le istanze.
- È possibile configurare il parco istanze spot per sostituire le istanze non integre solo al momento della sua creazione.
- Gli utenti possono utilizzare la sostituzione del controllo dell'integrità solo se hanno l'autorizzazione a chiamare l'operazione `ec2:DescribeInstanceStatus`.

Console

Per configurare un parco istanze spot per sostituire le istanze spot non integre

1. Seguire i passaggi per creare un parco istanze spot in Crea una richiesta di parco istanze spot utilizzando parametri definiti.
2. Per configurare il parco istanze per sostituire istanze spot non integre, espandi Parametri di avvio aggiuntivi e in Controllo dell'integrità, seleziona Sostituisci istanze non integre. Per abilitare questa opzione, è necessario innanzitutto scegliere Mantieni capacità target.

AWS CLI

Per configurare un parco istanze spot per sostituire le istanze spot non integre

Utilizza il comando request-spot-fleet con la proprietà `ReplaceUnhealthyInstances` di `SpotFleetRequestConfig`.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
        "TargetCapacity": 10,
        "ReplaceUnhealthyInstances": true
    }
}
```

PowerShell

Per configurare una richiesta del parco istanze spot per sostituire le istanze spot non integre

Utilizzare il Request-EC2SpotFleet cmdlet con il parametro. -SpotFleetRequestConfig_ReplaceUnhealthyInstance

```
-SpotFleetRequestConfig_ReplaceUnhealthyInstance $true
```

Applicare un tag a una richiesta nuova o esistente per un parco istanze spot e alle istanze e ai volumi che avvia

> **Important**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Per categorizzare e gestire le richieste del parco istanze spot e le istanze e i volumi che avvia, puoi contrassegnarle con tag contenenti metadati personalizzati. È possibile assegnare un tag a una richiesta di parco istanze spot alla sua creazione o successivamente. Allo stesso modo, puoi assegnare un tag alle istanze e ai volumi quando vengono lanciati dal parco istanze o in un secondo momento.

Quando si applica un tag a una richiesta del parco istanze, alle istanze e ai volumi che vengono avviati dal parco istanze non vengono automaticamente applicati tag. È necessario applicare esplicitamente tag alle istanze e ai volumi avviati dal parco istanze. È possibile scegliere di applicare tag solo alla richiesta del parco istanze o solo alle istanze avviate dal parco istanze oppure solo ai volumi collegati alle istanze avviate dal parco istanze o a tutti.

> **Note**
>
> È possibile contrassegnare solo i volumi collegati alle On-Demand istanze. Non è possibile applicare tag ai volumi collegati a Istanze spot.

È possibile assegnare tag utilizzando la console Amazon EC2 o lo strumento da riga di comando.

Per ulteriori informazioni sul funzionamento dei tag, consultare Tagging delle risorse Amazon EC2..

Indice

- Prerequisito
- Applicare un tag a un nuovo parco istanze spot e alle istanze e ai volumi che avvia
- Assegnazione di tag a un parco istanze spot esistente
- Visualizzare i tag della richiesta di parco istanze spot

Prerequisito

Concedi all'utente l'autorizzazione per taggare le risorse. Per ulteriori informazioni, consulta Esempio: aggiunta di tag alle risorse.

Per concedere a un utente l'autorizzazione per taggare le risorse

Creare una policy IAM che include quanto segue:

- L'operazione `ec2:CreateTags`. Ciò concede all'utente l'autorizzazione per creare tag.
- L'operazione `ec2:RequestSpotFleet`. Ciò concede all'utente l'autorizzazione per creare una richiesta di serie di istanze spot.
- Per `Resource`, è necessario specificare `"*"`. Ciò consente agli utenti di taggare tutti i tipi di risorse.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotFleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:RequestSpotFleet"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Important

Resource-level le autorizzazioni non sono attualmente supportate per la `spot-fleet-request` risorsa. Se si specifica `spot-fleet-request` come risorsa, si otterrà un'eccezione non autorizzata quando si tenta di taggare il parco istanze. Nell'esempio seguente viene mostrato come non impostare la policy.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:RequestSpotFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/*"
}
```

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- 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 Create a role for a third-party identity provider (federation) della Guida per l'utente IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina Create a role for an IAM user della Guida per l'utente IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente IAM.

Applicare un tag a un nuovo parco istanze spot e alle istanze e ai volumi che avvia

Per applicare tag a una nuova richiesta del parco istanze spot e alle istanze e ai volumi che avvia utilizzando la console

1. Seguire la procedura Crea una richiesta di parco istanze spot utilizzando parametri definiti.
2. Il modo in cui aggiungi un tag dipende dal fatto che tu abbia configurato manualmente il parco istanze o utilizzato un modello di avvio.

   - Se hai configurato manualmente il parco istanze, completa le seguenti operazioni:

     Per aggiungere un tag, espandi Parametri di avvio aggiuntivi, scegli Crea tag e inserisci la chiave e il valore per il tag. Ripetere per ogni tag.

     Per ogni tag, è possibile assegnare lo stesso tag alla richiesta del parco istanze spot e alle istanze. Per taggare entrambi, assicurarsi che Istanze e Parco istanze siano entrambi selezionati. Per assegnare tag solo alla richiesta della serie di istanze spot, deselezionare Instances (Istanze). Per assegnare tag solo alle istanze avviate dal parco istanze, deseleziona Fleet (parco istanze).

     > **Note**
     >
     > Quando configuri manualmente un parco istanze, non puoi applicare tag ai volumi. I tag di volume sono supportati solo per i volumi collegati alle On-Demand istanze. Quando configuri manualmente un parco istanze, non puoi specificare le On-Demand istanze.

   - Se hai utilizzato un modello di avvio, completa le seguenti operazioni:

     Per aggiungere un tag alla richiesta del parco istanze, in Tag, scegli Crea tag e inserisci la chiave e il valore per il tag. Ripetere per ogni tag.

     Per applicare tag alle risorse nel tuo parco istanze, devi specificare i tag nel modello di avvio.

Per contrassegnare una nuova richiesta Spot Fleet e le istanze e i volumi che viene avviata, utilizza AWS CLI

Per applicare tag a una richiesta di parco istanze spot al momento della creazione e per applicare tag alle istanze e ai volumi quando vengono avviati dal parco istanze, impostare la configurazione della richiesta di parco istanze spot nel modo seguente:

Tag della richiesta di parco istanze spot:

- Specificare i tag per la richiesta di serie di istanze spot in `SpotFleetRequestConfig`.
- Per `ResourceType`, specificare `spot-fleet-request`. Indicando un altro valore, la richiesta per il parco istanze fallisce.
- Per `Tags`, specificare la coppia chiave-valore. È possibile specificare più coppie chiave-valore.

Tag di istanza:

- Specificare i tag per le istanze in `LaunchSpecifications`.
- Per `ResourceType`, specificare `instance`. Indicando un altro valore, la richiesta per il parco istanze fallisce.
- Per `Tags`, specificare la coppia chiave-valore. È possibile specificare più coppie chiave-valore.

  In alternativa, è possibile specificare i tag per l'istanza nel modello di avvio al quale si fa riferimento nella richiesta di parco istanze spot.

Tag associati ai volumi:

- Specificare i tag per i volumi nel modello di avvio al quale si fa riferimento nella richiesta di parco istanze spot. Il tagging del volume in `LaunchSpecifications` non è supportato.

Nell'esempio seguente, la richiesta Spot Fleet è contrassegnata con due tag: Key=Environment e Value=Production e Key= e Value=123. Cost-Center Le istanze lanciate dalla flotta sono contrassegnate con un tag (che è lo stesso di uno dei tag per la richiesta Spot Fleet): Key= e Value=123. Cost-Center

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
```

```
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

Per etichettare le istanze lanciate da una Spot Fleet utilizzando AWS CLI

Per applicare tag alle istanze quando vengono avviate dal parco istanze, è possibile specificare i tag nel modello di avvio a cui si fa riferimento nella richiesta del parco istanze spot oppure specificare i tag nella configurazione della richiesta del parco istanze spot come segue:

- Specificare i tag per le istanze in `LaunchSpecifications`.
- Per `ResourceType`, specificare `instance`. Indicando un altro valore, la richiesta per il parco istanze fallisce.
- Per `Tags`, specificare la coppia chiave-valore. È possibile specificare più coppie chiave-valore.

Nell'esempio seguente, le istanze lanciate dalla flotta sono contrassegnate con un tag: Key= Cost-Center e Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
```

```
        "InstancePoolsToUseCount": 1
    }
}
```

Per etichettare i volumi collegati alle On-Demand istanze avviate da un parco istanze Spot utilizzando il AWS CLI

Per applicare tag ai volumi quando vengono avviati dal parco istanze, specificare i tag nel modello di avvio a cui si fa riferimento nella richiesta del parco istanze spot.

> **Note**
>
> I tag di volume sono supportati solo per i volumi collegati alle On-Demand istanze. Non è possibile applicare tag ai volumi collegati a Istanze spot.
> Il tagging del volume in `LaunchSpecifications` non è supportato.

Assegnazione di tag a un parco istanze spot esistente

Per assegnare tag a una richiesta di parco istanze spot esistente utilizzando la console

Dopo aver creato una richiesta di parco istanze spot, è possibile aggiungere tag alla richiesta del parco istanze utilizzando la console.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di parco istanze spot.
4. Scegliere la scheda Tags e scegliere Create Tag (Crea tag).

Per etichettare una richiesta Spot Fleet esistente utilizzando AWS CLI

Utilizzare il seguente comando create-tags per aggiungere un tag alle risorse esistenti. Nell'esempio seguente, la richiesta di parco istanze spot esistente è taggata con Key=purpose e Value=test.

```
aws ec2 create-tags \
    --resources sfr-11112222-3333-4444-5555-66666EXAMPLE \
    --tags Key=purpose,Value=test
```

Visualizzare i tag della richiesta di parco istanze spot

Per visualizzare i tag della richiesta di parco istanze spot utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Selezionare la richiesta di parco istanze spot e scegliere la scheda Tags.

Per descrivere i tag della richiesta del parco istanze spot

Utilizzare il comando describe-tags per visualizzare i tag per la risorsa specificata. Nell'esempio seguente vengono descritti i tag per la richiesta di parco istanze spot specificata.

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Production"
        },
        {
            "Key": "Another key",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Another value"
        }
    ]
}
```

Puoi visualizzare i tag di una richiesta di parco istanze spot anche descrivendo la richiesta di parco istanze spot.

Utilizzare il comando describe-spot-fleet-requests per visualizzare la configurazione della richiesta di parco istanze spot specificata, che include tutti i tag specificati per la richiesta del parco istanze.

```
aws ec2 describe-spot-fleet-requests \
```

```
    --spot-fleet-request-ids sfr-11112222-3333-4444-5555-66666EXAMPLE
```


```
{
    "SpotFleetRequestConfigs": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2020-02-13T02:49:19.709Z",
            "SpotFleetRequestConfig": {
                "AllocationStrategy": "capacityOptimized",
                "OnDemandAllocationStrategy": "lowestPrice",
                "ExcessCapacityTerminationPolicy": "Default",
                "FulfilledCapacity": 2.0,
                "OnDemandFulfilledCapacity": 0.0,
                "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-
tagging-role",
                "LaunchSpecifications": [
                    {
                        "ImageId": "ami-0123456789EXAMPLE",
                        "InstanceType": "c4.large"
                    }
                ],
                "TargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "Type": "maintain",
                "ReplaceUnhealthyInstances": false,
                "InstanceInterruptionBehavior": "terminate"
            },
            "SpotFleetRequestId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "SpotFleetRequestState": "active",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                },
                {
                    "Key": "Another key",
                    "Value": "Another value"
                }
            ]
        }
    ]
}
```

Descrivi una richiesta del parco istanze spot, le relative istanze e la cronologia degli eventi

> **Important**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Puoi descrivere la configurazione del tuo parco istanze spot, le istanze nel tuo parco istanze spot e la cronologia degli eventi del tuo parco istanze spot.

Console

Per descrivere il parco istanze spot

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di parco istanze spot. L'ID inizia con sfr-. Per vedere i dettagli di configurazione, scegliere Description (Descrizione).
4. Per elencare le istanze spot per il parco istanze spot, scegliere Instances (Istanze).
5. Per visualizzare la cronologia per il parco istanze spot, scegliere History (Cronologia).

AWS CLI

Per descrivere le richieste del parco istanze spot

Utilizza il comando describe-spot-fleet-requests.

```
aws ec2 describe-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Per descrivere le istanze in esecuzione per il parco istanze spot specificato

Utilizza il comando describe-spot-fleet-instances.

```
aws ec2 describe-spot-fleet-instances \
```

```
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Per descrivere la cronologia degli eventi per il parco istanze spot specificato

Utilizza il comando describe-spot-fleet-request-history.

```
aws ec2 describe-spot-fleet-request-history \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2024-05-18T00:00:00Z
```

PowerShell

Per descrivere le richieste del parco istanze spot

Utilizza il cmdlet Get-EC2SpotFleetRequest.

```
Get-EC2SpotFleetRequest
```

Per descrivere le istanze in esecuzione per il parco istanze spot specificato

Utilizza il cmdlet Get-EC2SpotFleetInstance.

```
Get-EC2SpotFleetInstance `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
```

Per descrivere la cronologia degli eventi per il parco istanze spot specificato

Utilizza il cmdlet Get-EC2SpotFleetRequestHistory.

```
Get-EC2SpotFleetRequestHistory `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -UtcStartTime 2024-05-18T00:00:00Z
```

Modificare una richiesta di parco istanze spot

> **Important**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

È possibile modificare una richiesta di parco istanze spot attiva per completare le attività seguenti:

- Aumentare la capacità e la porzione target totali On-Demand
- Riduci la capacità e la On-Demand porzione target totali

Quando aumenti la capacità target totale, il parco istanze spot avvia le istanze spot aggiuntive in base alla strategia di allocazione per la relativa richiesta del parco istanze spot. Quando aumenti la On-Demand porzione, Spot Fleet avvia On-Demand istanze aggiuntive.

Quando si diminuisce la capacità target totale, il parco istanze spot annulla qualsiasi richiesta aperta che supera la nuova capacità target. È possibile richiedere che il parco istanze spot termini le istanze spot finché la dimensione del parco istanze non raggiunge la nuova capacità obiettivo. Se la strategia di allocazione è `diversified`, la serie di istanze spot termina le istanze tra i pool. In alternativa, è possibile richiedere che il parco istanze spot mantenga il parco istanze alla sua dimensione attuale, ma che non sostituisca le istanze spot che vengono interrotte o tutte le istanze che vengono terminate manualmente.

Considerazioni

- Non è possibile modificare una richiesta di parco istanze spot una tantum. È possibile modificare una richiesta di parco istanze spot solo se è stata selezionata Maintain target capacity (Mantieni capacità obiettivo) quando la richiesta è stata creata.
- Quando un parco istanze spot termina un'istanza spot a seguito della diminuzione della capacità obiettivo, l'istanza riceve un avviso di interruzione dell'istanza spot.

Console

Per modificare una richiesta di parco istanze spot

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di parco istanze spot.
4. Scegliere Actions (Operazioni), quindi Modify target capacity (Modifica capacità target).
5. In Modify target capacity (Modifica capacità target), effettuare le operazioni seguenti:
   a. Inserisci la nuova capacità e On-Demand porzione target.

b. (Facoltativo) Se si diminuisce la capacità target ma si desidera mantenere il parco istanze alla dimensione attuale, deselezionare Terminate instances (Termina istanze).

c. Seleziona Submit (Invia).

AWS CLI

Per modificare una richiesta di parco istanze spot

Utilizzare il comando modify-spot-fleet-request per aggiornare la capacità obiettivo della richiesta del parco istanze spot specificata.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 20
```

È possibile modificare il comando precedente come segue per diminuire la capacità obiettivo del parco istanze spot specificata senza di conseguenza terminare le istanze spot.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 10 \
    --excess-capacity-termination-policy NoTermination
```

PowerShell

Per modificare una richiesta di parco istanze spot

Utilizza il Edit-EC2SpotFleetRequest cmdlet per aggiornare la capacità di destinazione della richiesta Spot Fleet specificata.

```
Edit-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacity 20
```

È possibile modificare il comando precedente come segue per diminuire la capacità obiettivo del parco istanze spot specificata senza di conseguenza terminare le istanze spot.

```
Edit-EC2SpotFleetRequest `
```

```
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacity 20 `
    -ExcessCapacityTerminationPolicy "NoTermination"
```

Annullare (eliminare) una richiesta di parco istanze spot

> **Important**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Se non hai più bisogno di un parco istanze spot, puoi annullare la richiesta del parco istanze spot, che elimina la richiesta. Dopo aver annullato la richiesta di un parco istanze, anche tutte le richieste di istanze spot associate al parco istanze vengono eliminate, in modo che nessuna istanza spot nuova venga avviata per tale parco.

Quando si annulla una richiesta di una serie di istanze spot, è necessario specificare se si desidera terminare tutte le relative istanze. Questi includono sia le On-Demand istanze che le istanze Spot.

> **Warning**
>
> La terminazione di un'istanza è permanente e irreversibile.
> Dopo aver terminato un'istanza, non puoi più connetterti a essa e non puoi ripristinarla. Inoltre, tutti i volumi Amazon EBS collegati e configurati per essere eliminati in caso di terminazione vengono eliminati in modo definitivo e non possono essere recuperati. Tutti i dati archiviati nei volumi di archivio dell'istanza vengono persi in modo definitivo. Per ulteriori informazioni, consulta Come funziona la terminazione delle istanze.
> Prima di terminare un'istanza, assicurati di aver eseguito il backup di tutti i dati che devi mantenere dopo la terminazione sull'archivio persistente.

Se specifichi che le istanze devono essere terminate quando annulli la richiesta del parco istanze, quest'ultima acquisisce lo stato `cancelled_terminating`. Altrimenti, esso acquisisce lo stato `cancelled_running` e l'esecuzione delle istanze continua finché esse non vengono interrotte o terminate manualmente.

Restrizioni

- È possibile annullare fino a 100 parchi istanze in un'unica richiesta. Se si supera il numero specificato, non viene annullato alcun parco istanze.

Console

Per annullare (eliminare) una richiesta di parco istanze spot

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di parco istanze spot.
4. Scegli Operazioni e Annulla richiesta.
5. Nella finestra di dialogo Annulla richiesta di istanze spot, esegui una delle operazioni indicate di seguito:

   a. Per terminare le istanze associate contemporaneamente all'annullamento della richiesta della serie di istanze spot, lascia selezionata la casella di spunta Termina istanze. Per annullare la richiesta di parco istanze spot senza terminare le istanze associate, deseleziona la casella di spunta Termina istanze.

   b. Scegli Conferma.

AWS CLI

Per annullare (eliminare) una richiesta di parco istanze spot e terminare le relative istanze

Utilizza il comando cancel-spot-fleet-requests con l'opzione `--terminate-instances`.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Di seguito è riportato un output di esempio.

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
```

```
            "CurrentSpotFleetRequestState": "cancelled_terminating",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

Per annullare (eliminare) una richiesta di parco istanze spot senza terminare le relative istanze

Modifica l'esempio precedente utilizzando invece l'opzione `--no-terminate-instances`.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Di seguito è riportato un output di esempio.

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_running",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

PowerShell

Per annullare (eliminare) una richiesta di parco istanze spot e terminare le relative istanze

Utilizza il Stop-EC2SpotFleetRequest cmdlet con il parametro. `-TerminateInstance`

```
Stop-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $true
```

Per annullare (eliminare) una richiesta di parco istanze spot senza terminare le relative istanze

Modifica l'esempio precedente cambiando il valore del parametro `-TerminateInstance`.

```
Stop-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $false
```

Informazioni sulla scalabilità automatica per il parco istanze spot

> **Important**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

La scalabilità automatica consente al parco istanze spot di aumentare o diminuire la capacità target on demand. Con la scalabilità automatica, un parco istanze spot può avviare le istanze (aumentare orizzontalmente) o terminare le istanze (ridurre orizzontalmente) entro un intervallo specificato, in risposta a una o più policy di scalabilità.

La scalabilità automatica per Spot Fleet è resa possibile da una combinazione delle API Amazon EC2 CloudWatch, Amazon e Application Auto Scaling. Le richieste Spot Fleet vengono create con Amazon EC2, gli allarmi con e le policy di scalabilità vengono create con CloudWatch Application Auto Scaling.

Tipi di dimensionamento automatico

Il parco istanze spot supporta i seguenti tipi di scalabilità automatica:

- Dimensionamento di monitoraggio degli obiettivi – Aumenta o riduce la capacità attuale del parco istanze definendo come target un valore per un parametro specifico. Questa operazione può essere paragonata al modo in cui il termostato regola la temperatura di una casa: si seleziona la temperatura desiderata e il termostato fa il resto.
- Step scaling (Dimensionamento per fasi): aumenta o diminuisce la capacità attuale del parco istanze in base a una serie di regolazioni del dimensionamento, chiamate regolazioni per fasi, che variano in base alla dimensione dell'utilizzo fuori limite segnalato dall'allarme.
- Scheduled scaling (Dimensionamento pianificato): aumenta o riduce la capacità corrente del parco istanze in base alla data e all'ora.

Considerazioni

Quando usi la scalabilità automatica per il parco istanze spot, tieni in considerazione quanto segue:

- Ponderazione delle istanze – Se si utilizza la ponderazione delle istanze, tenere presente che il parco istanze spot può superare la capacità target in base alle necessità. La capacità soddisfatta può essere un numero a virgola mobile, ma la capacità obiettivo deve essere un numero intero, pertanto il parco istanze spot esegue l'arrotondamento fino al numero intero successivo. È necessario tenere conto di questi comportamenti quando si esamina l'esito di una policy di dimensionamento quando viene attivato un allarme. Per esempio, supponiamo che la capacità di destinazione sia 30, la capacità soddisfatta 30,1 e che la policy di dimensionamento sottragga 1. Quando si attiva l'allarme, il processo di scalabilità automatica sottrae 1 da 30,1 ottenendo 29,1, che viene arrotondato a 30, quindi non viene intrapresa alcuna operazione di dimensionamento. Come altro esempio, supponiamo di aver selezionato i pesi di istanza 2, 4 e 8 e una capacità obiettivo di 10 ma non erano disponibili istanze di peso 2, così il parco istanze spot ha fornito in provisioning istanze di peso 4 e 8 per una capacità soddisfatta di 12. Se la policy di dimensionamento riduce la capacità di destinazione del 20% e si attiva un allarme, il processo di scalabilità automatica sottrae 12 x 0,2 da 12 ottenendo 9,6, che viene arrotondato a 10, quindi non viene intrapresa alcuna operazione di dimensionamento.
- Tempo di raffreddamento – Le policy di scalabilità create per il parco istanze spot supportano un tempo di raffreddamento. Si tratta del numero di secondi dopo il completamento di un'attività di dimensionamento in cui le precedenti attività di dimensionamento correlate all'attivazione possono influenzare gli eventi di dimensionamento futuri. Per le policy di dimensionamento, mentre è attivo il periodo di attesa, la capacità aggiunta all'evento di dimensionamento precedente che ha innescato l'attesa viene calcolata come parte della capacità desiderata per il dimensionamento successivo. L'intenzione è di aumentare di continuo (ma non in eccesso). Per le policy di riduzione, il periodo di attesa viene utilizzato per bloccare le richieste di riduzione ulteriori finché non è scaduto. L'intenzione è quella di ridurre in modo conservativo per proteggere la disponibilità dell'applicazione. Tuttavia, se un altro allarme attiva una policy di dimensionamento durante il periodo di attesa dopo un ridimensionamento, la scalabilità automatica aumenta immediatamente il target scalabile.
- Usare il monitoraggio dettagliato – Ti consigliamo di dimensionare in base a parametri di istanze con intervalli di 1 minuto, poiché questo garantisce una risposta più rapida alle variazioni di utilizzo. Il dimensionamento sui parametri a intervalli di 5 minuti potrebbe rallentare il tempo di risposta e causare il dimensionamento su dati di parametro obsoleti. Per inviare i dati sui parametri relativi alle istanze CloudWatch a intervalli di 1 minuto, puoi abilitare nello specifico il monitoraggio

dettagliato. Per ulteriori informazioni, consultare Gestione del monitoraggio dettagliato per le istanze EC2 e Crea una richiesta di parco istanze spot utilizzando parametri definiti.

- AWS CLI— Se utilizzi AWS CLI per configurare il ridimensionamento per Spot Fleet, utilizzerai i comandi application-autoscaling. https://docs.aws.amazon.com/cli/latest/reference/application-autoscaling

Autorizzazioni IAM richieste per la scalabilità automatica del parco istanze spot

La scalabilità automatica per Spot Fleet è resa possibile da una combinazione delle API Amazon EC2, Amazon e Application Auto Scaling. CloudWatch Le richieste Spot Fleet vengono create con Amazon EC2, gli allarmi con e le policy di scalabilità vengono create con CloudWatch Application Auto Scaling. In aggiunta alle autorizzazioni IAM richieste per usare il parco istanze spot e Amazon EC2, l'utente che accede alle impostazioni di scalabilità del parco istanze deve avere le autorizzazioni appropriate per i servizi che supportano la scalabilità automatica.

Per usare la scalabilità automatica per il parco istanze spot, gli utenti devono anche avere le autorizzazioni per utilizzare le operazioni mostrate nella seguente policy di esempio.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:*",
                "ec2:DescribeSpotFleetRequests",
                "ec2:ModifySpotFleetRequest",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DisableAlarmActions",
                "cloudwatch:EnableAlarmActions",
                "iam:CreateServiceLinkedRole",
                "sns:CreateTopic",
```

```
                "sns:Subscribe",
                "sns:Get*",
                "sns:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Puoi anche creare le tue policy IAM che consentono autorizzazioni più granulari per chiamate alle API Application Auto Scaling. Per ulteriori informazioni, consulta Gestione di identità e accesso per Application Auto Scaling nella Guida per l'utente di Application Auto Scaling.

Il servizio Application Auto Scaling richiede inoltre l'autorizzazione per descrivere la tua flotta Spot e gli CloudWatch allarmi e le autorizzazioni per modificare la capacità target di Spot Fleet per tuo conto. Se abiliti il dimensionamento automatico per la serie di istanze spot, viene creato un ruolo collegato ai servizi denominato `AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest`. Questo ruolo concede a Application Auto Scaling l'autorizzazione per descrivere gli allarmi per le policy, per monitorare la capacità attuale del parco istanze e modificare la capacità del parco istanze. Il ruolo originale della serie di istanze spot gestito per Application Auto Scaling era `aws-ec2-spot-fleet-autoscale-role`, ma non è più richiesto. Il ruolo collegato al servizio è il ruolo predefinito per Application Auto Scaling. Per ulteriori informazioni, consulta Service-linked i ruoli di Application Auto Scaling nella Guida per l'utente di Application Auto Scaling.

Dimensionamento con monitoraggio degli obiettivi: scala il parco istanze spot definendo come target un valore per una metrica specifica

Con il dimensionamento con monitoraggio degli obiettivi, crei una policy di dimensionamento con monitoraggio degli obiettivi selezionando un parametro e impostando un valore target. Spot Fleet crea e gestisce quindi gli CloudWatch allarmi che attivano la politica di ridimensionamento e calcola l'aggiustamento del ridimensionamento in base alla metrica scelta e al valore target. La policy di dimensionamento regola la capacità aggiungendo o rimuovendo istanze in base alle necessità per mantenere il parametro al valore target specificato o vicino a esso. Una policy di monitoraggio degli obiettivi non solo mantiene il parametro vicino al valore target, ma si adatta anche alle fluttuazioni del parametro dovute a un modello di carico fluttuante e riduce al minimo le fluttuazioni rapide della capacità.

È possibile creare più policy di dimensionamento con monitoraggio degli obiettivi per un parco istanze spot, purché ciascuna policy utilizzi parametri diversi. Il parco istanze si dimensiona in base alla

policy che specifica la capacità di parco istanze più ampia. Ciò ti consente di coprire più scenari per garantire una capacità sufficiente per i carichi di lavoro delle applicazioni.

Per garantire la disponibilità delle applicazioni, il parco istanze aumenta in proporzione al parametro il più veloce possibile, ma si riduce in modo più graduale.

Quando un parco istanze spot termina un'istanza spot a seguito della diminuzione della capacità obiettivo, l'istanza riceve un avviso di interruzione dell'istanza spot.

> **Note**
>
> Non modificate o eliminate gli CloudWatch allarmi gestiti da Spot Fleet per una politica di ridimensionamento del tracciamento degli obiettivi. Il parco istanze spot elimina gli allarmi automaticamente quando elimini la policy di dimensionamento con monitoraggio degli obiettivi.

Prerequisiti

- La richiesta del parco istanze spot deve avere un tipo di richiesta di `maintain`. La scalabilità automatica non è supportata per le richieste del tipo `request`.
- Configurare Autorizzazioni IAM richieste per la scalabilità automatica del parco istanze spot.
- Rivedere le Considerazioni.

Per configurare una policy di monitoraggio dei target

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di parco istanze spot.
4. Scegli la scheda Dimensionamento automatico nella parte inferiore dello schermo. Se hai selezionato il link per il tuo parco istanze spot, non è presente alcuna scheda; invece, scorri verso il basso fino alla sezione Dimensionamento automatico.
5. Se la scalabilità automatica non è configurata, selezionare Configure (Configurare).
6. Utilizzare Scale capacity between (Dimensionare capacità tra) per impostare la capacità minima e massima per il parco istanze. La scalabilità automatica non dimensiona il parco istanze al di sotto della capacità minima o al di sopra della capacità massima.
7. In Policy name (Nome policy), immettere un nome per la policy.

8. Selezionare un Target metric (Parametro di destinazione).
9. Immettere un Target value (Valore di destinazione) per il parametro.
10. Per il tempo di raffreddamento, specifica un nuovo valore (in secondi) o mantieni il valore predefinito.
11. (Facoltativo) Per omettere la creazione di una policy di ridimensionamento in base alla configurazione attuale, seleziona Disabilita dimensionamento. È possibile creare una policy di dimensionamento utilizzando una configurazione diversa.
12. Scegli Save (Salva).

Per configurare una politica di tracciamento degli obiettivi utilizzando AWS CLI

1. Registrare la richiesta del parco istanze spot come un obiettivo scalabile utilizzando il comando register-scalable-target
2. Creare una policy di dimensionamento utilizzando il comando put-scaling-policy.

Dimensionamento a fasi: scala il parco istanze spot utilizzando le policy di dimensionamento a fasi

Con le politiche di ridimensionamento graduale, si specificano gli CloudWatch allarmi per attivare il processo di ridimensionamento. Per esempio, se si vuole aumentare quando l'utilizzo della CPU raggiunge un determinato livello, creare un allarme utilizzando il parametro `CPUUtilization` fornito da Amazon EC2.

Quando si crea una policy di dimensionamento a fasi, bisogna specificare uno dei seguenti tipi di adeguamento dimensionamento:

- Add (Aggiungi) – Aumenta la capacità obiettivo del parco istanze di un numero specifico di unità di capacità o di una percentuale specifica della capacità attuale.
- Remove (Rimuovi) – Diminuisce la capacità obiettivo del parco istanze di un numero specifico di unità di capacità o di una percentuale specifica della capacità attuale.
- Set to (Imposta su) – Imposta la capacità obiettivo del parco istanze sul numero di unità di capacità specificato.

Quando viene innescato un allarme, il processo di scalabilità automatica calcola la nuova capacità target utilizzando la capacità soddisfatta e la policy di dimensionamento, quindi aggiorna la capacità

target di conseguenza. Per esempio, supponiamo che la capacità di destinazione e quella soddisfatta siano 10 e che la policy di dimensionamento aggiunga 1. Quando si attiva l'allarme, il processo di scalabilità automatica aggiunge 1 a 10 per ottenere 11, quindi il parco istanze spot avvia 1 istanza.

Quando un parco istanze spot termina un'istanza spot a seguito della diminuzione della capacità obiettivo, l'istanza riceve un avviso di interruzione dell'istanza spot.

Prerequisiti

- La richiesta del parco istanze spot deve avere un tipo di richiesta di `maintain`. La scalabilità automatica non è supportata per le richieste del tipo `request`.
- Configurare Autorizzazioni IAM richieste per la scalabilità automatica del parco istanze spot.
- Considerate quali CloudWatch metriche sono importanti per la vostra applicazione. Puoi creare CloudWatch allarmi in base alle metriche fornite da AWS o alle tue metriche personalizzate.
- Per le AWS metriche che utilizzerai nelle tue politiche di scalabilità, abilita la raccolta delle CloudWatch metriche se il servizio che fornisce le metriche non la abilita per impostazione predefinita.
- Rivedere le Considerazioni.

Per creare un allarme CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, espandi Allarmi, e scegli Tutti gli allarmi.
3. Selezionare Create Alarm (Crea allarme).
4. Nella pagina Specify metric and conditions (Specifica parametro e condizioni), scegliere Select metric (Seleziona parametro).
5. Scegli EC2 Spot, quindi Fleet Request Metrics, quindi seleziona una metrica (ad esempio TargetCapacity), quindi scegli Seleziona metrica.

   Viene visualizzata la pagina Specify metric and conditions (Specifica parametro e condizioni) contenente un grafico e altre informazioni sul parametro selezionato.
6. In Periodo, scegliere il periodo di valutazione per l'allarme, ad esempio 1 minuto. Durante la valutazione dell'allarme, ogni periodo è aggregato in un punto dati.

> **Note**
>
> Un periodo più breve crea un allarme più sensibile.

7. In Conditions (Condizioni), definire l'allarme specificando la condizione di soglia. Ad esempio, è possibile definire una soglia per attivare l'allarme ogni volta che il valore del parametro è maggiore o uguale all'80%.
8. In Additional configuration (Configurazione aggiuntiva), per Datapoints to alarm (Punto di dati per allarme), specificare il numero di punti di dati (periodi di valutazione) che devono trovarsi nello stato ALLARME per attivare l'allarme, ad esempio, 1 periodo di valutazione su 2 di 3 periodi di valutazione. Questo consente di creare un allarme che passa allo stato ALARM se si verifica un superamento durante tali periodi consecutivi. Per ulteriori informazioni, consulta Evaluating an alarm nella Amazon User Guide. CloudWatch
9. Per Missing data treatment (Trattamento dati mancanti), selezionare una delle opzioni (o lasciare il valore di default di Treat missing data as missing (Tratta i dati mancanti come mancanti)). Per ulteriori informazioni, consulta Configurare il modo in cui gli CloudWatch allarmi trattano i dati mancanti nella Amazon CloudWatch User Guide.
10. Scegli Next (Successivo).
11. (Facoltativo) Per ricevere la notifica di un evento di dimensionamento, per Notification (Notifica), è possibile scegliere o creare l'argomento Amazon SNS da utilizzare per ricevere notifiche. Altrimenti, è possibile eliminare ora le notifiche e aggiungerne una in un secondo momento ove necessario.
12. Scegli Next (Successivo).
13. In Aggiungere nome e descrizione, immettere un nome e una descrizione per l'allarme e scegliere Successivo).
14. Scegli Crea allarme.

Per configurare una policy di dimensionamento per fasi per il parco istanze spot

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di parco istanze spot.

4. Scegli la scheda Dimensionamento automatico nella parte inferiore dello schermo. Se hai selezionato il link per il tuo parco istanze spot, non è presente alcuna scheda; invece, scorri verso il basso fino alla sezione Dimensionamento automatico.
5. Se la scalabilità automatica non è configurata, selezionare Configure (Configurare).
6. Utilizzare Scale capacity between (Dimensionare capacità tra) per impostare la capacità minima e massima per il parco istanze. Le policy di dimensionamento non dimensionano il parco istanze al di sotto della capacità minima o al di sopra della capacità massima.
7. In Policy di dimensionamento, per Tipo di policy, scegli Policy di dimensionamento a fasi.
8. Inizialmente, le Policy di dimensionamento contengono policy di dimensionamento a fasi denominate ScaleUp e ScaleDown. È possibile completare tali policy o selezionare Remove policy (Rimuovi policy) per eliminarle. È possibile anche scegliere Add policy (Aggiungi policy).
9. Per definire una policy, effettuare le operazioni seguenti:

    a. In Policy name (Nome policy), immettere un nome per la policy.

    b. Per attivare la policy, seleziona un allarme esistente o scegli Crea allarme per aprire la CloudWatch console Amazon e creare un allarme.

    c. Per Modifica capacità, definisci la quantità in base alla quale dimensionare e il limite inferiore e superiore della regolazione del livello. È possibile aggiungere o rimuovere un numero specifico di istanze o una percentuale della dimensione del parco istanze esistente, oppure impostare il parco istanze su una dimensione specifica.

    Ad esempio, per creare una policy di dimensionamento a fasi che aumenti la capacità del parco istanze del 30 percento, scegli Aggiungi, digita 30 nel campo successivo e quindi scegli percento. Per impostazione predefinita, il limite inferiore per una policy di aggiunta è la soglia di allarme e il limite superiore è positivo (+) infinito. Per impostazione predefinita, il limite superiore per una policy di rimozione è la soglia di allarme e il limite inferiore è negativo (-) infinito.

    d. (Facoltativo) Per aggiungere un'altra fase, seleziona Aggiungi fase.

    e. Per il tempo di raffreddamento, specifica un nuovo valore (in secondi) o mantieni il valore predefinito.
10. Scegli Save (Salva).

Per configurare le policy di scalabilità graduale per la tua flotta Spot, utilizza AWS CLI

1. Registrare la richiesta del parco istanze spot come un obiettivo scalabile utilizzando il comando register-scalable-target
2. Creare una policy di dimensionamento utilizzando il comando put-scaling-policy.
3. Creare un allarme che attivi la policy di dimensionamento utilizzando il comando put-metric-alarm.

Dimensionamento pianificato: scala il parco istanze spot in base a una pianificazione

Il dimensionamento del parco istanze su una pianificazione consente di dimensionare le applicazioni in relazione alle variazioni di domanda prevedibili. Creando operazioni pianificate, puoi ordinare al parco istanze spot di eseguire attività di dimensionamento a orari specifici. Per creare un'operazione pianificata, devi specificare un parco istanze spot esistente, l'orario in cui l'attività di dimensionamento deve verificarsi e la capacità minima e massima desiderata. Le operazioni pianificate possono essere configurate in modo da scalare una sola volta o in base a una pianificazione ricorrente. Se hai bisogno di apportare cambiamenti, puoi modificare o eliminare operazioni pianificate.

Prerequisiti

- Le azioni pianificate possono essere create solo per i parchi istanze spot. Non è possibile creare operazioni pianificate quando crei un parco istanze spot.
- La richiesta del parco istanze spot deve avere un tipo di richiesta di `maintain`. La scalabilità automatica non è supportata per le richieste del tipo `request`.
- Configurare Autorizzazioni IAM richieste per la scalabilità automatica del parco istanze spot.
- Rivedere le Considerazioni.

Per creare un'operazione pianificata una tantum

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di parco istanze spot.
4. Scegli la scheda Dimensionamento pianificato nella parte inferiore dello schermo. Se hai selezionato il link per il tuo parco istanze Spot, non è presente alcuna scheda; invece, scorri verso il basso fino alla sezione Dimensionamento pianificato.

5. Scegli Crea operazione pianificata.
6. In Name (Nome), specificare un nome per l'operazione pianificata.
7. Immettere un valore per Minimum capacity (Capacità minima), Maximum capacity (Capacità massima) o per entrambi i campi.
8. Per Recurrence (Ricorrenza), scegliere Once (Una tantum).
9. (Facoltativo) Scegliere una data e un'ora per Start time (Ora di inizio), End time (Ora di fine) o per entrambi i campi.
10. Scegli Create (Crea).

Per creare un'operazione pianificata ricorrente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di parco istanze spot.
4. Scegli la scheda Dimensionamento pianificato nella parte inferiore dello schermo. Se hai selezionato il link per il tuo parco istanze Spot, non è presente alcuna scheda; invece, scorri verso il basso fino alla sezione Dimensionamento pianificato.
5. In Name (Nome), specificare un nome per l'operazione pianificata.
6. Immettere un valore per Minimum capacity (Capacità minima), Maximum capacity (Capacità massima) o per entrambi i campi.
7. Per Recurrence (Ricorrenza), scegliere uno dei piani predefiniti (ad esempio, Every day (Ogni giorno)), oppure scegliere Custom (Personalizzato) e immettere un'espressione cron. Per ulteriori informazioni sulle espressioni cron supportate dal ridimensionamento pianificato, consulta le espressioni Cron nella Amazon User Guide. EventBridge
8. (Facoltativo) Scegliere una data e un'ora per Start time (Ora di inizio), End time (Ora di fine) o per entrambi i campi.
9. Seleziona Submit (Invia).

Per modificare un'operazione pianificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di parco istanze spot.

4. Scegli la scheda Dimensionamento pianificato nella parte inferiore dello schermo. Se hai selezionato il link per il tuo parco istanze Spot, non è presente alcuna scheda; invece, scorri verso il basso fino alla sezione Dimensionamento pianificato.
5. Selezionare l'operazione pianificata e scegliere Actions (Operazioni), Edit (Modifica).
6. Apportare le modifiche necessarie e scegliere Invia.

Per eliminare un'operazione pianificata

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Spot Requests (Richieste Spot).
3. Seleziona la richiesta di parco istanze spot.
4. Scegli la scheda Dimensionamento pianificato nella parte inferiore dello schermo. Se hai selezionato il link per il tuo parco istanze Spot, non è presente alcuna scheda; invece, scorri verso il basso fino alla sezione Dimensionamento pianificato.
5. Selezionare l'operazione pianificata e scegliere Actions (Operazioni), Elimina.
6. Quando viene richiesta la conferma, seleziona Elimina.

Per gestire il ridimensionamento pianificato utilizzando AWS CLI

Utilizza il seguente comando:

- put-scheduled-action
- describe-scheduled-actions
- delete-scheduled-action

Monitoraggio del parco istanze EC2 o del parco istanze spot

Un monitoraggio efficace del parco istanze EC2 o del parco istanze Spot è essenziale per mantenere prestazioni ottimali e garantire l'affidabilità. Esistono vari strumenti per aiutarti a raggiungere questo obiettivo, tra cui Amazon CloudWatch e Amazon EventBridge, trattati in questo argomento.

Con CloudWatch, puoi raccogliere e tenere traccia delle metriche, impostare allarmi e reagire automaticamente ai cambiamenti nello stato della tua flotta.

Con EventBridge, puoi monitorare e rispondere in modo programmatico agli eventi emessi dalla tua flotta. Definendo delle regole in EventBridge, è possibile automatizzare le risposte a eventi

specifici della flotta, come la cessazione dell'istanza o le modifiche allo stato della flotta, migliorando l'efficienza operativa.

Argomenti

- Monitora la tua flotta EC2 o la tua flotta Spot utilizzando CloudWatch
- Monitora e rispondi in modo programmatico agli eventi emessi dalla tua flotta EC2 o dalla tua flotta Spot utilizzando Amazon EventBridge

Monitora la tua flotta EC2 o la tua flotta Spot utilizzando CloudWatch

Puoi monitorare la tua flotta EC2 o la tua flotta Spot utilizzando le CloudWatch metriche Amazon descritte in questa sezione.

> **Important**
>
> Per garantire l'accuratezza, consigliamo di attivare il monitoraggio dettagliato durante l'utilizzo di tali parametri. Per ulteriori informazioni, consulta Gestione del monitoraggio dettagliato per le istanze EC2.

Per ulteriori informazioni sull'utilizzo CloudWatch, consulta. Monitora le tue istanze utilizzando CloudWatch

Metriche del parco istanze EC2 e del parco istanze spot

Il `AWS/EC2Spot` namespace include le seguenti metriche per la tua flotta, oltre alle CloudWatch metriche per le istanze Spot della tua flotta. Per ulteriori informazioni, consulta Parametri dell'istanza.

Parametro	Description
`AvailableInstancePoolsCount`	I pool di capacità spot specificati nella richiesta di parco istanze. Unità: numero
`BidsSubmittedForCapacity`	La capacità per cui Amazon EC2 ha inviato richieste di parco istanze.

Parametro	Description
	Unità: numero
`EligibleInstancePoolCount`	I pool di capacità spot specificati nella richiesta di parco istanze in cui Amazon EC2 può evadere le richieste. Amazon EC2 non soddisfa le richieste nei pool in cui il prezzo massimo che sei disposto a pagare per le istanze Spot è inferiore al prezzo Spot o il prezzo Spot è superiore al prezzo delle istanze. On-Demand Unità: numero
`FulfilledCapacity`	La capacità soddisfatta da Amazon EC2. Unità: numero
`MaxPercentCapacityAllocation`	Il valore massimo di `PercentCapacityAllocation` in tutti i pool del parco istanze specificati nella richiesta di parco istanze. Unità: percentuale
`PendingCapacity`	La differenza tra `TargetCapacity` e `FulfilledCapacity`. Unità: numero
`PercentCapacityAllocation`	La capacità allocata per il pool di capacità spot per le dimensioni specificate. Per ottenere il valore massimo registrato in tutti i pool di capacità spot, utilizza `MaxPercentCapacityAllocation`. Unità: percentuale
`TargetCapacity`	La capacità target di una richiesta di parco istanze. Unità: numero

Parametro	Description
`TerminatingCapacity`	La capacità che si sta terminando perché la capacità di cui si è effettuato il provisioning supera quella di destinazione. Unità: numero

Se un'unità di misura per un parametro è `Count`, la statistica più utile è `Average`.

Dimensioni del parco istanze EC2 e del parco istanze spot

Per filtrare i dati relativi al parco istanze, usa le seguenti dimensioni.

Dimensioni	Descrizione
`AvailabilityZone`	Consente di filtrare i dati per zona di disponibilità.
`FleetRequestId`	Consente di filtrare i dati in base alla richiesta del parco istanze.
`InstanceType`	Consente di filtrare i dati per tipo di istanza.

Visualizza le CloudWatch metriche relative alla tua flotta EC2 o alla tua flotta Spot

Puoi visualizzare le CloudWatch metriche della tua flotta utilizzando la console Amazon. CloudWatch Tali parametri vengono visualizzati come grafici di monitoraggio. Tali grafici mostrano i punti dati se il parco istanze è attivo.

I parametri sono raggruppati in primo luogo in base al namespace e in secondo luogo in base alle diverse combinazioni delle dimensioni all'interno di ciascun namespace. Ad esempio, è possibile visualizzare tutti i parametri del parco istanze o i gruppi di parametri del parco istanze in base all'ID richiesta del parco istanze, al tipo di istanza o alla zona di disponibilità.

Per visualizzare i parametri del parco istanze

1. Apri la CloudWatch console all'indirizzo. https://console.aws.amazon.com/cloudwatch/
2. Nel pannello di navigazione, espandi Parametri, quindi scegli Tutti i parametri.
3. Scegliere il namespace Spot EC2.

> **Note**
>
> Se il namespace Spot EC2 non viene visualizzato, i motivi possono essere due. O non hai mai utilizzato EC2 Fleet o Spot Fleet nella regione: solo AWS i servizi che stai utilizzando inviano le metriche ad Amazon. CloudWatch Oppure, se hai utilizzato il parco istanze EC2 o il parco istanze spot nella regione, ma non nelle ultime due settimane, il namespace non viene visualizzato.

4. Per filtrare i parametri per dimensione, scegli una delle opzioni seguenti:
   - Parametri di richiesta di parco istanze - Raggruppare per richiesta di parco istanze
   - Per zona di disponibilità - Raggruppare per richiesta di parco istanze e zona di disponibilità
   - Per tipo di istanza - Raggruppare per richiesta di parco istanze e tipo di istanza
   - Per Zone/Instance tipo di disponibilità: raggruppa per richiesta del parco veicoli, zona di disponibilità e tipo di istanza
5. Per visualizzare i dati di un parametro, selezionare la casella di spunta accanto al parametro.

Monitora e rispondi in modo programmatico agli eventi emessi dalla tua flotta EC2 o dalla tua flotta Spot utilizzando Amazon EventBridge

Quando lo stato di un parco istanze EC2 o del parco istanze spot viene modificato, viene emessa una notifica. La notifica è disponibile come evento inviato ad Amazon EventBridge (precedentemente noto come Amazon CloudWatch Events). Gli eventi vengono emessi secondo il principio del massimo sforzo.

Puoi usare Amazon EventBridge per creare regole che attivano azioni programmatiche in risposta a un evento. Ad esempio, puoi creare due EventBridge regole: una attivata quando lo stato di una flotta cambia e un'altra attivata quando un'istanza della flotta viene interrotta. In questo esempio, se lo stato del parco istanze cambia, puoi configurare la prima regola in modo che richiami un argomento SNS, inviando inviare una notifica via e-mail. Se un'istanza nel parco istanze viene terminata, puoi configurare la seconda regola in modo che richiami una funzione Lambda per avviare una nuova istanza.

> **Note**
>
> Solo i parchi istanze di tipo `maintain` ed `request` emettono eventi. I parchi istanze del tipo `instant` non emettono eventi perché inviano richieste sincrone una tantum e lo stato del parco istanze è noto immediatamente nella risposta. Per utilizzare Amazon EventBridge per monitorare gli eventi della flotta, il tipo di richiesta deve essere o. `maintain` `request`

Per istruzioni su come descrivere la cronologia degli eventi di un parco istanze, consulta Descrivi la cronologia degli eventi per il parco istanze EC2.

Argomenti

- Crea EventBridge regole Amazon per monitorare gli eventi EC2 Fleet o Spot Fleet
- Tipi di eventi Parco istanze EC2
- Tipi di eventi del parco istanze spot

Crea EventBridge regole Amazon per monitorare gli eventi EC2 Fleet o Spot Fleet

Quando viene emessa una notifica di modifica dello stato per una flotta EC2 o una flotta Spot, viene inviata come evento ad Amazon EventBridge come file JSON. Se EventBridge rileva un modello di evento che corrisponde a uno schema definito in una regola, EventBridge richiama l'obiettivo (o i target) specificati nella regola.

È possibile scrivere EventBridge regole per automatizzare le azioni in base a modelli di eventi corrispondenti.

I campi seguenti nell'evento costituiscono il modello di evento definito nella regola:

```
"source": "aws.ec2fleet"
```

Identifica che l'evento proviene da parco istanze EC2.

```
"detail-type": "EC2 Fleet State Change"
```

Identifica il tipo di evento.

```
"detail": { "sub-type": "submitted" }
```

Identifica il sottotipo di evento.

Per l'elenco degli eventi del parco istanze EC2 e del parco istanze spot dei dati degli eventi di esempio, consulta Tipi di eventi Parco istanze EC2 e Tipi di eventi del parco istanze spot.

Esempi

- Crea una EventBridge regola per inviare una notifica
- Crea una EventBridge regola per attivare una funzione Lambda

Crea una EventBridge regola per inviare una notifica

L'esempio seguente crea una EventBridge regola per inviare un'e-mail, un messaggio di testo o una notifica push mobile ogni volta che Amazon EC2 emette una notifica di modifica dello stato della flotta EC2. Il segnale in questo esempio viene emesso come evento `EC2 Fleet State Change`, che attiva l'azione definita dalla regola.

Prerequisito

Prima di creare la EventBridge regola, devi creare l'argomento Amazon SNS per l'e-mail, il messaggio di testo o la notifica push mobile.

Per creare una EventBridge regola per inviare una notifica quando lo stato di una flotta EC2 cambia

1. Apri la EventBridge console Amazon all'indirizzo. https://console.aws.amazon.com/events/
2. Scegli Crea regola.
3. Per Define rule detail (Definisci dettagli della regola), effettua le seguenti operazioni:
   a. Immettere un Name (Nome) per la regola e, facoltativamente, una descrizione.

      Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso bus di eventi.
   b. Per Event bus (Bus di eventi), scegli default. Quando un AWS servizio del tuo account genera un evento, viene sempre indirizzato al bus eventi predefinito del tuo account.
   c. Per Tipo di regola, scegli Regola con un modello di eventi.
   d. Scegli Avanti.
4. Per Build event pattern (Crea modello di eventi), procedi come segue:
   a. Per Origine degli eventi, scegli AWS eventi o eventi EventBridge partner.
   b. Per Event pattern (Modello di eventi), ai fini di questo esempio specificherai il seguente modello di eventi in modo che corrisponda all'evento `EC2 Fleet Instance Change`.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"]
}
```

Per aggiungere il modello di eventi, puoi utilizzare un modello scegliendo Event pattern form (Formato del modello di eventi) o specificare il tuo modello scegliendo Custom pattern (JSON editor) (Modello personalizzato (editor JSON)), come segue:

i. Per utilizzare un modello per creare il modello di eventi, procedi come segue:

   A. Scegli Event pattern form (Formato del modello di eventi).

   B. Per Event source (Origine evento), scegli AWS services (Servizi).

   C. In AWS Service, scegli parco istanze EC2.

   D. Per Event type (Tipo di evento), scegli EC2 Fleet Instance Change (Modifica dell'istanza del parco istanze EC2).

   E. Per personalizzare il modello, scegli Edit pattern (Modifica modello) e apporta le modifiche in modo che corrisponda al modello di eventi di esempio.

ii. (Alternativa) Per specificare un modello di eventi personalizzato, procedi come segue:

   A. Scegli Custom pattern (JSON editor) (Modello personalizzato (editor JSON)).

   B. Nella casella Event pattern (Modello di eventi), aggiungi il modello di eventi per questo esempio.

c. Scegli Avanti.

5. Per Select target(s) (Seleziona destinazione/i), esegui queste operazioni:

   a. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).

   b. Per Select a target (Seleziona una destinazione, scegli SNS topic (Argomento SNS) per inviare un'e-mail, un messaggio di testo o una notifica push mobile quando si verifica l'evento.

   c. Per Argomento, scegliere un argomento esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) messaging (Utilizzo di Amazon SNS per la messaggistica da applicazione a persona (A2P)) nella Guida per lo sviluppatore di Amazon Simple Notification Service.

d. (Facoltativo) In Additional settings (Impostazioni aggiuntive), facoltativamente puoi configurare impostazioni aggiuntive. Per ulteriori informazioni, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi (passaggio 16) nella Amazon EventBridge User Guide.

e. Scegli Avanti.

6. (Opzionale) Per Tags (Tag), se desideri puoi assegnare uno o più tag alla regola, quindi scegli Next (Successivo).

7. Per Review and create (Verifica e crea), procedi come segue:

a. Verifica i dettagli della regola e modificali se necessario.

b. Scegli Crea regola.

Per ulteriori informazioni, consulta EventBridge le regole di Amazon e i modelli di EventBridge eventi Amazon nella Amazon EventBridge User Guide

Crea una EventBridge regola per attivare una funzione Lambda

L'esempio seguente crea una EventBridge regola per attivare una funzione Lambda ogni volta che Amazon EC2 emette una notifica di modifica dell'istanza EC2 Fleet per l'avvio di un'istanza. Il segnale in questo esempio viene emesso come evento `EC2 Fleet Instance Change`, sottotipo `launched`, che attiva l'azione definita dalla regola.

Prima di creare la EventBridge regola, devi creare la funzione Lambda.

Per creare la funzione Lambda da utilizzare nella regola EventBridge

1. Apri la AWS Lambda console all'indirizzo. https://console.aws.amazon.com/lambda/
2. Selezionare Create function (Crea funzione).
3. Immettere un nome per la funzione, configurare il codice, quindi scegliere Create function (Crea funzione).

   Per ulteriori informazioni, consulta Create your first Lambda function nella Guida per gli sviluppatori di AWS Lambda .

Per creare una EventBridge regola per attivare una funzione Lambda quando un'istanza in una flotta EC2 cambia stato

1. Apri la EventBridge console Amazon all'indirizzo. https://console.aws.amazon.com/events/
2. Scegli Crea regola.
3. Per Define rule detail (Definisci dettagli della regola), effettua le seguenti operazioni:

   a. Immettere un Name (Nome) per la regola e, facoltativamente, una descrizione.

      Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso bus di eventi.

   b. Per Event bus (Bus di eventi), scegli default. Quando un AWS servizio del tuo account genera un evento, viene sempre indirizzato al bus eventi predefinito del tuo account.

   c. Per Tipo di regola, scegli Regola con un modello di eventi.

   d. Scegli Avanti.
4. Per Build event pattern (Crea modello di eventi), procedi come segue:

   a. Per Origine degli eventi, scegli AWS eventi o eventi EventBridge partner.

   b. Per Event pattern (Modello di eventi), ai fini di questo esempio specificherai il seguente modello di eventi in modo che corrisponda all'evento `EC2 Fleet Instance Change` e al sottotipo `launched`.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"],
 "detail": {
   "sub-type": ["launched"]
}
```

      Per aggiungere il modello di eventi, puoi utilizzare un modello scegliendo Event pattern form (Formato del modello di eventi) o specificare il tuo modello scegliendo Custom pattern (JSON editor) (Modello personalizzato (editor JSON)), come segue:

      i. Per utilizzare un modello per creare il modello di eventi, procedi come segue:

         A. Scegli Event pattern form (Formato del modello di eventi).

         B. Per Event source (Origine evento), scegli AWS services (Servizi).

         C. In AWS Service, scegli parco istanze EC2.

D. Per Event type (Tipo di evento), scegli EC2 Fleet Instance Change (Modifica dell'istanza del parco istanze EC2).

E. Scegli Edit pattern (Modifica modello) e aggiungi `"detail": {"sub-type": ["launched"]` per creare una corrispondenza con il modello di evento di esempio. Per il corretto formato JSON, inserisci una virgola (`,`) dopo la parentesi quadrata precedente (`]`).

ii. (Alternativa) Per specificare un modello di eventi personalizzato, procedi come segue:

A. Scegli Custom pattern (JSON editor) (Modello personalizzato (editor JSON)).

B. Nella casella Event pattern (Modello di eventi), aggiungi il modello di eventi per questo esempio.

c. Scegli Avanti.

5. Per Select target(s) (Seleziona destinazione/i), esegui queste operazioni:

a. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).

b. Per Select a target (Seleziona una destinazione, scegli SNS topic (Argomento SNS) per inviare un'e-mail, un messaggio di testo o una notifica push mobile quando si verifica l'evento.

c. Per Target, scegli Lambda function (Funzione Lambda), e in Function (Funzione), scegli la funzione creata per rispondere quando si verifica l'evento.

d. (Facoltativo) In Additional settings (Impostazioni aggiuntive), facoltativamente puoi configurare impostazioni aggiuntive. Per ulteriori informazioni, consulta Creazione di EventBridge regole Amazon che reagiscono agli eventi (passaggio 16) nella Amazon EventBridge User Guide.

e. Scegli Avanti.

6. (Opzionale) Per Tags (Tag), se desideri puoi assegnare uno o più tag alla regola, quindi scegli Next (Successivo).

7. Per Review and create (Verifica e crea), procedi come segue:

a. Verifica i dettagli della regola e modificali se necessario.

b. Scegli Crea regola.

Per un tutorial su come creare una funzione Lambda e una EventBridge regola che esegua la funzione Lambda, consulta Tutorial: Log the State of an Amazon EC2 Instance Using EventBridge in the AWS Lambda Developer Guide.

Tipi di eventi Parco istanze EC2

Esistono cinque tipi di eventi Parco istanze EC2. Per ogni tipo di evento, ci sono diversi sottotipi.

Event types (Tipi di evento)

- Cambiamento di stato del parco istanze EC2
- Richiesta di modifica dell'istanza spot del parco istanze EC2
- Modifica dell'istanza del parco istanze EC2
- Informazioni sul parco istanze EC2
- Errore parco istanze EC2

Cambiamento di stato del parco istanze EC2

La flotta EC2 invia un `EC2 Fleet State Change` evento ad Amazon EventBridge quando una flotta EC2 cambia stato.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "715ed6b3-b8fc-27fe-fad6-528c7b8bf8a2",
    "detail-type": "EC2 Fleet State Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:20Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "sub-type": "active"
    }
}
```

I valori possibili per `sub-type` sono:

`active`

La richiesta parco istanze EC2 è stata convalidata ed Amazon EC2 sta tentando di mantenere il numero previsto di istanze in esecuzione.

`deleted`

Il parco istanze EC2 viene eliminato e non ha istanze in esecuzione. La richiesta parco istanze EC2 viene eliminata due giorni dopo e le sue istanze vengono terminate.

`deleted_running`

La richiesta Parco istanze EC2 viene eliminata e non avvia istanze aggiuntive. Le sue istanze esistenti continuano a essere eseguite finché non vengono interrotte o terminate. La richiesta rimane in questo stato finché tutte le istanze non vengono interrotte o terminate.

`deleted_terminating`

La richiesta del parco istanze EC2 viene eliminata e le sue istanze vengono terminate. La richiesta rimane in questo stato finché tutte le istanze non vengono terminate.

`expired`

La richiesta parco istanze EC2 è scaduta. Se la richiesta è stata creata con un set `TerminateInstancesWithExpiration`, un evento successivo `terminated` indica che le istanze sono terminate.

`modify_in_progress`

La richiesta parco istanze EC2 è in fase di modifica. La richiesta rimane in questo stato finché la modifica non viene completamente elaborata.

`modify_succeeded`

La richiesta parco istanze EC2 è stata modificata.

`submitted`

La richiesta parco istanze EC2 è in fase di valutazione ed Amazon EC2 si sta preparando ad avviare il numero previsto di istanze.

`progress`

La richiesta parco istanze EC2 è in procinto di essere soddisfatta.

Richiesta di modifica dell'istanza spot del parco istanze EC2

EC2 Fleet invia un `EC2 Fleet Spot Instance Request Change` evento ad Amazon EventBridge quando una richiesta di istanza Spot nella flotta cambia stato.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "19331f74-bf4b-a3dd-0f1b-ddb1422032b9",
    "detail-type": "EC2 Fleet Spot Instance Request Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:05Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"
    ],
    "detail": {
        "spot-instance-request-id": "sir-rmqske6h",
        "description": "SpotInstanceRequestId sir-rmqske6h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

I valori possibili per `sub-type` sono:

`active`

La richiesta è stata soddisfatta e ha un'istanza spot associata.

`cancelled`

Hai annullato la richiesta dell'istanza spot o la richiesta dell'istanza spot è scaduta.

`disabled`

Hai arrestato l'istanza spot.

`submitted`

La richiesta dell'istanza spot viene inviata.

Modifica dell'istanza del parco istanze EC2

EC2 Fleet invia un `EC2 Fleet Instance Change` evento ad Amazon EventBridge quando un'istanza della flotta cambia stato.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "542ce428-c8f1-0608-c015-e8ed6522c5bc",
    "detail-type": "EC2 Fleet Instance Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:23Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "instance-id": "i-0c594155dd5ff1829",
        "description": "{\"instanceType\":\"c5.large\",\"image\":\"ami-6057e21a\",
\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":\"us-east-1d\"}",
        "sub-type": "launched"
    }
}
```

I valori possibili per `sub-type` sono:

`launched`

È stata lanciata una nuova istanza.

`terminated`

L'istanza è stata terminata.

`termination_notified`

Una notifica di terminazione dell'istanza è stata inviata quando un'istanza spot è stata terminata da Amazon EC2 durante la riduzione orizzontale, quando la capacità target del parco istanze è stata modificata, ad esempio, da una capacità target di 4 a una capacità target di 3.

Informazioni sul parco istanze EC2

EC2 Fleet invia un `EC2 Fleet Information` evento ad Amazon EventBridge in caso di errore durante l'evasione. L'evento informativo non impedisce al parco istanze di tentare di raggiungere la sua capacità target.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "76529817-d605-4571-7224-d36cc1b2c0c4",
    "detail-type": "EC2 Fleet Information",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T08:17:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-8becf5fe-
bb9e-415d-8f54-3fa5a8628b91"
    ],
    "detail": {
        "description": "c4.xlarge, ami-0947d2ba12ee1ff75, Linux/UNIX, us-east-1a,
 Spot price in either SpotFleetRequestConfigData or SpotFleetLaunchSpecification or
 LaunchTemplate or LaunchTemplateOverrides is less than Spot market price $0.0619",
        "sub-type": "launchSpecUnusable"
    }
}
```

I valori possibili per `sub-type` sono:

`fleetProgressHalted`

Il prezzo in ogni specifica di avvio non è valido perché è inferiore al prezzo istanza spot (tutte le specifiche di avvio hanno prodotto eventi `launchSpecUnusable`). Una specifica di avvio potrebbe diventare valida se il prezzo Spot cambia.

`launchSpecTemporarilyBlacklisted`

La configurazione non è valida e vari tentativi di avvio delle istanze non sono riusciti. Per ulteriori informazioni, consulta la descrizione dell'evento.

`launchSpecUnusable`

Il prezzo in una specifica di avvio non è valido perché è inferiore al prezzo istanza spot o il prezzo istanza spot è inferiore al prezzo on demand.

`registerWithLoadBalancersFailed`

Tentativo di registrazione di istanze con bilanciamento del carico non riuscito. Per ulteriori informazioni, consulta la descrizione dell'evento.

Errore parco istanze EC2

EC2 Fleet invia un `EC2 Fleet Error` evento ad Amazon in caso di errore EventBridge durante l'evasione dell'ordine. L'evento di errore impedisce al parco istanze di tentare di raggiungere la sua capacità target.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "69849a22-6d0f-d4ce-602b-b47c1c98240e",
    "detail-type": "EC2 Fleet Error",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-10-07T01:44:24Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-9bb19bc6-60d3-4fd2-ae47-
d33e68eafa08"
    ],
    "detail": {
        "description": "m3.large, ami-00068cd7555f543d5, Linux/UNIX: IPv6 is not
 supported for the instance type 'm3.large'. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

I valori possibili per `sub-type` sono:

`iamFleetRoleInvalid`

Il parco istanze EC2 non include le autorizzazioni necessarie per avviare o terminare un'istanza.

`allLaunchSpecsTemporarilyBlacklisted`

Nessuna delle configurazioni è valida e vari tentativi di avvio delle istanze non sono riusciti. Per ulteriori informazioni, consulta la descrizione dell'evento.

`spotInstanceCountLimitExceeded`

Hai raggiunto il limite del numero di istanze spot che puoi avviare.

`spotFleetRequestConfigurationInvalid`

La configurazione non è valida. Per ulteriori informazioni, consulta la descrizione dell'evento.

Tipi di eventi del parco istanze spot

> **Note**
>
> Spot Fleet utilizza un'API legacy senza investimenti pianificati. Consigliamo invece di utilizzare EC2 Fleet o un gruppo Auto Scaling. Per ulteriori informazioni, consulta Qual è il metodo per parco istanze migliore da utilizzare?.

Esistono cinque tipi di eventi del parco istanze spot Per ogni tipo di evento, ci sono diversi sottotipi.

Event types (Tipi di evento)

- Cambiamento dello stato del parco istanze spot di EC2
- Modifica della richiesta del parco istanze spot EC2
- Modifica dell'istanza del parco istanze spot di EC2
- Informazioni sul parco istanze spot di EC2
- Errore del parco istanze spot EC2

Cambiamento dello stato del parco istanze spot di EC2

Spot Fleet invia un `EC2 Spot Fleet State Change` evento ad Amazon EventBridge quando una flotta Spot cambia stato.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
```

```
    "version": "0",
    "id": "d1af1091-6cc3-2e24-203a-3b870e455d5b",
    "detail-type": "EC2 Spot Fleet State Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:57:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-4b6d274d-0cea-4b2c-
b3be-9dc627ad1f55"
    ],
    "detail": {
        "sub-type": "submitted"
    }
}
```

I valori possibili per `sub-type` sono:

`active`

La richiesta del parco istanze spot è stata convalidata e Amazon EC2 sta tentando di mantenere il numero previsto di istanze in esecuzione.

`cancelled`

La richiesta del parco istanze spot viene annullata e non contiene istanze in esecuzione. Il parco istanze spot verrà eliminato due giorni dopo la chiusura delle istanze.

`cancelled_running`

La richiesta del parco istanze spot viene annullata e non avvia istanze aggiuntive. Le sue istanze esistenti continuano a essere eseguite finché non vengono interrotte o terminate. La richiesta rimane in questo stato finché tutte le istanze non vengono interrotte o terminate.

`cancelled_terminating`

La richiesta del parco istanze spot viene annullata e le sue istanze sono in terminazione. La richiesta rimane in questo stato finché tutte le istanze non vengono terminate.

`expired`

La richiesta del parco istanze spot è scaduta. Se la richiesta è stata creata con un set `TerminateInstancesWithExpiration`, un evento successivo `terminated` indica che le istanze sono terminate.

`modify_in_progress`

La richiesta del parco istanze spot è in fase di modifica. La richiesta rimane in questo stato finché la modifica non viene completamente elaborata.

`modify_succeeded`

La richiesta del parco istanze spot è stata modificata.

`submitted`

La richiesta del parco istanze spot è in fase di valutazione e Amazon EC2 si sta preparando ad avviare il numero previsto di istanze.

`progress`

La richiesta del parco istanze spot sta per essere evasa.

Modifica della richiesta del parco istanze spot EC2

Spot Fleet invia un `EC2 Spot Fleet Spot Instance Request Change` evento ad Amazon EventBridge quando una richiesta di istanza Spot nella flotta cambia stato.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "cd141ef0-14af-d670-a71d-fe46e9971bd2",
    "detail-type": "EC2 Spot Fleet Spot Instance Request Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:53:21Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-
a98d2133-941a-47dc-8b03-0f94c6852ad1"
    ],
    "detail": {
        "spot-instance-request-id": "sir-a2w9gc5h",
        "description": "SpotInstanceRequestId sir-a2w9gc5h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

I valori possibili per `sub-type` sono:

`active`

La richiesta è stata soddisfatta e ha un'istanza spot associata.

`cancelled`

Hai annullato la richiesta dell'istanza spot o la richiesta dell'istanza spot è scaduta.

`disabled`

Hai arrestato l'istanza spot.

`submitted`

La richiesta dell'istanza spot viene inviata.

Modifica dell'istanza del parco istanze spot di EC2

Spot Fleet invia un `EC2 Spot Fleet Instance Change` evento ad Amazon EventBridge quando un'istanza della flotta cambia stato.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "11591686-5bd7-bbaa-eb40-d46529c2710f",
    "detail-type": "EC2 Spot Fleet Instance Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T07:25:02Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-c8a764a4-bedc-4b62-
af9c-0095e6e3ba61"
    ],
    "detail": {
        "instance-id": "i-08b90df1e09c30c9b",
        "description": "{\"instanceType\":\"r4.2xlarge\",\"image\":
\"ami-032930428bf1abbff\",\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":
\"us-east-1a\"}",
        "sub-type": "launched"
    }
```

```
}
```

I valori possibili per `sub-type` sono:

`launched`

È stata lanciata una nuova istanza.

`terminated`

L'istanza è stata terminata.

`termination_notified`

Una notifica di terminazione dell'istanza è stata inviata quando un'istanza spot è stata terminata da Amazon EC2 durante la riduzione orizzontale, quando la capacità target del parco istanze è stata modificata, ad esempio, da una capacità target di 4 a una capacità target di 3.

Informazioni sul parco istanze spot di EC2

Spot Fleet invia un `EC2 Spot Fleet Information` evento ad Amazon EventBridge in caso di errore durante l'evasione. L'evento informativo non impedisce al parco istanze di tentare di raggiungere la sua capacità target.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "73a60f70-3409-a66c-635c-7f66c5f5b669",
    "detail-type": "EC2 Spot Fleet Information",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-08T20:56:12Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-2531ea06-
af18-4647-8757-7d69c94971b1"
    ],
    "detail": {
        "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot
 bid price is less than Spot market price $0.5291",
        "sub-type": "launchSpecUnusable"
    }
```

```
}
```

I valori possibili per `sub-type` sono:

`fleetProgressHalted`

Il prezzo in ogni specifica di avvio non è valido perché è inferiore al prezzo istanza spot (tutte le specifiche di avvio hanno prodotto eventi `launchSpecUnusable`). Una specifica di avvio potrebbe diventare valida se il prezzo Spot cambia.

`launchSpecTemporarilyBlacklisted`

La configurazione non è valida e vari tentativi di avvio delle istanze non sono riusciti. Per ulteriori informazioni, consulta la descrizione dell'evento.

`launchSpecUnusable`

Il prezzo in una specifica di avvio non è valido perché è inferiore al prezzo istanza spot o il prezzo istanza spot è inferiore al prezzo on demand.

`registerWithLoadBalancersFailed`

Tentativo di registrazione di istanze con bilanciamento del carico non riuscito. Per ulteriori informazioni, consulta la descrizione dell'evento.

Errore del parco istanze spot EC2

Spot Fleet invia un `EC2 Spot Fleet Error` evento ad Amazon EventBridge in caso di errore durante l'evasione dell'ordine. L'evento di errore impedisce al parco istanze di tentare di raggiungere la sua capacità target.

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "version": "0",
    "id": "10adc4e7-675c-643e-125c-5bfa1b1ba5d2",
    "detail-type": "EC2 Spot Fleet Error",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T06:56:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/
sfr-38725d30-25f1-4f30-83ce-2907c56dba17"
```

```
    ],
    "detail": {
        "description": "r4.2xlarge, ami-032930428bf1abbff, Linux/UNIX: The
 associatePublicIPAddress parameter can only be specified for the network interface
 with DeviceIndex 0. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

I valori possibili per `sub-type` sono:

`iamFleetRoleInvalid`

La serie di istanze spot non include le autorizzazioni necessarie per avviare o terminare un'istanza.

`allLaunchSpecsTemporarilyBlacklisted`

Nessuna delle configurazioni è valida e vari tentativi di avvio delle istanze non sono riusciti. Per ulteriori informazioni, consulta la descrizione dell'evento.

`spotInstanceCountLimitExceeded`

Hai raggiunto il limite del numero di istanze spot che puoi avviare.

`spotFleetRequestConfigurationInvalid`

La configurazione non è valida. Per ulteriori informazioni, consulta la descrizione dell'evento.

Tutorial per parco istanze EC2

Vi sono diversi modi per configurare un parco istanze EC2. La configurazione scelta dipende dal caso d'uso specifico.

I seguenti tutorial coprono alcuni dei possibili casi d'uso e forniscono le attività necessarie per implementarli.

Caso d'uso	Link al tutorial
Utilizza la ponderazione delle istanze per gestire la disponibilità e le prestazioni del parco istanze EC2.	Tutorial: Configura il parco istanze EC2 per usare la ponderazione dell'istanza

Caso d'uso	Link al tutorial
Con la ponderazione delle istanze, assegni un peso a ciascun tipo di istanza del parco istanze EC2 per rappresentarne la capacità di calcolo e le prestazioni reciproche. In base ai pesi, il parco istanze può utilizzare qualsiasi combinazione dei tipi di istanza specificati, purché sia in grado di soddisfare la capacità target desiderata.	
Usa la On-Demand capacità per garantire la disponibilità durante i periodi di punta, ma approfitta della capacità Spot aggiuntiva a un costo inferiore. Configura la tua flotta EC2 per utilizzare On-Demand le istanze come capacità principale per garantire la capacità disponibile durante i periodi di punta. Inoltre, alloca parte della capacità alle istanze spot per usufruire di prezzi scontati, tenendo presente che le istanze spot possono essere interrotte se Amazon EC2 ha di nuovo bisogno della capacità.	Tutorial: configura la flotta EC2 per utilizzare le On-Demand istanze come capacità principale

Caso d'uso	Link al tutorial
Utilizza Capacity Reservations per riservare la capacità di calcolo per le tue istanze. On-Demand Configura la tua flotta EC2 per utilizzare prima le prenotazioni `targeted` di capacità all'avvio On-Demand delle istanze. Se i tuoi requisiti di capacità sono rigorosi e stai eseguendo carichi di lavoro aziendali critici che richiedono un certo livello di garanzia della capacità a lungo o breve termine, ti consigliamo di creare una prenotazione della capacità per assicurarti di avere sempre accesso alla capacità di Amazon EC2 quando ne hai bisogno, per tutto il tempo necessario.	Tutorial: configura la flotta EC2 per avviare On-Demand istanze utilizzando prenotazioni di capacità mirate
Usa i blocchi di capacità per prenotare le istanze GPU più richieste per i tuoi carichi di lavoro ML. Configura il tuo parco istanze EC2 per avviare istanze in blocchi di capacità.	Tutorial: Configura il tuo parco istanze EC2 per avviare istanze in Blocchi di capacità
Utilizza Interruptible Capacity Reservations per riutilizzare temporaneamente la capacità inattiva in tutta l'organizzazione e risparmiare sui costi. AWS Configura la tua flotta EC2 per avviare le istanze nelle prenotazioni di capacità interrompibile, che rappresentano la capacità inutilizzata all'interno della tua organizzazione. AWS I proprietari della capacità possono recuperare la capacità in qualsiasi momento. Una volta recuperata, EC2 chiude le istanze con un preavviso di 2 minuti.	Tutorial: configura la tua flotta EC2 per avviare le istanze in prenotazioni di capacità interrompibile

Caso d'uso	Link al tutorial
Utilizza un singolo Capacity Reservation Resource Group per avviare le istanze in più tipi di Capacity Reservation. Configura la tua flotta EC2 per lanciare istanze su più tipi di prenotazione di capacità (prenotazioni di On-Demand capacità, blocchi di capacità per ML e prenotazioni di capacità interrompibili) utilizzando un unico gruppo di risorse per la prenotazione della capacità. Puoi dare priorità ai tipi di prenotazione della capacità in un ordine specifico e, facoltativamente, ricorrere alla On-Demand capacità quando la capacità riservata non è sufficiente per raggiungere l'obiettivo.	Tutorial: configura la tua flotta EC2 per avviare le istanze in più tipi di prenotazione della capacità utilizzando un gruppo di risorse per la prenotazione della capacità

Tutorial: Configura il parco istanze EC2 per usare la ponderazione dell'istanza

In questo tutorial viene utilizzata una società fittizia chiamata Example Corp per illustrare il processo di richiesta di un parco istanze EC2 con l'utilizzo della ponderazione dell'istanza.

Obiettivo

Example Corp, una società farmaceutica, vuole utilizzare la potenza di calcolo di Amazon EC2 per lo screening di composti chimici che potrebbero essere utilizzati per combattere il cancro.

Pianificazione

Prime analisi Example Corp Best Practice Spot. Poi, Example Corp stabilisce i requisiti seguenti per EC2 Fleet.

Tipi di istanza

Example Corp dispone di un'applicazione ad alta intensità di calcolo e di memoria che offre le migliori prestazioni con almeno 60 GB di memoria e otto CPU virtuali (vCPU). Il suo scopo è massimizzare

tali risorse per l'applicazione al prezzo più basso possibile. Example Corp stabilisce che uno dei seguenti tipi di istanza EC2 soddisfa le proprie esigenze:

Tipo di istanza	Memoria (GiB)	vCPU
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Capacità di destinazione in unità

Con la ponderazione delle istanze, la capacità target può essere uguale a un numero di istanze (impostazione predefinita) o a una combinazione di fattori come core (vCPU), memoria () e storage (GiBsGB). Considerando la base per la loro applicazione (60 GB di RAM e otto vCPU) come un'unità, Example Corp decide che 20 volte questa quantità soddisferebbe le proprie esigenze. Dunque, la società imposta la capacità target della propria richiesta del parco istanze EC2 a 20 unità.

Pesi dell'istanza

Dopo aver stabilito la capacità di destinazione, Example Corp calcola i pesi dell'istanza. Per calcolare il peso dell'istanza per ogni tipo di istanza, la società stabilisce le unità di ogni tipo di istanza necessarie al raggiungimento della capacità di destinazione come segue:

- r3.2xlarge (61,0 GB, 8 vCPU) = 1 unità da 20
- r3.4xlarge (122,0 GB, 16 vCPU) = 2 unità da 20
- r3.8xlarge (244,0 GB, 32 vCPU) = 4 unità da 20

Pertanto, Example Corp assegna pesi di istanza di 1, 2 e 4 alle rispettive configurazioni di avvio nella propria richiesta di EC2 Fleet.

Prezzo all'ora per unità

Example Corp utilizza il On-Demand prezzo per ora di istanza come punto di partenza per il prezzo. La società può anche utilizzare i prezzi Spot recenti o una combinazione dei due. Per calcolare il prezzo all'ora per unità, la società divide il prezzo iniziale all'ora per istanza per il peso. Ad esempio:

Tipo di istanza	On-Demand prezzo	Peso dell'istanza	Prezzo all'ora per unità
r3.2xLarge	0,7 $	1	0,7 $
r3.4xLarge	1,4 $	2	0,7 $
r3.8xLarge	$2,8	4	0,7 $

Example Corp può utilizzare un prezzo globale di 0,7 $ all'ora per unità ed essere competitiva per tutti e tre i tipi di istanza. Potrebbero anche utilizzare un prezzo globale di 0,7 USD per unità ora e un prezzo specifico di 0,9 USD per unità ora nella specifica di avvio `r3.8xlarge`.

Verificare le autorizzazioni

Prima di creare un parco istanze EC2, Example Corp verifica che abbia un ruolo IAM con le autorizzazioni necessarie. Per ulteriori informazioni, consulta Prerequisiti di parco istanze EC2.

Creazione di un modello di avvio

Successivamente, Example Corp crea un modello di avvio. L'ID del modello di avvio viene utilizzato nella fase seguente. Per ulteriori informazioni, consulta Creare un modello di avvio Amazon EC2.

Creazione del parco istanze EC2

Example Corp crea un file, `config.json`, con la configurazione seguente per il proprio parco istanze EC2. Nell'esempio seguente sostituire gli identificatori di risorsa con i propri identificatori di risorsa.

```
{
    "LaunchTemplateConfigs": [
        {
```

```
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r3.2xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "r3.4xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 2
                },
                {
                    "InstanceType": "r3.8xlarge",
                    "MaxPrice": "0.90",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 4
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Example Corp crea EC2 Fleet utilizzando il comando create-fleet seguente.

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.

adempimento

La strategia di allocazione stabilisce da quali pool di capacità spot provengono le istanze spot.

Con la strategia `lowest-price` (ovvero la strategia predefinita), le Istanze spot provengono dal pool con il prezzo per unità più basso al momento dell'elaborazione. Per fornire 20 unità di capacità, EC2

Fleet avvia 20 istanze `r3.2xlarge` (20 diviso 1), 10 istanze `r3.4xlarge` (20 diviso 2) o 5 istanze `r3.8xlarge` (20 diviso 4).

Se Example Corp utilizzasse la strategia `diversified`, le Istanze spot proverrebbero da tutti e tre i pool. Il parco istanze EC2 avvierebbe 6 istanze `r3.2xlarge` (per ottenere 6 unità), 3 istanze `r3.4xlarge` (per ottenere 6 unità) e 2 istanze `r3.8xlarge` (per ottenere 8 unità), per un totale di 20 unità.

Tutorial: configura la flotta EC2 per utilizzare le On-Demand istanze come capacità principale

Questo tutorial utilizza una società fittizia chiamata ABC Online per illustrare il processo di richiesta di una flotta EC2 con capacità principale e capacità On-Demand Spot, se disponibile.

Obiettivo

ABC Online, un'azienda di consegne a domicilio per ristoranti, punta ad assegnare la capacità Amazon EC2 in tutti i tipi di istanza EC2 e opzioni di acquisto per raggiungere le dimensioni, le prestazioni e i costi desiderati.

Pianificazione

ABC Online necessita di una capacità fissa per gestire i periodi di picco, ma vuole trarre vantaggio dalla capacità aggiuntiva a un prezzo inferiore. L'azienda stabilisce i requisiti seguenti per il parco istanze EC2:

- On-Demand Capacità delle istanze: ABC Online richiede 15 On-Demand istanze per garantire la capacità di gestire il traffico nei periodi di punta.
- Capacità istanza spot – Per migliorare le prestazioni, ma a un prezzo inferiore, ABC Online intende eseguire il provisioning di 5 istanze spot.

Verificare le autorizzazioni

Prima di creare un parco istanze EC2, ABC Online verifica che abbia un ruolo IAM con le autorizzazioni necessarie. Per ulteriori informazioni, consulta Prerequisiti di parco istanze EC2.

Creazione di un modello di avvio

Successivamente, ABC Online crea un modello di avvio. L'ID del modello di avvio viene utilizzato nella fase seguente. Per ulteriori informazioni, consulta Creare un modello di avvio Amazon EC2.

Creazione del Parco istanze EC2

ABC Online crea un file, `config.json`, con la configurazione seguente per il proprio parco istanze EC2. Nell'esempio seguente sostituire gli identificatori di risorsa con i propri identificatori di risorsa.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "2"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity":15,
        "DefaultTargetCapacityType": "spot"
    }
}
```

ABC Online crea EC2 Fleet utilizzando il comando create-fleet seguente.

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.

Adempimento

La strategia di allocazione determina che la On-Demand capacità sia sempre soddisfatta, mentre il saldo della capacità target viene soddisfatto come Spot se c'è capacità disponibile.

Tutorial: configura la flotta EC2 per avviare On-Demand istanze utilizzando prenotazioni di capacità mirate

Questo tutorial illustra tutti i passaggi da eseguire affinché il parco istanze EC2 inserisca le istanze nelle prenotazioni di capacità. On-Demand `targeted`

Imparerai come configurare un parco istanze per utilizzare innanzitutto le prenotazioni di `targeted` On-Demand capacità al momento del lancio delle istanze. On-Demand Imparerai anche a configurare

il parco veicoli in modo che, quando la capacità totale On-Demand target supera il numero di prenotazioni di capacità non utilizzate disponibili, il parco veicoli utilizzi la strategia di allocazione specificata per selezionare i pool di istanze in cui lanciare la capacità target rimanente.

Configurazione del parco istanze EC2

In questo tutorial, il parco istanze è configurato come indicato di seguito:

- Capacità target: 10 istanze On-Demand
- Numero totale di prenotazioni `targeted` di capacità inutilizzate: 6 (inferiori alla capacità On-Demand target di 10 On-Demand istanze prevista dalla flotta)
- Numero di prenotazioni della capacità per pool: 2 (`us-east-1a` e `us-east-1b`)
- Numero di prenotazioni della capacità per pool: 3
- On-Demand strategia di allocazione: `lowest-price` (quando il numero di prenotazioni di capacità inutilizzate è inferiore alla capacità On-Demand obiettivo, la flotta determina i pool in cui lanciare la On-Demand capacità residua in base alla On-Demand strategia di allocazione).

  Tenere presente che è anche possibile utilizzare la strategia di allocazione `prioritized` invece della strategia di allocazione `lowest-price`.

Per avviare On-Demand le istanze in targeted Capacity Reservations, devi eseguire una serie di passaggi, come segue:

- Fase 1: creazione di prenotazioni della capacità
- Fase 2: creazione di un gruppo di risorse di prenotazione della capacità
- Fase 3: aggiunta delle prenotazioni della capacità al gruppo di risorse di prenotazione della capacità
- (Facoltativo) Fase 4: visualizzazione delle prenotazioni delle capacità nel gruppo di risorse
- Fase 5: creazione di un modello di avvio che specifichi che la prenotazione della capacità è destinata a un gruppo di risorse specifico
- (Facoltativo) Fase 6: descrizione del modello di avvio
- Fase 7: creazione di un parco istanze EC2
- (Facoltativo) Fase 8: visualizzazione del numero di prenotazioni delle capacità non utilizzate rimanenti

Fase 1: creazione di prenotazioni della capacità

Utilizzare il comando create-capacity-reservation per creare le prenotazioni della capacità, tre per `us-east-1a` e altre tre per `us-east-1b`. Ad eccezione della zona di disponibilità, gli altri attributi delle prenotazioni della capacità sono identici.

3 prenotazioni della capacità in **`us-east-1a`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1a \
    --instance-type c5.xlarge \
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Esempio di ID prenotazione della capacità risultante

```
cr-1234567890abcdef1
```

3 prenotazioni della capacità in **`us-east-1b`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1b \
    --instance-type c5.xlarge \
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Esempio di ID prenotazione della capacità risultante

```
cr-54321abcdef567890
```

Fase 2: creazione di un gruppo di risorse di prenotazione della capacità

Utilizzare il servizio `resource-groups` e il comando create-group per creare un gruppo di risorse prenotazioni della capacità. In questo esempio, il gruppo di risorse è denominato `my-cr-group`. Per informazioni sul motivo per cui è necessario creare un gruppo di risorse, consulta Usa Capacity Reservations per riservare On-Demand capacità nella flotta EC2.

```
aws resource-groups create-group \
```

```
    --name my-cr-group \
    --configuration '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Fase 3: aggiunta delle prenotazioni della capacità al gruppo di risorse di prenotazione della capacità

Utilizzare il servizio `resource-groups` e il comando group-resources per aggiungere le prenotazioni della capacità create nella fase 1 al gruppo di risorse prenotazioni della capacità. Tieni presente che devi fare riferimento alle prenotazioni di On-Demand capacità tramite i relativi ARN.

```
aws resource-groups group-resources \
    --group my-cr-group \
    --resource-arns \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Output di esempio

```
{
   "Failed": [],
   "Succeeded": [
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
   ]
}
```

(Facoltativo) Fase 4: visualizzazione delle prenotazioni delle capacità nel gruppo di risorse

Utilizzare il servizio `resource-groups` e il comando list-group-resources per descrivere facoltativamente il gruppo di risorse per visualizzarne le prenotazioni della capacità.

```
aws resource-groups list-group-resources --group my-cr-group
```

Output di esempio

```
{
```

```
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
    ]
}
```

Fase 5: creazione di un modello di avvio che specifichi che la prenotazione della capacità è destinata a un gruppo di risorse specifico

Utilizzare il comando create-launch-template per creare un modello di avvio in cui specificare le prenotazioni della capacità da utilizzare. In questo esempio, il parco istanze utilizza le prenotazioni della capacità `targeted` che sono state aggiunte a un gruppo di risorse. Pertanto, i dati del modello di avvio specificano che la prenotazione della capacità è destinata a un gruppo di risorse specifico. In questo esempio, il modello di avvio è denominato `my-launch-template`.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --launch-template-data \
        '{"ImageId": "ami-0123456789example",
          "CapacityReservationSpecification":
            {"CapacityReservationTarget":
                { "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-
east-1:123456789012:group/my-cr-group" }
            }
        }'
```

(Facoltativo) Fase 6: descrizione del modello di avvio

Utilizzare il comando describe-launch-template-versions per descrivere facoltativamente il modello di avvio per visualizzarne la configurazione.

```
aws ec2 describe-launch-template-versions --launch-template-name my-launch-template
```

Output di esempio

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-01234567890example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2021-01-19T20:50:19.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Admin",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0947d2ba12ee1ff75",
                "CapacityReservationSpecification": {
                    "CapacityReservationTarget": {
                        "CapacityReservationResourceGroupArn": "arn:aws:resource-
groups:us-east-1:123456789012:group/my-cr-group"
                    }
                }
            }
        }
    ]
}
```

Fase 7: creazione di un parco istanze EC2

Creare un parco istanze EC2 che specifichi le informazioni di configurazione per le istanze che avvierà. La seguente configurazione del parco istanze EC2 mostra solo le configurazioni pertinenti per questo esempio. Il modello di avvio `my-launch-template` è il modello di avvio creato al passaggio 5. Esistono due pool di istanze, entrambi con lo stesso tipo di istanza (`c5.xlarge`) ma con diverse zone di disponibilità (`us-east-1a` e `us-east-1b`). Il prezzo dei pool di istanze è lo stesso perché la determinazione dei prezzi è definita per la Regione, non per la zona di disponibilità. La capacità obiettivo totale è 10 e il tipo di capacità obiettivo predefinito è `on-demand`. La strategia di On-Demand allocazione è. `lowest-price` La strategia di utilizzo per la prenotazione della capacità è `use-capacity-reservations-first`.

> **Note**
>
> Il tipo di parco istanze deve essere `instant`. Altri tipi di parchi istanze non supportano `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Dopo aver creato il parco istanze `instant` utilizzando la configurazione precedente, vengono avviate le seguenti 10 istanze per soddisfare la capacità obiettivo:

- Le prenotazioni di capacità vengono utilizzate innanzitutto per avviare 6 On-Demand istanze come segue:
  - 3 On-Demand istanze vengono lanciate nelle 3 prenotazioni di `c5.xlarge` `targeted` capacità in `us-east-1a`
  - 3 On-Demand istanze vengono lanciate nelle 3 prenotazioni di `c5.xlarge` `targeted` capacità in `us-east-1b`

- Per raggiungere la capacità prevista, 4 On-Demand istanze aggiuntive vengono avviate alla On-Demand capacità normale in base alla strategia di On-Demand allocazione, illustrata `lowest-price` in questo esempio. Tuttavia, poiché i pool hanno lo stesso prezzo (poiché il prezzo è per regione e non per zona di disponibilità), la flotta lancia le 4 On-Demand istanze rimanenti in uno dei pool.

(Facoltativo) Fase 8: visualizzazione del numero di prenotazioni delle capacità non utilizzate rimanenti

Dopo l'avvio del parco istanze, puoi facoltativamente eseguire describe-capacity-reservations per vedere quante prenotazioni della capacità sono rimaste inutilizzate. In questo esempio, dovresti vedere la seguente risposta, che mostra che tutti i Prenotazioni di capacità del pool sono stati utilizzati.

```
{ "CapacityReservationId":  "cr-111",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}

 { "CapacityReservationId":  "cr-222",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}
```

Tutorial: Configura il tuo parco istanze EC2 per avviare istanze in Blocchi di capacità

Questo tutorial illustra tutti i passaggi da eseguire in modo che il parco istanze EC2 avvii le istanze in Blocchi di capacità.

Nella maggior parte dei casi, la capacità di destinazione della richiesta del parco istanze EC2 deve essere inferiore o uguale alla capacità disponibile della prenotazione del blocco di capacità che hai scelto come destinazione. Le richieste di capacità di destinazione che superano i limiti della prenotazione del blocco di capacità non verranno soddisfatte. Se la richiesta di capacità di destinazione supera i limiti della prenotazione del blocco di capacità, riceverai una `Insufficient Capacity Exception` per la capacità che supera i limiti della prenotazione del blocco di capacità.

> **Note**
>
> Per i blocchi di capacità, EC2 Fleet non ricorrerà al lancio di On-Demand istanze per il resto della capacità target desiderata.

Se il parco istanze EC2 non è in grado di soddisfare la capacità di destinazione richiesta in una prenotazione del blocco di capacità disponibile, il parco istanze EC2 soddisferà tutta la capacità possibile e restituirà le istanze che è stato in grado di avviare. È possibile ripetere nuovamente la chiamata al parco istanze EC2 fino al provisioning di tutte le istanze.

Dopo aver configurato la richiesta del parco istanze EC2, è necessario attendere la data di inizio della prenotazione del blocco di capacità. Se richiedi al parco istanze EC2 di avviare un blocco di capacità che non è ancora stato avviato, riceverai un `Insufficient Capacity Error`.

Dopo che la prenotazione del blocco di capacità diventa attiva, puoi effettuare chiamate all'API del parco istanze EC2 ed eseguire il provisioning delle istanze nel tuo blocco di capacità in base ai parametri selezionati. Le istanze in esecuzione nel blocco di capacità continuano a funzionare finché non le interrompi manualmente o le termini, oppure finché Amazon EC2 non termina le istanze al termine della prenotazione del blocco di capacità.

Per ulteriori informazioni sui blocchi di capacità, consulta Blocchi di capacità per ML.

Considerazioni

- Sono supportate solo le richieste di di parco istanze EC2 di tipo `instant` per l'avvio di istanze in blocchi di capacità. Per ulteriori informazioni, consulta Configurare un parco istanze EC2 di tipo instant.
- Non sono supportati più blocchi di capacità nella stessa richiesta di parco istanze EC2.
- L'utilizzo di `OnDemandTargetCapacity` o `SpotTargetCapacity` contemporaneamente all'impostazione di `capacity-block` come `DefaultTargetCapacity` non è supportato.
- Se `DefaultTargetCapacityType` è impostato su `capacity-block`, non puoi specificare `OnDemandOptions::CapacityReservationOptions`. Si verificherà un'eccezione.

Per configurare un parco istanze EC2 per avviare istanze in Blocchi di capacità

1. Creazione di un modello di avvio.

Nel modello di avvio, eseguire queste operazioni:

- Per `InstanceMarketOptionsRequest`, imposta `MarketType` su `capacity-block`.
- Per definire come target la prenotazione del blocco di capacità, per `CapacityReservationID`, specifica l'ID di prenotazione del blocco di capacità.

Annota il nome e la versione del modello di avvio. Userai queste informazioni nella fase successiva.

Per ulteriori informazioni sulla creazione di un modello di lancio, consulta Creare un modello di avvio Amazon EC2.

2. Configura il parco istanze EC2.

Crea un file, `config.json`, con la seguente configurazione per il parco istanze EC2. Nell'esempio seguente sostituire gli identificatori di risorsa con i propri identificatori di risorsa.

Per ulteriori informazioni sulla configurazione di un parco istanze EC2, consulta Creazione di un parco istanze EC2.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "CBR-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "p5.48xlarge",
                    "AvailabilityZone": "us-east-1a"
                },
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "capacity-block"
    },
    "Type": "instant"
```

```
}
```

3. Avvia il parco istanze.

   Utilizza il comando create-fleet.

   ```
   aws ec2 create-fleet --cli-input-json file://config.json
   ```

   Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.

Tutorial: configura la tua flotta EC2 per avviare le istanze in prenotazioni di capacità interrompibile

Questo tutorial illustra i passaggi da eseguire affinché la tua flotta EC2 avvii le istanze nelle prenotazioni di capacità interrompibile.

Le prenotazioni di capacità interrompibile rappresentano la capacità inutilizzata prestata dai proprietari delle prenotazioni di capacità all'interno della tua organizzazione. On-Demand AWS Queste prenotazioni sono adatte per carichi di lavoro interrompibili perché il proprietario della capacità può recuperare la capacità in qualsiasi momento con un preavviso di interruzione di 2 minuti, dopodiché EC2 chiude le istanze. Per ulteriori informazioni sulle prenotazioni di capacità interrompibile, vedere. Prenotazioni di capacità interrompibile

La capacità target della richiesta della flotta EC2 deve essere inferiore o uguale alla capacità disponibile della riserva di capacità interrompibile a cui si sta mirando. Se la richiesta di capacità target supera la capacità disponibile della tua prenotazione di capacità interrompibile, EC2 Fleet avvia quante più istanze possibile e riporta le istanze avviate nella risposta API.

Le istanze in esecuzione in una Interruptible Capacity Reservation continuano a funzionare finché non vengono interrotte o terminate manualmente o finché il proprietario della capacità non recupera la capacità. Quando il proprietario della capacità recupera la capacità, Amazon EC2 invia una EventBridge notifica Amazon 2 minuti prima di terminare le istanze.

Considerazioni

- Sono supportate solo le richieste di tipo EC2 Fleet per l'avvio delle istanze in `instant` Interruptible Capacity Reservations.
- L'utilizzo `OnDemandTargetCapacity` o `SpotTargetCapacity` durante l'impostazione `reserved-capacity` come «non è supportato. `DefaultTargetCapacityType`

- Quando si specificano più modelli di avvio, ciascuno destinato a una prenotazione di capacità interrompibile diversa, EC2 Fleet esegue il provisioning delle istanze per tutte le prenotazioni corrispondenti.
- Per le prenotazioni di capacità interrompibile, EC2 Fleet non ricorre al lancio di On-Demand istanze o istanze Spot per il resto della capacità target desiderata.

Verificare le autorizzazioni

Prima di creare una flotta EC2, verifica di disporre di un ruolo IAM con le autorizzazioni richieste. Per ulteriori informazioni, consulta Prerequisiti di parco istanze EC2.

Per avviare le istanze in una Interruptible Capacity Reservation, devi eseguire i seguenti passaggi:

Fase 1: creazione di un modello di avvio

Utilizzate il comando create-launch-template per creare un modello di avvio che specifichi l'Interruptible Capacity Reservation a cui destinare. Nel modello di avvio, impostate `interruptible-capacity-reservation` e specificate il valore della vostra prenotazione `MarketType` di capacità interrompibile. `CapacityReservationId`

Esempio di configurazione del modello di avvio:

```
{
    "LaunchTemplateName": "interruptible-cr-launch-template",
    "LaunchTemplateData": {
        "InstanceType": "m5.large",
        "ImageId": "ami-0abcdef1234567890",
        "CapacityReservationSpecification": {
            "CapacityReservationTarget": {
                "CapacityReservationId": "cr-0123456789abcdef0"
            }
        },
        "InstanceMarketOptions": {
            "MarketType": "interruptible-capacity-reservation"
        }
    }
}
```

Output di esempio

```
{
```

```
    "LaunchTemplate": {
        "LaunchTemplateId": "lt-0123456789example",
        "LaunchTemplateName": "interruptible-cr-launch-template",
        "CreateTime": "2026-03-12T10:00:00.000Z",
        "CreatedBy": "arn:aws:iam::123456789012:user/Admin",
        "DefaultVersionNumber": 1,
        "LatestVersionNumber": 1
    }
}
```

Per ulteriori informazioni, consulta Creare un modello di avvio Amazon EC2.

Fase 2: Configurazione della flotta EC2

Crea un file di configurazione per la flotta EC2 che specifichi il modello di lancio e la capacità target. La seguente configurazione utilizza il modello `interruptible-cr-launch-template` di lancio creato nel passaggio 1.

È necessario specificare `ReservedCapacityOptions` con `ReservationType` set to `interruptible-capacity-reservation` quando si utilizza `reserved-capacity` come`DefaultTargetCapacityType`.

Crea un file denominato `config.json` con i seguenti contenuti:

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "interruptible-cr-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "m5.large",
                    "AvailabilityZone": "us-east-1a"
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "reserved-capacity"
```

```
    },
    "ReservedCapacityOptions": {
        "ReservationType": ["interruptible-capacity-reservation"]
    },
    "Type": "instant"
}
```

Parametri di configurazione chiave:

Parametro	Description
`DefaultTargetCapacityType`	Impostato `reserved-capacity` per indicare che le istanze devono essere avviate con capacità riservata.
`ReservedCapacityOptions`	Specifica il tipo di capacità riservata. Per le prenotazioni di capacità interrompibile, impostare su. `ReservationType` `["interruptible-capacity-reservation"]`
`Type`	Deve essere impostato su `instant`. Per le prenotazioni di capacità interrompibile sono supportate solo le flotte istantanee.

Fase 3: Avvia la flotta e visualizza i risultati

Usa il comando create-fleet per creare la flotta:

```
aws ec2 create-fleet \
    --cli-input-json file://config.json
```

Dopo aver creato la `instant` flotta utilizzando la configurazione precedente, EC2 Fleet avvia 10 istanze nella Interruptible Capacity Reservation per raggiungere la capacità target.

> **Note**
>
> Se la flotta non è in grado di soddisfare la piena capacità prevista, la risposta include le istanze avviate e gli eventuali errori dovuti alla capacità non soddisfatta.

Output di esempio

```
{
    "FleetId": "fleet-12345678-1234-1234-1234-123456789012",
    "Instances": [
        {
            "LaunchTemplateAndOverrides": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-0123456789example",
                    "Version": "1"
                },
                "Overrides": {
                    "InstanceType": "m5.large",
                    "AvailabilityZone": "us-east-1a"
                }
            },
            "Lifecycle": "interruptible-capacity-reservation",
            "InstanceIds": [
                "i-0123456789example1",
                "i-0123456789example2",
                "i-0123456789example3",
                "i-0123456789example4",
                "i-0123456789example5",
                "i-0123456789example6",
                "i-0123456789example7",
                "i-0123456789example8",
                "i-0123456789example9",
                "i-0123456789example0"
            ],
            "InstanceType": "m5.large",
            "Platform": "Linux/UNIX"
        }
    ],
    "Errors": []
}
```


Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.

Eliminazione

Per evitare di incorrere in addebiti, interrompi le istanze quando non sono più necessarie. Tieni presente che EC2 termina automaticamente anche le istanze avviate in una riserva di capacità interrompibile quando il proprietario della capacità recupera la capacità.

Risorse correlate

- Prenotazioni di capacità interrompibile
- Riserva la capacità di calcolo con EC2 On-Demand Capacity Reservations
- Lavorare con un parco istanze EC2
- Creazione di un parco istanze EC2
- Archivia i parametri di avvio dell'istanza nei modelli di avvio di Amazon EC2

Tutorial: configura la tua flotta EC2 per avviare le istanze in più tipi di prenotazione della capacità utilizzando un gruppo di risorse per la prenotazione della capacità

Questo tutorial illustra i passaggi per configurare una flotta EC2 che avvia istanze su più tipi di prenotazione della capacità (ODCR), blocchi di On-Demand capacità per ML e prenotazioni di capacità interrompibili, utilizzando un unico gruppo di risorse per la prenotazione della capacità.

Scoprirai come creare un gruppo di risorse per la prenotazione della capacità che contenga diversi tipi di prenotazione della capacità, configurare la tua flotta EC2 per dare priorità ai tipi di prenotazione della capacità in un ordine specifico e, facoltativamente, ricorrere alla On-Demand capacità quando la capacità riservata è insufficiente per raggiungere il tuo obiettivo.

Considerazioni

- Solo le richieste di tipo EC2 Fleet sono supportate durante l'utilizzo`instant`. `ReservedCapacityOptions`
- È necessario specificare esplicitamente quali tipi di prenotazione di capacità scegliere come target nell'`ReservationTypes`elenco. EC2 Fleet avvia le istanze solo nei tipi di prenotazione della capacità specificati.
- `ReservedCapacityOptions`si esclude a vicenda con. `OnDemandOptions.CapacityReservationOptions` Non puoi utilizzarli entrambi nella stessa richiesta EC2 Fleet.

Questo tutorial presuppone che tu abbia già le seguenti prenotazioni di capacità nel tuo account:

- Un ODCR (`cr-1234567890abcdef1`) per `p5.48xlarge` `us-east-1a`

- Un ODCR (`cr-abcdef1234567890a`) per in `p4d.48xlarge` `us-east-1b`
- Un Capacity Block (`cr-0123456789abcdef0`) per in `p5.48xlarge` `us-east-1a`
- Una Capacity Reservation (`cr-9876543210fedcba9`) interrompibile da `p5.48xlarge` utilizzare in`us-east-1a`, condivisa con te da un altro account della tua organizzazione

Verificare le autorizzazioni

Prima di creare una flotta EC2, verifica di disporre di un ruolo IAM con le autorizzazioni richieste. Per ulteriori informazioni, consulta Prerequisiti di parco istanze EC2.

Fase 1: Creare un gruppo di risorse per la prenotazione delle capacità

Crea un gruppo di risorse per la prenotazione della capacità per contenere le prenotazioni di capacità previste dalla tua flotta EC2. Configura il gruppo in modo che accetti le prenotazioni di capacità di qualsiasi tipo di istanza e il tipo di prenotazione della capacità, il che consente al gruppo di contenere una combinazione di tipi di prenotazione di capacità. Per istruzioni dettagliate, consulta Gruppi di prenotazione di capacità.

> **Note**
>
> Quando si crea il gruppo, non specificare i `reservation-type` parametri `instance-type` o nella configurazione. `AWS::EC2::CapacityReservationPool` L'omissione di questi parametri consente al gruppo di accettare prenotazioni di capacità di qualsiasi tipo di istanza e tipo di prenotazione di capacità.

Passaggio 2: aggiungere le prenotazioni di capacità al gruppo

Aggiungi le tue prenotazioni di capacità al gruppo di risorse per le prenotazioni di capacità. È possibile aggiungere qualsiasi combinazione di ODCR, blocchi di capacità per ML, prenotazioni di capacità interrompibili e blocchi di capacità. UltraServer Per questo tutorial, aggiungi le quattro prenotazioni di capacità elencate all'inizio di questo tutorial. Per istruzioni dettagliate, consulta Gruppi di prenotazione della capacità.

Fase 3: creazione di un modello di avvio

Usa il comando create-launch-template per creare un modello di avvio destinato al Capacity Reservation Resource Group. Quando si utilizza `ReservedCapacityOptions` nella configurazione

della flotta EC2, non è necessario impostare un valore `MarketType` nel modello di avvio: EC2 Fleet lo imposta automaticamente per ogni tipo di prenotazione di capacità.

```
aws ec2 create-launch-template \
    --launch-template-name my-cr-resource-group-template \
    --launch-template-data \
        '{"ImageId": "ami-0123456789example",
          "CapacityReservationSpecification":
            {"CapacityReservationTarget":
                {"CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-
east-1:123456789012:group/my-cr-resource-group"}
            }
        }'
```

Fase 4: Creare una flotta EC2

Crea una flotta EC2 destinata a più tipi di prenotazione della capacità nel tuo gruppo di risorse per la prenotazione della capacità. La configurazione chiave è`ReservedCapacityOptions`, che specifica quanto segue:

- `ReservationTypes`— Un elenco ordinato di tipi di prenotazione di capacità da scegliere come target. EC2 Fleet utilizza i tipi in questo ordine. I valori validi sono `on-demand-capacity-reservation`, `capacity-block` e `interruptible-capacity-reservation`.
- `AllocationStrategy`— Come viene assegnata la priorità ai tipi di istanza all'interno di ciascun tipo di prenotazione di capacità. Imposta in modo che `prioritized` segua l'ordine di sovrascrittura del tipo di istanza.
- `ReservedCapacityFallbackOptions`— Impostato `MarketTypes` per `["on-demand"]` avviare le On-Demand istanze quando la capacità riservata è insufficiente. Se non specifichi le opzioni di riserva, EC2 Fleet non ricorre a nessun altro tipo di mercato una volta esauriti i tipi di prenotazione di capacità specificati.

Crea un archivio denominato `config.json` con i seguenti contenuti. Nell'esempio seguente sostituire gli identificatori di risorsa con i propri identificatori di risorsa.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-cr-resource-group-template",
```

```
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "p5.48xlarge",
                    "AvailabilityZone": "us-east-1a",
                    "Priority": 1
                },
                {
                    "InstanceType": "p4d.48xlarge",
                    "AvailabilityZone": "us-east-1b",
                    "Priority": 2
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 100,
        "DefaultTargetCapacityType": "reserved-capacity"
    },
    "ReservedCapacityOptions": {
        "ReservationTypes": ["on-demand-capacity-reservation", "capacity-block",
 "interruptible-capacity-reservation"],
        "ReservedCapacityFallbackOptions": {
            "MarketTypes": ["on-demand"]
        },
        "AllocationStrategy": "prioritized"
    },
    "Type": "instant"
}
```

Usa il comando create-fleet per lanciare la flotta:

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Per ulteriori informazioni, consulta Creazione di un parco istanze EC2.

In che modo EC2 Fleet risolve le prenotazioni di capacità

In base alla configurazione precedente, EC2 Fleet tenta di avviare le istanze nel seguente ordine:

1. ODCR: prima `p5.48xlarge` le prenotazioni (il tipo di istanza con la priorità più alta) e poi le prenotazioni. `p4d.48xlarge` All'interno di ogni tipo di istanza, se esistono più ODCR, ne viene selezionato uno a caso.
2. Blocchi di capacità: se non rimane capacità disponibile in tutti gli ODCR, EC2 Fleet si rivolge ai blocchi di capacità. `p5.48xlarge`prima le prenotazioni e poi `p4d.48xlarge` selezionate a caso all'interno di ogni tipo di istanza.
3. Prenotazioni di capacità interrompibile: se non rimane capacità disponibile in tutti i blocchi di capacità, EC2 Fleet punta alle prenotazioni di capacità interrompibili. `p5.48xlarge`prima le prenotazioni e poi`p4d.48xlarge`, selezionate a caso all'interno di ciascun tipo di istanza.
4. On-Demand fallback: se la capacità riservata non è sufficiente per raggiungere l'obiettivo di 100 istanze, la capacità rimanente viene avviata come On-Demand istanze. EC2 Fleet avvia queste On-Demand istanze in base alla strategia di allocazione specificata in. `OnDemandOptions`

> **Note**
>
> EC2 Fleet risolve prima il tipo di prenotazione della capacità e poi il tipo di istanza all'interno di ciascun tipo di prenotazione della capacità. Ogni tipo di prenotazione della capacità è completamente esaurito prima che EC2 Fleet passi al tipo successivo nell'elenco ordinato.

(Facoltativo) Fase 5: verifica delle proprietà dell'istanza

Utilizzate il comando describe-instances per verificare quale tipo di prenotazione della capacità è stato utilizzato da ciascuna istanza. Le istanze lanciate dal parco macchine mostrano le seguenti proprietà.

Proprietà	On-Demand Valore della prenotazione della capacità	Valore del blocco di capacità	Valore di prenotazione della capacità interrompibile	On-Demand valore
`instance-lifecycle`	`null`	`capacity-block`	`interruptible-capacity-reservation`	`null`

Proprietà	On-Demand Valore della prenotazione della capacità	Valore del blocco di capacità	Valore di prenotazione della capacità interrompibile	On-Demand valore
`capacity-reservation-id`	ID di prenotazione della capacità consumato	ID di prenotazione della capacità consumato	ID di prenotazione della capacità consumato	Non presente
`capacity-reservation-specification`	ARN del gruppo	Gruppo ARN	Gruppo ARN	Non presente

È possibile filtrare le istanze per Capacity Reservation Resource Group utilizzando il seguente comando:

```
aws ec2 describe-instances \
    --filters "Name=capacity-reservation-specification.capacity-reservation-target.capacity-reservation-resource-group-arn,Values=arn:aws:resource-groups:us-east-1:123456789012:group/my-cr-resource-group"
```

Eliminazione

Per evitare di incorrere in addebiti, chiudi le istanze quando non sono più necessarie. Tieni presente che le istanze avviate in Capacity Block vengono terminate automaticamente al termine della prenotazione del Capacity Block. Le istanze avviate nelle prenotazioni di capacità interrompibili vengono automaticamente terminate se il proprietario della capacità recupera la capacità.

Risorse correlate

- Gruppi Prenotazione della capacità
- Blocchi di capacità per ML
- Prenotazioni di capacità interrompibile
- Riserva la capacità di calcolo con EC2 On-Demand Capacity Reservations

- Lavorare con un parco istanze EC2
- Creazione di un parco istanze EC2
- Archivia i parametri di avvio dell'istanza nei modelli di avvio di Amazon EC2

Esempi di configurazioni di CLI per parco istanze EC2

Puoi definire la configurazione dell'EC2 Fleet in un file JSON, poi fare riferimento a tale file con il comando create-fleet per creare il tuo parco istanze, come indicato di seguito:

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

I seguenti esempi illustrano le configurazioni di avvio per vari casi d'uso del parco istanze EC2. Per ulteriori informazioni sui parametri di configurazione, consulta create-fleet.

Esempi

- Esempio 1: Avviare Istanze spot come opzione di acquisto predefinita
- Esempio 2: Launch On-Demand Instances come opzione di acquisto predefinita
- Esempio 3: Launch On-Demand Instances come capacità principale
- Esempio 4: avvio di On-Demand istanze utilizzando più prenotazioni di capacità
- Esempio 5: On-Demand istanze di avvio che utilizzano le prenotazioni di capacità quando la capacità totale di destinazione supera il numero di prenotazioni di capacità non utilizzate
- Esempio 6: avvio di On-Demand istanze utilizzando prenotazioni di capacità mirate
- Esempio 7: Configurare il ribilanciamento della capacità per avviare la sostituzione delle istanze spot
- Esempio 8: Avviare le istanze spot in un parco istanze ottimizzato per la capacità
- Esempio 9: Avviare le istanze spot in un parco istanze ottimizzato per la capacità con priorità
- Esempio 10: avvio di istanze spot in un parco istanze ottimizzato per prezzo e capacità
- Esempio 11: configurazione della selezione del tipo di istanza basata su attributi
- Esempio 12: avvia le istanze in più tipi di prenotazione di capacità utilizzando un gruppo di risorse per la prenotazione di capacità

Per altri esempi di CLI per parchi istanze di tipo `instant`, consulta Configurare un parco istanze EC2 di tipo instant.

Esempio 1: Avviare Istanze spot come opzione di acquisto predefinita

L'esempio seguente indica i parametri minimi necessari in un parco istanze EC2: un modello di lancio, una capacità di destinazione e un'opzione d'acquisto predefinita. Il modello di avvio viene identificato dall'ID e dal numero di versione del modello di avvio. La capacità target per il parco istanze è di 2 istanze e l'opzione d'acquisto predefinita è `spot`; ne consegue che il parco istanze avvia 2 Istanze spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Esempio 2: Launch On-Demand Instances come opzione di acquisto predefinita

L'esempio seguente indica i parametri minimi necessari in un Parco istanze EC2: un modello di avvio, una capacità di destinazione e un'opzione d'acquisto predefinita. Il modello di avvio viene identificato dall'ID e dal numero di versione del modello di avvio. La capacità target per il parco istanze è di 2 istanze e l'opzione di acquisto predefinita è`on-demand`, il che comporta il lancio di 2 istanze da parte del parco istanze. On-Demand

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
```

```
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "on-demand"
    }
}
```

Esempio 3: Launch On-Demand Instances come capacità principale

L'esempio seguente specifica la capacità target totale di 2 istanze per il parco istanze e una capacità target di 1 istanza. On-Demand L'opzione di acquisto predefinita è `spot`. Il parco istanze avvia 1 On-Demand istanza come specificato, ma deve lanciarne un'altra per soddisfare la capacità totale prevista. L'opzione di acquisto per la differenza viene calcolata come `TotalTargetCapacity` – `OnDemandTargetCapacity` = `DefaultTargetCapacityType`, ne consegue che il parco istanze avvia 1 istanza spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Esempio 4: avvio di On-Demand istanze utilizzando più prenotazioni di capacità

È possibile configurare un parco veicoli in modo da utilizzare prima le prenotazioni di On-Demand capacità all'avvio On-Demand delle istanze impostando la strategia di utilizzo per le prenotazioni

di capacità su. `use-capacity-reservations-first` In questo esempio viene illustrato come il parco istanze seleziona la prenotazione della capacità da utilizzare quando sono presenti più prenotazioni della capacità di quelle necessarie per soddisfare la capacità obiettivo.

In questo esempio, la configurazione del parco istanze è la seguente:

- Capacità target: 12 istanze On-Demand
- Numero totale di prenotazioni di capacità inutilizzate: 15 (più della capacità prevista per la flotta di 12 istanze) On-Demand
- Numero di prenotazioni della capacità per pool: 3 (`m5.large`, `m4.xlarge` e `m4.2xlarge`)
- Numero di prenotazioni della capacità per pool: 5
- On-Demand strategia di allocazione: `lowest-price` (quando sono presenti più prenotazioni di capacità inutilizzate in più pool di istanze, la flotta determina i pool in cui avviare le On-Demand istanze in base alla strategia di allocazione). On-Demand

  Tenere presente che è anche possibile utilizzare la strategia di allocazione `prioritized` invece della strategia di allocazione `lowest-price`.

Prenotazioni di capacità

L'account presenta le seguenti 15 prenotazioni di capacità inutilizzati in 3 diversi pool. Il numero di Prenotazioni di capacità in ogni pool è indicato da `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
```

```
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Configurazione del parco istanze

La seguente configurazione del parco istanze mostra solo le configurazioni pertinenti per questo esempio. La capacità di destinazione totale è 12 e il tipo di capacità di destinazione predefinito è `on-demand`. La On-Demand strategia di allocazione è. `lowest-price` La strategia di utilizzo per la prenotazione della capacità è `use-capacity-reservations-first`.

In questo esempio, il prezzo dell' On-Demand istanza è:

- `m5.large` – 0,096 USD all'ora
- `m4.xlarge` – 0,20 USD all'ora
- `m4.2xlarge` – 0,40 USD all'ora

> **Note**
>
> Il tipo di parco istanze deve essere di tipo `instant`. Altri tipi di parchi istanze non supportano `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-abc1234567example",
                "Version": "1"
            },
            "Overrides": [
```

```
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant"
}
```

Dopo aver creato il parco istanze `instant` utilizzando la configurazione precedente, vengono avviate le seguenti 12 istanze per soddisfare la capacità di destinazione:

- 5 `m5.large` On-Demand Instances in `us-east-1a` — `m5.large` in `us-east-1a` è il prezzo più basso e sono disponibili 5 prenotazioni di capacità non utilizzate `m5.large`
- 5 `m4.xlarge` On-Demand istanze in us-east-1a — `m4.xlarge` in `us-east-1a` è il secondo prezzo più basso e sono disponibili 5 prenotazioni di capacità non utilizzate `m4.xlarge`
- 2 `m4.2xlarge` On-Demand esempi in us-east-1a — `m4.2xlarge` in `us-east-1a` è il terzo prezzo più basso e sono disponibili 5 riserve di capacità inutilizzate, di cui solo 2 sono necessarie per raggiungere la `m4.2xlarge` capacità prevista

Dopo l'avvio del parco istanze, puoi eseguire describe-capacity-reservations per vedere quante prenotazioni di capacità sono rimaste inutilizzate. In questo esempio, dovresti vedere la seguente risposta, che mostra che sono state utilizzate tutte le prenotazioni della capacità `m5.large` e `m4.xlarge`, con 3 prenotazioni della capacità `m4.2xlarge` rimaste inutilizzate.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 3
}
```

Esempio 5: On-Demand istanze di avvio che utilizzano le prenotazioni di capacità quando la capacità totale di destinazione supera il numero di prenotazioni di capacità non utilizzate

È possibile configurare un parco veicoli in modo da utilizzare innanzitutto le prenotazioni di On-Demand capacità all'avvio On-Demand delle istanze impostando la strategia di utilizzo per le prenotazioni di capacità su. `use-capacity-reservations-first` Questo esempio dimostra come il parco veicoli seleziona i pool di istanze in cui avviare On-Demand le istanze quando la capacità totale di destinazione supera il numero di prenotazioni di capacità inutilizzate disponibili.

In questo esempio, la configurazione del parco istanze è la seguente:

- Capacità target: 16 istanze On-Demand
- Totale prenotazioni di capacità inutilizzate: 15 (inferiori alla capacità obiettivo della flotta di 16 On-Demand istanze)
- Numero di prenotazioni della capacità per pool: 3 (`m5.large`, `m4.xlarge` e `m4.2xlarge`)

- Numero di prenotazioni della capacità per pool: 5
- On-Demand strategia di allocazione: `lowest-price` (quando il numero di prenotazioni di capacità inutilizzate è inferiore alla capacità On-Demand obiettivo, la flotta determina i pool in cui lanciare la On-Demand capacità residua in base alla On-Demand strategia di allocazione).

  Tenere presente che è anche possibile utilizzare la strategia di allocazione `prioritized` invece della strategia di allocazione `lowest-price`.

Prenotazioni di capacità

L'account presenta le seguenti 15 prenotazioni di capacità inutilizzati in 3 diversi pool. Il numero di Prenotazioni di capacità in ogni pool è indicato da `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
```

```
}
```

Configurazione del parco istanze

La seguente configurazione del parco istanze mostra solo le configurazioni pertinenti per questo esempio. La capacità di destinazione totale è 16 e il tipo di capacità di destinazione predefinito è `on-demand`. La strategia di On-Demand allocazione è. `lowest-price` La strategia di utilizzo per la prenotazione della capacità è `use-capacity-reservations-first`.

In questo esempio, il prezzo dell' On-Demand istanza è:

- m5.large – $0,096 all'ora
- m4.xlarge – $0,20 all'ora
- m4.2xlarge – 0,40 USD all'ora

> **Note**
>
> Il tipo di parco istanze deve essere `instant`. Altri tipi di parchi istanze non supportano `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            },
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
```

```
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 16,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Dopo aver creato il parco istanze `instant` utilizzando la configurazione precedente, vengono avviate le seguenti 16 istanze per soddisfare la capacità di destinazione:

- 6 `m5.large` On-Demand Instances in `us-east-1a` — `m5.large` in `us-east-1a` è il prezzo più basso e sono disponibili 5 prenotazioni di `m5.large` capacità inutilizzate. Le prenotazioni di capacità vengono utilizzate per prime per avviare 5 On-Demand istanze. Una volta utilizzate le prenotazioni rimanenti `m4.xlarge` e quelle relative alla `m4.2xlarge` capacità, per raggiungere la capacità target viene lanciata un' On-Demand istanza aggiuntiva in base alla strategia di On-Demand allocazione, illustrata `lowest-price` in questo esempio.
- 5 `m4.xlarge` On-Demand Instances in `us-east-1a` — `m4.xlarge` in `us-east-1a` è il prezzo successivo più basso e sono disponibili 5 prenotazioni di capacità non utilizzate `m4.xlarge`
- 5 `m4.2xlarge` On-Demand Instances in `us-east-1a` — `m4.2xlarge` in `us-east-1a` è il terzo prezzo più basso e sono disponibili 5 prenotazioni di capacità inutilizzate `m4.2xlarge`

Dopo l'avvio del parco istanze, puoi eseguire describe-capacity-reservations per vedere quante prenotazioni di capacità sono rimaste inutilizzate. In questo esempio, dovresti vedere la seguente risposta, che mostra che tutti i Prenotazioni di capacità del pool sono stati utilizzati.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 0
}
```

Esempio 6: avvio di On-Demand istanze utilizzando prenotazioni di capacità mirate

È possibile configurare un parco veicoli in modo da utilizzare prima le prenotazioni di `targeted` On-Demand capacità all'avvio On-Demand delle istanze impostando la strategia di utilizzo per le prenotazioni di capacità su. `use-capacity-reservations-first` Questo esempio dimostra come avviare On-Demand le istanze in `targeted` Capacity Reservations, dove gli attributi delle Capacity Reservations sono gli stessi tranne che per le relative zone di disponibilità (e). `us-east-1a` `us-east-1b` Dimostra inoltre come il parco veicoli seleziona i pool di istanze in cui avviare On-Demand le istanze quando la capacità totale di destinazione supera il numero di prenotazioni di capacità inutilizzate disponibili.

In questo esempio, la configurazione del parco istanze è la seguente:

- Capacità target: 10 istanze On-Demand
- Numero totale di prenotazioni `targeted` di capacità inutilizzate: 6 (inferiori alla capacità On-Demand target di 10 On-Demand istanze prevista dalla flotta)
- Numero di prenotazioni della capacità per pool: 2 (`us-east-1a` e `us-east-1b`)
- Numero di prenotazioni della capacità per pool: 3

- On-Demand strategia di allocazione: `lowest-price` (quando il numero di prenotazioni di capacità inutilizzate è inferiore alla capacità On-Demand obiettivo, la flotta determina i pool in cui lanciare la On-Demand capacità residua in base alla On-Demand strategia di allocazione).

  Tenere presente che è anche possibile utilizzare la strategia di allocazione `prioritized` invece della strategia di allocazione `lowest-price`.

Per una spiegazione passo per passo delle procedure che è necessario eseguire per riprodurre questo esempio, consultare Tutorial: configura la flotta EC2 per avviare On-Demand istanze utilizzando prenotazioni di capacità mirate.

Prenotazioni di capacità

L'account presenta le seguenti 6 prenotazioni della capacità inutilizzati in 2 diversi pool. In questo esempio, i pool differiscono per la zona di disponibilità. Il numero di Prenotazioni di capacità in ogni pool è indicato da `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1b",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Configurazione del parco istanze

La seguente configurazione del parco istanze mostra solo le configurazioni pertinenti per questo esempio. La capacità obiettivo totale è 10 e il tipo di capacità obiettivo predefinito è `on-demand`. La

strategia di On-Demand allocazione è. `lowest-price` La strategia di utilizzo per la prenotazione della capacità è `use-capacity-reservations-first`.

In questo esempio, il prezzo di On-Demand Instance per `c5.xlarge` in `us-east-1` è di 0,17 USD all'ora.

> **Note**
>
> Il tipo di parco istanze deve essere `instant`. Altri tipi di parchi istanze non supportano `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
```

```
}
```

Dopo aver creato il parco istanze `instant` utilizzando la configurazione precedente, vengono avviate le seguenti 10 istanze per soddisfare la capacità obiettivo:

- Le prenotazioni di capacità vengono utilizzate per prime per avviare 6 On-Demand istanze come segue:
  - 3 On-Demand istanze vengono lanciate nelle 3 prenotazioni di `c5.xlarge` `targeted` capacità in `us-east-1a`
  - 3 On-Demand istanze vengono lanciate nelle 3 prenotazioni di `c5.xlarge` `targeted` capacità in `us-east-1b`
- Per raggiungere la capacità prevista, 4 On-Demand istanze aggiuntive vengono avviate alla On-Demand capacità normale in base alla strategia di On-Demand allocazione, illustrata `lowest-price` in questo esempio. Tuttavia, poiché i pool hanno lo stesso prezzo (poiché il prezzo è per regione e non per zona di disponibilità), la flotta lancia le 4 On-Demand istanze rimanenti in uno dei pool.

Dopo l'avvio del parco istanze, puoi eseguire describe-capacity-reservations per vedere quante prenotazioni di capacità sono rimaste inutilizzate. In questo esempio, dovresti vedere la seguente risposta, che mostra che tutti i Prenotazioni di capacità del pool sono stati utilizzati.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}
```

Esempio 7: Configurare il ribilanciamento della capacità per avviare la sostituzione delle istanze spot

Nell'esempio seguente viene configurato EC2 Fleet affinché avvii un'istanza spot sostitutiva quando Amazon EC2 emette un suggerimento di ribilanciamento per un'istanza spot del parco istanze.

Per configurare la sostituzione automatica delle istanze spot, per `ReplacementStrategy`, specificare `launch-before-terminate`. Per configurare il ritardo temporale dal momento in cui vengono avviate le nuove istanze spot sostitutive a quando le vecchie istanze spot vengono eliminate automaticamente, per `termination-delay`, specificare un valore in secondi. Per ulteriori informazioni, consulta Opzioni di configurazione.

> **Note**
>
> Si consiglia di utilizzare `launch-before-terminate` solo se è possibile prevedere il tempo necessario per il completamento delle procedure di arresto dell'istanza in modo che le vecchie istanze vengano terminate solo dopo il completamento di queste procedure. Saranno addebitati i costi per entrambe le istanze durante la loro esecuzione.

L'efficacia della strategia di ribilanciamento della capacità dipende dal numero di pool di capacità spot specificati nella richiesta parco istanze EC2. Si consiglia di configurare il parco istanze con un insieme diversificato di tipi di istanza e zone di disponibilità e per `AllocationStrategy`, specificare `capacity-optimized`. Per ulteriori informazioni sugli aspetti da considerare durante la configurazione di un parco istanze EC2 per il ribilanciamento della capacità, consulta Utilizza il ribilanciamento della capacità nel parco istanze EC2 e nel parco istanze spot per sostituire le istanze spot a rischio.

```
{
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "LaunchTemplate",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
```

```
                            "WeightedCapacity": 1,
                             "Placement": {
                                "AvailabilityZone": "us-east-1a"
                            }
                        },
                        {
                            "InstanceType": "c5.large",
                            "WeightedCapacity": 1,
                             "Placement": {
                                "AvailabilityZone": "us-east-1a"
                            }
                        }
                ]
          }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Esempio 8: Avviare le istanze spot in un parco istanze ottimizzato per la capacità

Nell'esempio seguente viene illustrato come configurare un parco istanze EC2 con una strategia di allocazione spot che ottimizza la capacità. Per ottimizzare la capacità, è necessario impostare `AllocationStrategy` su `capacity-optimized`.

Nell'esempio seguente, le tre specifiche di avvio specificano tre pool di capacità spot. La capacità obiettivo è di 50 Istanze spot. Il parco istanze EC2 tenta di avviare 50 istanze spot nel pool di capacità spot con capacità ottimale per il numero di istanze che si stanno avviando.

```
{
```

```
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                  ]
           }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"

    }
}
```

Esempio 9: Avviare le istanze spot in un parco istanze ottimizzato per la capacità con priorità

Nell'esempio seguente viene illustrato come configurare un parco istanze EC2 con una strategia di allocazione spot che ottimizza la capacità che applica la priorità in base al miglior tentativo.

Quando si utilizza la strategia di allocazione `capacity-optimized-prioritized`, è possibile utilizzare il parametro `Priority` per specificare le priorità dei pool di capacità spot, dove a un numero inferiore corrisponde la priorità più alta. È inoltre possibile impostare la stessa priorità per diversi pool di capacità spot, se si preferisce non applicare priorità differenti. Se non si imposta una priorità per un pool, il pool verrà considerato ultimo in termini di priorità.

Per assegnare priorità ai pool di capacità spot, è necessario impostare `AllocationStrategy` su `capacity-optimized-prioritized`. Il parco istanze EC2 ottimizzerà innanzitutto la capacità, ma rispetterà le priorità sulla base del miglior tentativo (ad esempio, se il rispetto delle priorità non influirà in modo significativo sulla capacità del parco istanze EC2 di fornire capacità ottimale). Questa è una buona opzione per i carichi di lavoro in cui è necessario ridurre al minimo la possibilità di interruzioni e la preferenza per determinati tipi di istanza è importante.

Nell'esempio seguente, le tre specifiche di avvio specificano tre pool di capacità spot. Ogni pool ha una priorità, dove a un numero inferiore corrisponde la priorità più alta. La capacità obiettivo è di 50 Istanze spot. Il parco istanze EC2 tenta di avviare 50 istanze spot nel pool di capacità spot con la priorità più alta sulla base del miglior tentativo, ma prima ottimizza la capacità.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                           "InstanceType": "r4.2xlarge",
                           "Priority": 1,
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
```

```
                    },
                     {
                         "InstanceType": "m4.2xlarge",
                         "Priority": 2,
                         "Placement": {
                             "AvailabilityZone": "us-west-2b"
                         },
                     },
                     {
                         "InstanceType": "c5.2xlarge",
                         "Priority": 3,
                         "Placement": {
                             "AvailabilityZone": "us-west-2b"
                         }
                     }
                ]
            }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"
}
```

Esempio 10: avvio di istanze spot in un parco istanze ottimizzato per prezzo e capacità

Nell'esempio seguente viene illustrato come configurare un parco istanze EC2 con una strategia di allocazione spot che ottimizza sia la capacità sia il prezzo più basso. Per ottimizzare la capacità tenendo conto del prezzo, è necessario impostare la `AllocationStrategy` spot su `price-capacity-optimized`.

Nell'esempio seguente, le tre specifiche di avvio specificano tre pool di capacità spot. La capacità obiettivo è di 50 Istanze spot. Il parco istanze EC2 tenta di avviare 50 istanze spot nel pool di capacità spot con capacità ottimale per il numero di istanze che si stanno avviando, scegliendo al contempo il pool con il prezzo più basso.

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MinTargetCapacity": 2,
        "SingleInstanceType": true
```

```
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                  ]
           }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 50,
        "OnDemandTargetCapacity":0,
        "SpotTargetCapacity":50,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Esempio 11: configurazione della selezione del tipo di istanza basata su attributi

Nell'esempio seguente viene illustrato come configurare un parco istanze EC2 in modo da utilizzare la selezione del tipo di istanza basata su attributi per identificare i tipi di istanza. Per specificare gli attributi di istanza richiesti, specifica gli attributi nella struttura `InstanceRequirements`.

Nell'esempio precedente, vengono specificati due attributi di istanza:

- `VCpuCount`: viene specificato un minimo di 2 vCPU. Poiché non è specificato alcun massimo, non esiste un limite massimo.
- `MemoryMiB`: viene specificato un minimo di 4 MiB di memoria. Poiché non è specificato alcun massimo, non esiste un limite massimo.

Verranno identificati tutti i tipi di istanza con 2 o più vCPU e 4 MiB o più di memoria. Tuttavia, la protezione dei prezzi e la strategia di allocazione potrebbero escludere alcuni tipi di istanze quando il parco istanze EC2 alloca le istanze.

Per un elenco e una descrizione di tutti i possibili attributi che puoi specificare, consulta l'API Reference InstanceRequirements di Amazon EC2.

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
```

```
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

Esempio 12: avvia le istanze in più tipi di prenotazione di capacità utilizzando un gruppo di risorse per la prenotazione di capacità

L'esempio seguente configura una flotta `instant` EC2 per avviare istanze su più tipi di prenotazione della capacità (prenotazioni di capacità, blocchi di On-Demand capacità per ML e prenotazioni di capacità interrompibili) utilizzando un unico gruppo di risorse per la prenotazione della capacità. Queste preferenze vengono specificate nella `ReservedCapacityOptions` struttura e impostate su. `DefaultTargetCapacityType` `reserved-capacity`

Nel seguente esempio:

- `ReservationTypes`— Un elenco ordinato dei tipi di prenotazione di capacità da scegliere come target. EC2 Fleet elabora i tipi in questo ordine:`on-demand-capacity-reservation`, poi`capacity-block`, poi`interruptible-capacity-reservation`.
- `AllocationStrategy`— Impostare su per dare priorità `prioritized` ai tipi di istanza all'interno di ciascun tipo di prenotazione di capacità in base all'ordine di sostituzione del tipo di istanza.
- `ReservedCapacityFallbackOptions`— `MarketTypes` è impostato su`["on-demand"]`, in modo che il parco On-Demand istanze avvii qualsiasi capacità target che non può essere soddisfatta con la capacità riservata. Se si omette questa impostazione, la flotta non rientrerà in nessun altro tipo di mercato una volta esauriti i tipi di prenotazione di capacità specificati.

Il modello di lancio è destinato al Capacity Reservation Resource Group. Quando si utilizza`ReservedCapacityOptions`, non è necessario impostare un valore `MarketType` nel modello di lancio: EC2 Fleet lo imposta automaticamente per ogni tipo di prenotazione di capacità.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-cr-resource-group-template",
```

```
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "p5.48xlarge",
                    "AvailabilityZone": "us-east-1a",
                    "Priority": 1
                },
                {
                    "InstanceType": "p4d.48xlarge",
                    "AvailabilityZone": "us-east-1b",
                    "Priority": 2
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 100,
        "DefaultTargetCapacityType": "reserved-capacity"
    },
    "ReservedCapacityOptions": {
        "ReservationTypes": ["on-demand-capacity-reservation", "capacity-block",
 "interruptible-capacity-reservation"],
        "ReservedCapacityFallbackOptions": {
            "MarketTypes": ["on-demand"]
        },
        "AllocationStrategy": "prioritized"
    },
    "Type": "instant"
}
```

Per un tutorial dettagliato, consulta. Tutorial: configura la tua flotta EC2 per avviare le istanze in più tipi di prenotazione della capacità utilizzando un gruppo di risorse per la prenotazione della capacità

Configurazioni CLI di esempi per parco istanze spot

Puoi definire la configurazione di Spot Fleet in un file JSON e quindi fare riferimento a quel file utilizzando il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/request-spot-fleet.html AWS CLI request-spot-fleet per creare la tua flotta, come segue:

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://file_name.json
```

I seguenti esempi illustrano le configurazioni di avvio per vari casi d'uso del parco istanze spot. Per ulteriori informazioni sui parametri di configurazione, consulta request-spot-fleet. Per ulteriori informazioni sulla creazione del parco istanze spot, consulta Creazione di un parco istanze Spot.

> **Note**
>
> Per parco istanze spot, non è possibile specificare un ID di interfaccia di rete in un modello di avvio o in una specifica di avvio. Assicurati di omettere il parametro `NetworkInterfaceID` ne modello di avvio o nella specifica di avvio.

Esempi

- Esempio 1: Avvia le Istanze spot utilizzando la zona di disponibilità con il prezzo più basso nella regione
- Esempio 2: Avvia le Istanze spot utilizzando la zona di disponibilità con il prezzo più basso da un elenco
- Esempio 3: Avvia le Istanze spot utilizzando il tipo di istanza con il prezzo più basso da un elenco
- Esempio 4. Sostituire il prezzo per la richiesta.
- Esempio 5: Avvia un parco istanze spot utilizzando la strategia di allocazione diversificata
- Esempio 6: Avvia un parco istanze spot utilizzando la ponderazione di istanza
- Esempio 7: avvio di una flotta Spot utilizzando la On-Demand capacità
- Esempio 8: Configura il ribilanciamento della capacità per avviare la sostituzione delle istanze spot
- Esempio 9: Avvia le istanze spot in un parco istanze ottimizzato per la capacità
- Esempio 10: Avviare le istanze spot in un parco istanze ottimizzato per la capacità con priorità
- Esempio 11: avvio di istanze Spot in un prezzo CapacityOptimized parco istanze
- Esempio 12: configurazione della selezione del tipo di istanza basata su attributi

Esempio 1: Avvia le Istanze spot utilizzando la zona di disponibilità con il prezzo più basso nella regione

L'esempio seguente indica una specifica di avvio singola senza una zona di disponibilità o una sottorete. Il parco istanze spot avvia le istanze nella zona di disponibilità con il prezzo più basso che ha una sottorete predefinita. Il prezzo da pagare non supera il On-Demand prezzo.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Esempio 2: Avvia le Istanze spot utilizzando la zona di disponibilità con il prezzo più basso da un elenco

Gli esempi seguenti indicano due specifiche di avvio con zone di disponibilità o sottoreti diverse, ma con tipo di istanza e AMI uguali.

Zone di disponibilità

Il parco istanze spot avvia le istanze nella sottorete predefinita della zona di disponibilità specificata.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
```

```
            "InstanceType": "m3.medium",
            "Placement": {
                "AvailabilityZone": "us-west-2a, us-west-2b"
            },
            "IamInstanceProfile": {
                "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
            }
        }
    ]
}
```

Sottoreti

È possibile specificare sottoreti predefinite o sottoreti non predefinite. Queste ultime possono essere da un VPC predefinito o da un VPC non predefinito. Il servizio Spot avvia le istanze in qualsiasi sottorete si trovi nella zona di disponibilità con il prezzo più basso.

Non è possibile specificare sottoreti diverse dalla stessa zona di disponibilità in una richiesta di parco istanze spot.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Se le istanze vengono lanciate in un VPC predefinito, esse ricevono un indirizzo IPv4 pubblico per impostazione predefinita. Se le istanze vengono lanciate in un VPC non predefinito, esse non

ricevono un indirizzo IPv4 pubblico per impostazione predefinita. Utilizzare un'interfaccia di rete nella specifica di avvio per assegnare un indirizzo IPv4 pubblico alle istanze avviate in un VPC non predefinito. Quando si specifica un'interfaccia di rete, bisogna includere l'ID della sottorete e l'ID del gruppo di sicurezza utilizzando l'interfaccia di rete.

```
  ...
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "InstanceType": "m3.medium",
          "NetworkInterfaces": [
              {
                  "DeviceIndex": 0,
                  "SubnetId": "subnet-1a2b3c4d",
                  "Groups": [ "sg-1a2b3c4d" ],
                  "AssociatePublicIpAddress": true
              }
          ],
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ...
```

Esempio 3: Avvia le Istanze spot utilizzando il tipo di istanza con il prezzo più basso da un elenco

Gli esempi seguenti indicano due configurazioni di avvio con tipi di istanza diversi, ma con AMI e zona di disponibilità o sottorete uguali. Il parco istanze spot avvia le istanze utilizzando il tipo di istanza specificato con il prezzo più basso.

Zona di disponibilità

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
```

```
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "c5.4xlarge",
        "Placement": {
          "AvailabilityZone": "us-west-2b"
        }
    },
    {
        "ImageId": "ami-1a2b3c4d",
        "SecurityGroups": [
            {
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "r3.8xlarge",
        "Placement": {
            "AvailabilityZone": "us-west-2b"
        }
    }
  ]
}
```

Sottorete

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
        "ImageId": "ami-1a2b3c4d",
        "SecurityGroups": [
            {
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "c5.4xlarge",
        "SubnetId": "subnet-1a2b3c4d"
    },
    {
        "ImageId": "ami-1a2b3c4d",
        "SecurityGroups": [
            {
```

```
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "r3.8xlarge",
        "SubnetId": "subnet-1a2b3c4d"
    }
  ]
}
```

Esempio 4. Sostituire il prezzo per la richiesta.

Ti consigliamo di utilizzare il prezzo massimo predefinito, che è il On-Demand prezzo. Se si preferisce, è possibile specificare un prezzo massimo per la richiesta del parco istanze e dei prezzi massimi per le specifiche di avvio singole.

Gli esempi seguenti specificano un prezzo massimo per la richiesta del parco istanze e dei prezzi massimi per due delle tre specifiche di avvio. Il prezzo massimo per la richiesta del parco istanze viene utilizzata per ogni specifica di avvio che non indica un prezzo massimo. Il parco istanze spot avvia le istanze utilizzando il tipo di istanza con il prezzo più basso.

Zona di disponibilità

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.20"
```

```
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.8xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        }
    ]
}
```

Sottorete

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "SpotPrice": "0.20"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.8xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      }
  ]
}
```

Esempio 5: Avvia un parco istanze spot utilizzando la strategia di allocazione diversificata

L'esempio seguente utilizza la strategia di allocazione `diversified`. Le specifiche di avvio hanno tipi di istanza diversi ma AMI e zona di disponibilità o sottorete uguali. Il parco istanze spot distribuisce le 30 istanze tra le tre specifiche di avvio, in modo che ci siano 10 istanze di ogni tipo. Per ulteriori informazioni, consulta Utilizza le strategie di allocazione per determinare in che modo EC2 Fleet o Spot Fleet soddisfano Spot e la capacità On-Demand.

Zona di disponibilità

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
  ]
}
```

Sottorete

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Una best practice per aumentare la possibilità che una richiesta spot venga soddisfatta dalla capacità EC2 nel caso si verifichi un'interruzione in una delle zone di disponibilità è diversificare e varie zone. Per questo scenario, includi ogni zona di disponibilità che hai a disposizione nella specifica di avvio. E, invece di utilizzare la stessa sottorete ogni volta, utilizza tre sottoreti univoche (ognuna che mappa a una zona diversa).

Zona di disponibilità

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
```

```
                "AvailabilityZone": "us-west-2a"
            }
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2c"
            }
        }
    ]
}
```

Sottorete

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-2a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-3a2b3c4d"
        }
```

```
    ]
}
```

Esempio 6: Avvia un parco istanze spot utilizzando la ponderazione di istanza

Gli esempi seguenti utilizzano la ponderazione d'istanza, il che significa che il prezzo è all'ora per unità anziché all'ora per istanza. Ogni configurazione di avvio elenca un tipo di istanza diverso e un peso diverso. Il parco istanze spot seleziona il tipo di istanza con il prezzo più basso all'ora per unità. Il parco istanze spot calcola il numero di istanze spot da avviare dividendo la capacità obiettivo per il peso dell'istanza. Se il risultato non è un numero intero, il Parco istanze spot lo arrotonda al numero intero successivo, in modo che la dimensione del parco istanze non sia inferiore alla sua capacità obiettivo.

Se la richiesta `r3.2xlarge` va a buon fine, lo Spot assegna 4 di queste istanze. Dividere 20 per 6 per un totale di 3,33 istanze, quindi arrotondare fino a 4 istanze.

Se la richiesta `c3.xlarge` va a buon fine, lo Spot assegna 7 di queste istanze. Dividere 20 per 3 per un totale di 6,66 istanze, quindi arrotondare fino a 7 istanze.

Per ulteriori informazioni, consulta Utilizza la ponderazione delle istanze per gestire i costi e le prestazioni del parco istanze EC2 o del parco istanze spot.

Zona di disponibilità

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
```

```
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            },
            "WeightedCapacity": 3
        }
    ]
}
```

Sottorete

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 3
      }
  ]
}
```

Esempio 7: avvio di una flotta Spot utilizzando la On-Demand capacità

Per assicurarti di disporre sempre della capacità di istanze, puoi includere una richiesta di On-Demand capacità nella tua richiesta Spot Fleet. Se c'è capacità, la On-Demand richiesta è sempre soddisfatta. mentre il saldo della capacità target viene soddisfatto come Spot se ci sono capacità e disponibilità.

L'esempio seguente specifica la capacità target desiderata come 10, di cui 5 devono essere On-Demand capacità. La capacità spot non è specificata; è implicita nel saldo tra la capacità target e la capacità. On-Demand Amazon EC2 lancia 5 unità di capacità come On-Demand Spot e 5 unità di capacità (10-5=5) come Spot se sono disponibili capacità e disponibilità di Amazon EC2.

```
{
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "AllocationStrategy": "lowestPrice",
  "TargetCapacity": 10,
  "SpotPrice": null,
  "ValidFrom": "2018-04-04T15:58:13Z",
  "ValidUntil": "2019-04-04T15:58:13Z",
  "TerminateInstancesWithExpiration": true,
  "LaunchSpecifications": [],
  "Type": "maintain",
  "OnDemandTargetCapacity": 5,
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0dbb04d4a6cca5ad1",
        "Version": "2"
      },
      "Overrides": [
        {
          "InstanceType": "t2.medium",
          "WeightedCapacity": 1,
          "SubnetId": "subnet-d0dc51fb"
        }
      ]
    }
  ]
}
```

Esempio 8: Configura il ribilanciamento della capacità per avviare la sostituzione delle istanze spot

Nell'esempio seguente viene configurato il parco istanze spot affinché avvii un'istanza spot sostitutiva quando Amazon EC2 emette un suggerimento di ribilanciamento per un'istanza spot del parco istanze. Per configurare la sostituzione automatica delle istanze spot, per `ReplacementStrategy`, specificare `launch-before-terminate`. Per configurare il ritardo temporale dal momento in cui vengono avviate le nuove istanze spot sostitutive a quando le vecchie istanze spot vengono eliminate automaticamente, per `termination-delay`, specificare un valore in secondi. Per ulteriori informazioni, consulta Opzioni di configurazione.

> **Note**
>
> Consigliamo di utilizzare `launch-before-terminate` solo se è possibile prevedere il tempo necessario per il completamento delle procedure di arresto dell'istanza. Ciò garantirà che le vecchie istanze vengano terminate solo dopo il completamento delle procedure di arresto. Saranno addebitati i costi per entrambe le istanze durante la loro esecuzione.

L'efficacia della strategia di ribilanciamento della capacità dipende dal numero di pool di istanze spot specificati nella richiesta del parco istanze spot. Si consiglia di configurare il parco istanze con un insieme diversificato di tipi di istanza e zone di disponibilità e per `AllocationStrategy`, specificare `capacityOptimized`. Per ulteriori informazioni sugli aspetti da considerare durante la configurazione di una serie di istanze spot per il ribilanciamento della capacità, consulta Utilizza il ribilanciamento della capacità nel parco istanze EC2 e nel parco istanze spot per sostituire le istanze spot a rischio.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "LaunchTemplate",
                    "Version": "1"
                },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
```

```
                    },
                    {
                        "InstanceType": "c5.large",
                        "WeightedCapacity": 1,
                        "Placement": {
                            "AvailabilityZone": "us-east-1a"
                        }
                    }
                ]
            }
    ],
        "TargetCapacity": 5,
        "SpotMaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Esempio 9: Avvia le istanze spot in un parco istanze ottimizzato per la capacità

Nell'esempio seguente viene illustrato come configurare un parco istanze spot con una strategia di allocazione spot che ottimizza la capacità. Per ottimizzare la capacità, è necessario impostare `AllocationStrategy` su `capacityOptimized`.

Nell'esempio seguente, le tre specifiche di avvio specificano tre pool di capacità spot. La capacità obiettivo è di 50 Istanze spot. Il parco istanze spot tenta di avviare 50 istanze spot nel pool di capacità spot con capacità ottimale per il numero di istanze che si stanno avviando.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
```

```
            },
            "Overrides": [
                {
                    "InstanceType": "r4.2xlarge",
                    "AvailabilityZone": "us-west-2a"
                },
                {
                    "InstanceType": "m4.2xlarge",
                    "AvailabilityZone": "us-west-2b"
                },
                {
                    "InstanceType": "c5.2xlarge",
                    "AvailabilityZone": "us-west-2b"
                }
            ]
        }
    ]
}
```

Esempio 10: Avviare le istanze spot in un parco istanze ottimizzato per la capacità con priorità

Nell'esempio seguente viene illustrato come configurare un parco istanze spot con una strategia di allocazione spot che ottimizza la capacità che applica la priorità in base al miglior tentativo.

Quando si utilizza la strategia di allocazione `capacityOptimizedPrioritized`, è possibile utilizzare il parametro `Priority` per specificare le priorità dei pool di capacità spot, dove a un numero inferiore corrisponde la priorità più alta. È inoltre possibile impostare la stessa priorità per diversi pool di capacità spot, se si preferisce non applicare priorità differenti. Se non si imposta una priorità per un pool, il pool verrà considerato ultimo in termini di priorità.

Per assegnare priorità ai pool di capacità spot, è necessario impostare `AllocationStrategy` su `capacityOptimizedPrioritized`. Il parco istanze spot ottimizzerà innanzitutto la capacità, ma rispetterà le priorità sulla base del miglior tentativo (ad esempio, se il rispetto delle priorità non influirà in modo significativo sulla capacità del parco istanze spot di fornire capacità ottimale). Questa è una buona opzione per i carichi di lavoro in cui è necessario ridurre al minimo la possibilità di interruzioni e la preferenza per determinati tipi di istanza è importante.

Nell'esempio seguente, le tre specifiche di avvio specificano tre pool di capacità spot. Ogni pool ha una priorità, dove a un numero inferiore corrisponde la priorità più alta. La capacità obiettivo è di 50

Istanze spot. Il parco istanze EC2 tenta di avviare 50 istanze spot nel pool di capacità spot con la priorità più alta sulla base del miglior tentativo, ma prima ottimizza la capacità.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimizedPrioritized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r4.2xlarge",
                   "Priority": 1,
                    "AvailabilityZone": "us-west-2a"
                },
                {
                          "InstanceType": "m4.2xlarge",
                          "Priority": 2,
                          "AvailabilityZone": "us-west-2b"
                },
                {
                          "InstanceType": "c5.2xlarge",
                          "Priority": 3,
                          "AvailabilityZone": "us-west-2b"
                }
            ]
        }
    ]
}
```

Esempio 11: avvio di istanze Spot in un prezzo CapacityOptimized parco istanze

Nell'esempio seguente viene illustrato come configurare un parco istanze spot con una strategia di allocazione spot che ottimizza sia la capacità sia il prezzo più basso. Per ottimizzare la capacità tenendo conto del prezzo, è necessario impostare la `AllocationStrategy` spot su `priceCapacityOptimized`.

Nell'esempio seguente, le tre specifiche di avvio specificano tre pool di capacità spot. La capacità obiettivo è di 50 Istanze spot. Il parco istanze spot tenta di avviare 50 istanze spot nel pool di capacità spot con capacità ottimale per il numero di istanze che si stanno avviando, scegliendo al contempo il pool con il prezzo più basso.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "OnDemandAllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111111111111:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-0123456789example",
                    "Version": "1"
                },
                "Overrides": [
                     {
                          "InstanceType": "r4.2xlarge",
                          "AvailabilityZone": "us-west-2a"
                     },
                     {
                          "InstanceType": "m4.2xlarge",
                          "AvailabilityZone": "us-west-2b"
                     },
                     {
                          "InstanceType": "c5.2xlarge",
                          "AvailabilityZone": "us-west-2b"
                     }
                ]
            }
        ],
        "TargetCapacity": 50,
        "Type": "request"
    }
}
```

Esempio 12: configurazione della selezione del tipo di istanza basata su attributi

Nell'esempio seguente viene illustrato come configurare un parco istanze spot in modo da utilizzare la selezione del tipo di istanza basata su attributi per identificare i tipi di istanza. Per specificare gli attributi di istanza richiesti, specifica gli attributi nella struttura `InstanceRequirements`.

Nell'esempio precedente, vengono specificati due attributi di istanza:

- `VCpuCount`: viene specificato un minimo di 2 vCPU. Poiché non è specificato alcun massimo, non esiste un limite massimo.
- `MemoryMiB`: viene specificato un minimo di 4 MiB di memoria. Poiché non è specificato alcun massimo, non esiste un limite massimo.

Verranno identificati tutti i tipi di istanza con 2 o più vCPU e 4 MiB o più di memoria. Tuttavia, la protezione dei prezzi e la strategia di allocazione potrebbero escludere alcuni tipi di istanze quando il parco istanze spot alloca le istanze.

Per un elenco e una descrizione di tutti i possibili attributi che puoi specificare, consulta l'API InstanceRequirements Reference di Amazon EC2.

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
```

```
 }]
}
```

Quote per il parco istanze EC2 e il parco istanze spot

Hai delle Account AWS quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota è. Region-specific

Alle istanze avviate da un parco istanze EC2 o da un parco istanze spot si applicano le consuete quote di Amazon EC2, ad esempio limiti di istanze spot e limiti di volume.

Inoltre, hai le Account AWS seguenti quote relative a EC2 Fleet e Spot Fleet:

Descrizione della quota	Quota
Il numero di parchi istanze EC2 e di parchi istanze Spot per regione di tipo `maintain` e `request` negli stati `active`, `deleted_running` e `cancelled_running`	1.000 [1] [2] [3]
Il numero di parchi istanze EC2 di tipo `instant`	Illimitato
Il numero di pool di capacità spot (combinazione univoca di tipo di istanza e sottorete) per i parchi istanze EC2 e i parchi istanze spot di tipo `maintain` e `request`	300 [1]
Il numero di pool di capacità spot (combinazione univoca di tipo di istanza e sottorete) per i parchi istanze EC2 di tipo `instant`	Illimitato
La dimensione dei dati utente in una specifica di avvio	16 KB [2]
La capacità obiettivo per il parco istanze EC2 o la serie di istanze Spot	10.000

Descrizione della quota	Quota
Il numero di prenotazioni di capacità per richiesta della flotta EC2 quando si utilizza `ReservedCapacityOptions`	5.000 m²
La capacità obiettivo per tutti i parchi istanze EC2 e le serie di istanze Spot in una regione	100.000 ¹
Una richiesta di parco istanze EC2 o una richiesta di parco istanze spot non può comprendere Regioni diverse.	
Una richiesta di parco istanze EC2 o una richiesta di parco istanze spot non può comprendere sottoreti diverse della stessa zona di disponibilità.	

¹ Queste quote si applicano ai parchi istanze EC2 e alle serie di istanze Spot.

² Tali quote sono rigide. Non puoi richiedere l'aumento di queste quote.

³ Dopo aver eliminato un parco istanze EC2 o annullato una richiesta di serie di istanze Spot, e se hai specificato che il parco istanze non deve terminare le istanze spot quando hai eliminato o annullato la richiesta, la richiesta del parco istanze entra nello stato `deleted_running` (parco istanze EC2) o `cancelled_running` (serie di istanze Spot) e l'esecuzione delle istanze continua finché non viene interrotta o terminata manualmente. Se termini le istanze, la richiesta del parco istanze assume lo stato `deleted_terminating` (parco istanze EC2) o `cancelled_terminating` (serie di istanze Spot) e non conta ai fini di questa quota. Per ulteriori informazioni, consulta Eliminazione di una richiesta del parco istanze EC2 e delle istanze nel parco istanze e Annullare (eliminare) una richiesta di parco istanze spot.

Richiesta di un aumento della quota per la capacità obiettivo

Se hai bisogno di estendere la quota di default per la capacità obiettivo, puoi richiedere un aumento della quota.

Come richiedere un aumento della quota per la capacità obiettivo

1. Apri il modulo Supporto Center Create case.
2. Selezionare Service limit increase (Aumento limiti del servizio).
3. In Limit type (Tipo di limite), scegli EC2 Fleet (parco istanze EC2).
4. Per Regione, scegli la AWS regione in cui richiedere l'aumento della quota.
5. In Limit (Limite), scegli Target Fleet Capacity per Fleet (in units) (Capacità del parco istanze di destinazione per parco istanze [in unità]) oppure Target Fleet Capacity per Region (in units) (Capacità del parco istanze di destinazione per regione [in unità]), a seconda della quota che desideri aumentare.
6. In New limit value (Nuovo valore limite), inserisci il valore della nuova quota.
7. Per richiedere un aumento per un'altra quota, scegli Add another request (Aggiungi un'altra richiesta) e ripeti i passaggi da 4 a 6.
8. In Use case description (Descrizione del caso d'uso), inserisci il motivo della richiesta di aumento della quota.
9. In Contact options (Opzioni di contatto), specifica la lingua e il metodo di contatto preferiti.
10. Seleziona Invia.

Reti in Amazon EC2

Amazon VPC ti consente di lanciare AWS risorse, come le istanze Amazon EC2, in una rete virtuale dedicata al AWS tuo account, nota come cloud privato virtuale (VPC). Quando si avvia un'istanza, è possibile selezionare una sottorete dal VPC. L'istanza è configurata con un'interfaccia di rete primaria, ovvero una scheda di rete virtuale logica. L'istanza riceve un indirizzo IP privato primario dall' IPv4 indirizzo della sottorete e viene assegnata all'interfaccia di rete principale.

Puoi controllare se l'istanza riceve un indirizzo IP pubblico dal pool di indirizzi IP pubblici di Amazon. L'indirizzo IP pubblico di un'istanza è associato all'istanza solo fino a quando non questa viene arrestata o terminata. Se hai bisogno di un indirizzo IP pubblico persistente, puoi allocare un indirizzo IP elastico per il tuo AWS account e associarlo a un'istanza o un'interfaccia di rete. Un indirizzo IP elastico rimane associato al tuo AWS account fino a quando non lo rilasci e puoi spostarlo da un'istanza all'altra secondo necessità. Puoi inoltre portare il tuo intervallo di indirizzi IP all'interno dell'account AWS , dove viene visualizzato come pool di indirizzi; puoi quindi allocare degli indirizzi IP elastici da questo pool di indirizzi.

Per aumentare le prestazioni di rete e ridurre la latenza, puoi avviare istanze in un gruppo di posizionamento. Puoi ottenere prestazioni di pacchetto al secondo (PPS) significativamente più elevate utilizzando la connettività di rete migliorata. Utilizzando un Elastic Fabric Adapter (EFA), un dispositivo di rete che puoi collegare a un tipo di istanza supportato, puoi accelerare le applicazioni di machine learning e di elaborazione ad alte prestazioni.

Funzionalità

- Regioni e zone
- Indirizzamento IP per le istanze Amazon EC2
- Hostname e domini delle istanze EC2
- Trasferire i propri indirizzi IP (BYOIP) in Amazon EC2
- Indirizzi IP elastici
- Interfacce di rete elastiche
- Larghezza di banda di rete dell'istanza Amazon EC2
- Rete migliorata per le istanze Amazon EC2
- Elastic Fabric Adapter per AI/ML carichi di lavoro HPC su Amazon EC2
- Topologia Amazon EC2

- Gruppi di collocamento per le tue istanze Amazon EC2
- Unità massima di trasmissione (MTU) di rete per istanza EC2
- Cloud privati virtuali per le istanze EC2
- Reti secondarie

Regioni e zone

Amazon EC2 è ospitato in più località in tutto il mondo. Queste località sono composte da zone di disponibilità Regioni AWS AWS Outposts, zone locali e zone di lunghezza d'onda.

- Le Regioni sono aree geografiche separate.
- Le zone di disponibilità sono più posizioni isolate all'interno di ogni Regione.
- Le zone locali offrono la possibilità di collocare le risorse, come calcolo e archiviazione, in più posizioni più vicine agli utenti finali.
- Le zone Wavelength offrono la possibilità di creare applicazioni che forniscono latenze molto basse a dispositivi 5G e utenti finali. Wavelength implementa servizi di AWS elaborazione e archiviazione standard ai margini delle reti 5G dei gestori di telecomunicazioni.
- AWS Outpostsoffre AWS servizi, infrastrutture e modelli operativi nativi praticamente in qualsiasi data center, spazio di colocation o struttura locale.

AWS gestisce data center all'avanguardia e ad alta disponibilità. Anche se rari, i guasti che compromettono la disponibilità di istanze nella stessa ubicazione possono verificarsi. Se ospiti tutte le istanze in un'unica ubicazione in cui si verifica un guasto, nessuna di esse risulterà disponibile.

Per ulteriori informazioni, consulta Infrastruttura globale di AWS.

Indice

- Regioni
- Zone di disponibilità
- Local Zones
- Zone Wavelength
- AWS Outposts

Regioni

Ogni regione è pensata per essere isolata dalle altre regioni . Ciò consente di raggiungere la maggiore stabilità e tolleranza ai guasti possibile.

Quando avvii un'istanza, seleziona una Regione che collochi le istanze più vicine a clienti specifici o che soddisfi i requisiti legali o di altro tipo. Puoi avviare istanze in più Regioni.

Quando visualizzi le tue risorse, vedi soltanto le risorse legate alla regione specificata. Questo perché le regioni sono isolate l'una dall'altra e le risorse non vengono replicate in automatico tra le regioni .

Regioni disponibili

Per un elenco delle Regioni disponibili, consulta AWS Regions.

Endpoint regionali per Amazon EC2

Quando utilizzi un'istanza tramite l'interfaccia a riga di comando o le operazioni API, è necessario specificare il relativo endpoint regionale. Per ulteriori informazioni sulle regioni e sugli endpoint per Amazon EC2, consulta la pagina relativa a servizi endpoint Amazon EC2 nella Guida per gli sviluppatori EC2 di Amazon.

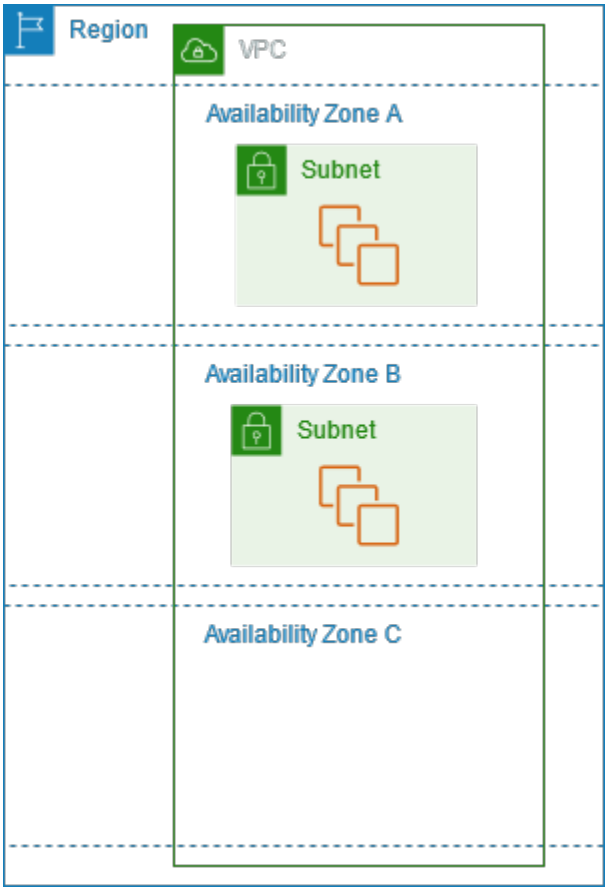
Per ulteriori informazioni, consulta Regioni AWS nella Guida per l'utente di Regioni AWS e zone di disponibilità.

Zone di disponibilità

Ciascuna regione presenta più località isolate, conosciute come zone di disponibilità. Il codice per la zona di disponibilità è il codice della Regione seguito da un identificatore con una lettera. Ad esempio, `us-east-1a`.

Avviando le istanze EC2 in più zone di disponibilità, puoi proteggere le applicazioni dai guasti di una singola posizione nella Regione.

Il diagramma seguente illustra più zone di disponibilità in una regione. AWS La zona di disponibilità A e la zona di disponibilità B hanno una sottorete ciascuna e ogni sottorete contiene istanze EC2. La zona di disponibilità C non ha sottoreti, pertanto non puoi avviare istanze in questa zona di disponibilità.



Per ulteriori informazioni, consulta Cloud privati virtuali per le istanze EC2.

Zone di disponibilità per Regione

Per l'elenco di zone di disponibilità per Regione, consulta Zone di disponibilitàAWS.

istanze nelle zone di disponibilità

Quando avvii un'istanza, selezioni una Regione e un cloud privato virtuale (VPC). In seguito, puoi selezionare una sottorete da una delle zone di disponibilità o consentirci di sceglierne una per te. Quando avvii le istanze iniziali, ti consigliamo di consentirci di selezionare una zona di disponibilità per te a seconda dello stato del sistema e della capacità disponibile. Se avvii istanze aggiuntive, specifica una zona di disponibilità solo se le nuove istanze devono essere vicine alle istanze esistenti o separate da esse.

Se distribuisci le istanze tra più zone di disponibilità e si verifica un errore in un'istanza, puoi progettare l'applicazione affinché un'istanza di un'altra zona di disponibilità possa gestire le richieste.

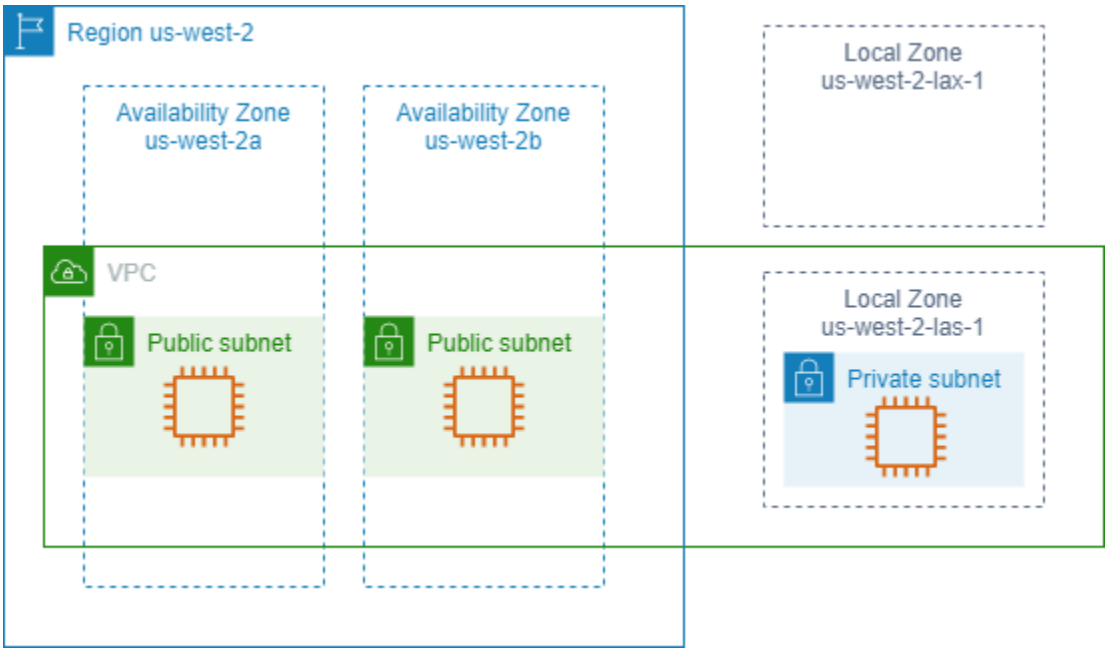
Per ulteriori informazioni, consulta AWS Availability Zones nella Guida per l'utente di Regioni AWS e zone di disponibilità.

Local Zones

Una zona locale è un'estensione di una AWS regione in prossimità geografica degli utenti. Le zone locali dispongono di connessioni a Internet e supporto propri Direct Connect, in modo che le risorse create in una zona locale possano servire gli utenti locali con comunicazioni a bassa latenza. Per ulteriori informazioni, vedi Cosa sono le zone AWS locali? nella Guida per l'utente delle zone AWS locali.

Il codice di una zona locale è il relativo codice della Regione seguito da un identificatore che ne indica la posizione fisica. Ad esempio, `us-west-2-lax-1` a Los Angeles.

Il diagramma seguente illustra la AWS regione`us-west-2`, due delle sue zone di disponibilità e due delle sue zone locali. Il VPC copre le zone di disponibilità e una delle zone locali. Ogni zona del VPC contiene una sottorete e ogni sottorete contiene un'istanza.



Zone locali disponibili

Per l'elenco delle zone locali disponibili, consulta Zone locali disponibili nella Guida per l'utente alle zone locali AWS . Per l'elenco delle zone locali annunciate, consulta Posizioni delle zone locali AWS.

Istanze nelle zone locali

Per utilizzare Local Zone, occorre dapprima abilitarlo. Quindi, crea una sottorete nella zona locale. Puoi specificare la sottorete della zona locale all'avvio delle istanze, collocandole così nella sottorete della zona locale.

Quando avvii un'istanza in una zona locale, assegni anche un indirizzo IP da un gruppo di confine di rete. Un gruppo di confini di rete è un insieme univoco di zone di disponibilità, zone locali o zone di lunghezza d'onda da cui AWS pubblicizza gli indirizzi IP, ad esempio. `us-west-2-lax-1a` Puoi allocare gli indirizzi IP seguenti da un gruppo di confine di rete:

- Amazon-provided Indirizzi IPv4 elastici
- Amazon-provided Indirizzi VPC IPv6 (disponibili solo nelle zone di Los Angeles)

Per ulteriori informazioni su come avviare un'istanza in una zona locale, consulta Getting started with Local Zones nella AWS AWS Local Zones User Guide.

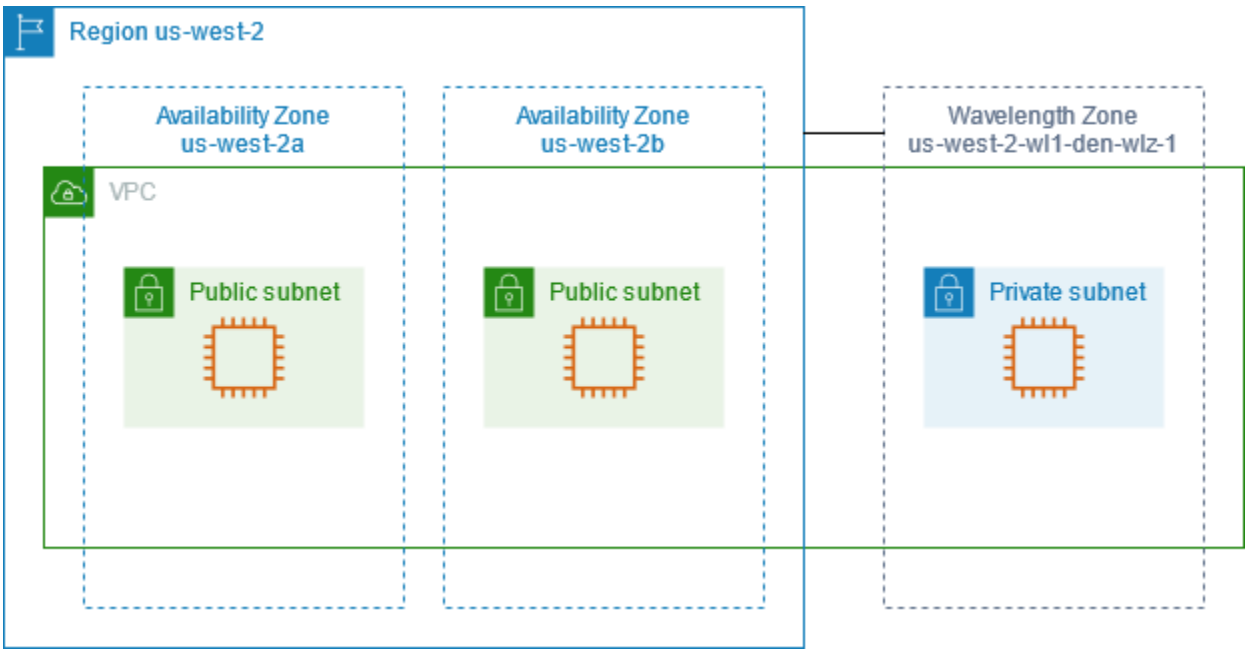
Zone Wavelength

AWS Wavelength consente agli sviluppatori di creare applicazioni che offrono latenze estremamente basse ai dispositivi mobili e agli utenti finali. Wavelength implementa servizi di AWS elaborazione e archiviazione standard ai margini delle reti 5G dei gestori di telecomunicazioni. Gli sviluppatori possono estendere un cloud privato virtuale (VPC) a una o più zone di lunghezza d'onda e quindi utilizzare AWS risorse come le istanze Amazon EC2 per eseguire applicazioni che richiedono una latenza estremamente bassa e una connessione ai servizi nella regione. AWS

Una zona Wavelength è una zona isolata nella posizione carrier in cui viene distribuita l'infrastruttura Wavelength. Le zone Wavelength sono legate a una regione. Una zona Wavelength è un'estensione logica di una regione ed è gestita dal piano di controllo nella regione.

Il codice di una zona Wavelength è il relativo codice della Regione seguito da un identificatore che ne indica la posizione fisica. Ad esempio, `us-east-1-wl1-bos-wlz-1` a Boston.

Il diagramma seguente illustra la AWS regione`us-west-2`, due delle sue zone di disponibilità e una zona di lunghezza d'onda. Il VPC copre le zone di disponibilità e la zona Wavelength. Ogni zona del VPC contiene una sottorete e ogni sottorete contiene un'istanza.



Le zone Wavelength non sono disponibili in tutte le regioni. Per informazioni sulle regioni che supportano le zone Wavelength, consulta Zone Wavelength disponibili nella Guida per gli sviluppatori di AWS Wavelength .

Zone Wavelength disponibili

Per la lista delle zone Wavelength disponibili, consulta Zone Wavelength disponibili nella Guida AWS Wavelength .

Istanze nelle zone Wavelength

Per utilizzare una zona Wavelength, devi prima accettare esplicitamente la zona. Quindi, crea una sottorete nella zona Wavelength. Puoi specificare la sottorete Wavelength all'avvio delle istanze. Inoltre puoi assegnare un indirizzo IP da un gruppo di confine di rete, che è un insieme univoco di zone di disponibilità, zone locali o zone Wavelength da cui AWS pubblicizza gli indirizzi IP, ad esempio `us-east-1-wl1-bos-wlz-1`.

Per informazioni dettagliate su come avviare un'istanza in una zona Wavelength, consulta Nozioni di base su AWS Wavelength nella Guida per gli sviluppatori di AWS Wavelength .

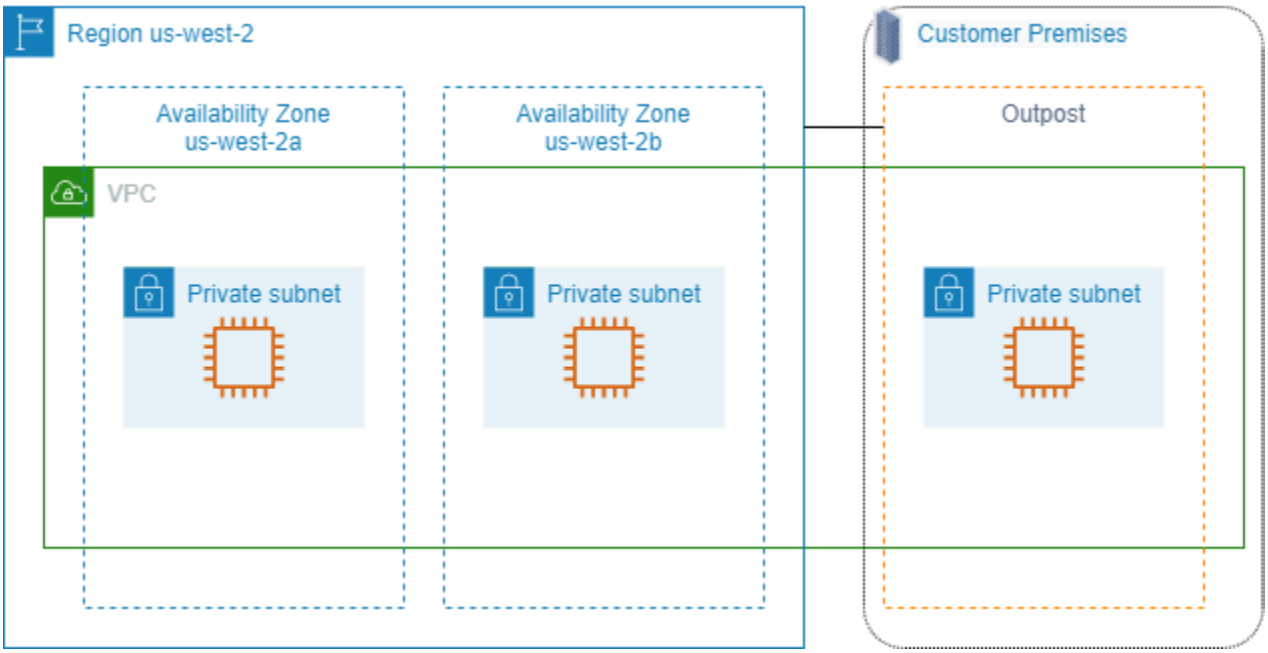
AWS Outposts

AWS Outposts è un servizio completamente gestito che estende l' AWS infrastruttura, i servizi, le API e gli strumenti alle sedi dei clienti. Fornendo l'accesso locale all'infrastruttura AWS gestita,

AWS Outposts consente ai clienti di creare ed eseguire applicazioni in locale utilizzando le stesse interfacce di programmazione AWS delle regioni, utilizzando al contempo risorse di elaborazione e archiviazione locali per esigenze di latenza inferiore e di elaborazione locale dei dati.

Un Outpost è un pool di capacità di AWS elaborazione e archiviazione distribuito presso la sede del cliente. AWS opera, monitora e gestisce questa capacità come parte di una regione. AWS Puoi creare sottoreti sul tuo Outpost e specificarle quando crei le risorse. AWS Le istanze nelle sottoreti Outpost comunicano con altre istanze nella AWS regione utilizzando indirizzi IP privati, tutti all'interno dello stesso VPC.

Il diagramma seguente illustra la AWS regione`us-west-2`, due delle sue zone di disponibilità e un avamposto. Il VPC copre le zone di disponibilità e l'Outpost. L'Outpost si trova in un data center on-premises del cliente. Ogni zona del VPC contiene una sottorete e ogni sottorete contiene un'istanza.



Istanze su un Outpost

Per iniziare a utilizzarlo AWS Outposts, devi creare un Outpost e ordinare la capacità Outpost. AWS Outposts offre due fattori di forma, i rack Outposts e i server Outposts. Per ulteriori informazioni sulle configurazioni degli Outpost, consulta Famiglia AWS Outposts. Dopo aver installato l'apparecchiatura Outpost, la capacità di calcolo e archiviazione è disponibile quando avvii le istanze EC2 sul tuo Outpost.

Per avviare istanze EC2, devi creare una sottorete Outpost. I gruppi di sicurezza controllano il traffico in entrata e in uscita per le istanze di una sottorete Outpost, proprio come per le istanze di una sottorete zona di disponibilità. Per connetterti a istanze in una sottorete Outpost utilizzando SSH,

specifica una coppia di chiavi quando le avvii, proprio come fai per le istanze nelle sottoreti delle zone di disponibilità.

Per ulteriori informazioni, consulta la Guida introduttiva ai rack Outposts o la Guida introduttiva ai server Outposts.

Volumi su un rack Outposts

Se la capacità di calcolo del tuo Outpost si trova su un rack Outpost, puoi creare volumi EBS nella sottorete Outpost che hai creato. Quando crei il volume, specifica il nome della risorsa Amazon (ARN) dell'Outpost.

Il seguente comando create-volume crea un volume vuoto di 50 GB nell'Outpost specificato.

```
aws ec2 create-volume --availability-zone us-east-2a --outpost-arn arn:aws:outposts:us-east-2:123456789012:outpost/op-03e6fecad652a6138 --size 50
```

Puoi modificare dinamicamente la dimensione dei tuoi volumi gp2 Amazon EBS senza scollegarli. Per ulteriori informazioni sulla modifica di un volume senza scollegarlo, consulta Richiesta di modifiche ai volumi EBS nella Guida per l'utente di Amazon EBS.

Ti consigliamo di limitare il volume root per un'istanza su un rack Outpost a 30 GiB o meno. È possibile specificare i volumi di dati nel mappatura dei dispositivi a blocchi dell'AMI o dell'istanza per fornire ulteriore archiviazione. Per tagliare i blocchi inutilizzati dal volume di avvio, consulta Come realizzare volumi EBS di bassa densità nel blog di Partner Network AWS .

Si consiglia di aumentare il timeout NVMe per il volume root. Per ulteriori informazioni, consulta I/O Operation Timeout nella Amazon EBS User Guide.

Volumi su un server Outposts

Le istanze sui server Outposts includono volumi di archivio dell'istanza ma non supportano i volumi EBS. Scegli un'Amazon EBS-backed AMI con un solo snapshot EBS. Scegli una dimensione dell'istanza un archivio istanza sufficiente per soddisfare le esigenze della tua applicazione. Per ulteriori informazioni, consulta Limiti di volume di archivio dell'istanza.

Indirizzamento IP per le istanze Amazon EC2

Amazon EC2 e Amazon VPC supportano entrambi i protocolli di indirizzamento IPv4 e IPv6. Per impostazione predefinita, Amazon VPC utilizza il protocollo di indirizzamento IPv4; tale

comportamento non può essere disabilitato. Quando crei un VPC, devi specificare un blocco CIDR IPv4 (un intervallo di indirizzi IPv4 privati). Facoltativamente, è possibile decidere di assegnare un blocco CIDR IPv6 al VPC e alle sottoreti e di assegnare gli indirizzi IPv6 del blocco alle istanze presenti nelle sottoreti.

Quando avvii un'istanza EC2, puoi specificare un VPC e una sottorete. L'istanza riceve un indirizzo IPv4 privato dall'intervallo CIDR della sottorete. Facoltativamente, puoi scegliere di configurare le istanze con indirizzi IPv4 e IPv6 pubblici. Se le istanze EC2 in diversi VPC comunicano utilizzando indirizzi IP pubblici, il traffico rimane nella rete globale AWS privata e non attraversa la rete Internet pubblica.

Indice

- Indirizzi IPv4 privati
- Indirizzi IPv4 pubblici
- Ottimizzazione dell'indirizzo IPv4 pubblico
- Indirizzi IPv6
- Indirizzi IP multipli
- Nomi host per le istanze EC2
- Link-local indirizzi
- Gestisci gli indirizzi IPv4 per le istanze EC2
- Gestisci gli indirizzi IPv6 per le istanze EC2
- Indirizzi IP secondari per le istanze EC2
- Configura indirizzi IPv4 privati secondari per istanze Windows

Indirizzi IPv4 privati

Un indirizzo IPv4 privato è un indirizzo IP non raggiungibile tramite Internet. Si possono utilizzare gli indirizzi IPv4 privati per la comunicazione tra istanze nello stesso VPC. Per ulteriori informazioni sugli standard e sulle specifiche degli indirizzi IPv4 privati, consulta RFC 1918. Gli indirizzi IPv4 privati vengono allocati sulle istanze tramite DHCP.

> **Note**
>
> Puoi creare un VPC dotato di un blocco CIDR instradabile pubblicamente che non rientra negli intervalli di indirizzi IPv4 privati specificati in RFC 1918. Tuttavia, per gli scopi di questa

documentazione, ci riferiamo agli indirizzi IPv4 privati (o "Indirizzi IP privati") come agli indirizzi IP compresi nell'intervallo CIDR IPv4 del tuo VPC.

Le sottoreti VPC possono essere dei seguenti tipi:

- IPv4-only sottoreti: è possibile creare risorse in queste sottoreti solo a cui sono assegnati indirizzi IPv4.
- IPv6-only sottoreti: è possibile creare risorse in queste sottoreti solo a cui sono assegnati indirizzi IPv6.
- Sottoreti IPv4 e IPv6: è possibile creare risorse in queste sottoreti sia con gli indirizzi IPv4 che IPv6 assegnati.

Quando si avvia un'istanza EC2 in una IPv4-only o più sottoreti (IPv4 e IPv6), l'istanza riceve un indirizzo IP privato primario dall'intervallo di indirizzi IPv4 della sottorete. Per ulteriori informazioni, consulta la sezione Assegnazione di indirizzi IP nella Guida per l'utente di Amazon VPC. Se quando avvii l'istanza non specifichi un indirizzo IP privato primario, saremo noi a selezionare per tuo conto un indirizzo IP disponibile nell'intervallo IPv4 della sottorete. Ogni istanza dispone di un'interfaccia di rete predefinita (index 0) a cui è assegnato l'indirizzo IPv4 privato primario. Si possono anche specificare ulteriori indirizzi IPv4 privati, i cosiddetti indirizzi IPv4 privati secondari. A differenza di quelli primari, gli indirizzi IP privati secondari possono essere riassegnati da un'istanza all'altra. Per ulteriori informazioni, consulta Indirizzi IP multipli.

Un indirizzo IPv4 privato, a prescindere che si tratti di un indirizzo primario o secondario, rimane associato all'interfaccia di rete quando l'istanza viene arrestata e riavviata o ibernata e avviata, e viene rilasciato quando l'istanza viene terminata.

Indirizzi IPv4 pubblici

Un indirizzo IP pubblico è un indirizzo IPv4 raggiungibile tramite Internet. Puoi utilizzare gli indirizzi pubblici per la comunicazione tra le istanze e Internet.

Quando avvii un'istanza in un VPC predefinito, viene assegnato un indirizzo IP pubblico per impostazione predefinita. Quando avvii un'istanza in un VPC non predefinito, la sottorete ha un attributo che determina se le istanze avviate in quella sottorete ricevono un indirizzo IP pubblico dal pool di indirizzi IPv4 pubblici. Per impostazione predefinita, alle istanze avviate in una sottorete non predefinita non vengono assegnati indirizzi IP pubblici.

Puoi controllare se la tua istanza riceve un indirizzo IP pubblico come segue:

- Modifica l'attributo di indirizzamento IP pubblico della sottorete. Per ulteriori informazioni, consulta Modifica dell'attributo di assegnazione degli indirizzi IPv4 pubblici della sottorete nella Guida per l'utente di Amazon VPC.
- Abilita o disabilita la funzionalità di indirizzamento IP pubblico durante l'avvio. In questo modo, viene sovrascritto l'attributo di indirizzamento IP pubblico della sottorete. Per ulteriori informazioni, consulta Assegnare un indirizzo IPv4 pubblico all'avvio.
- Annulla l'assegnazione di un indirizzo IP pubblico all'istanza dopo l'avvio. Per ulteriori informazioni, consulta the section called "Gestire gli indirizzi IP".

Un indirizzo IP pubblico viene assegnato alla tua istanza dal pool di indirizzi IPv4 pubblici di Amazon e non è associato al tuo account. AWS Quando un indirizzo IP pubblico viene disassociato dalla tua istanza, viene reinserito nel pool di indirizzi IPv4 pubblici e non potrai riutilizzarlo.

Rilasciamo l'indirizzo IP pubblico dall'istanza e ne assegniamo uno nuovo nei seguenti casi:

- Rilasciamo l'indirizzo IP pubblico quando l'istanza viene arrestata, ibernata o terminata. Assegniamo un nuovo indirizzo IP pubblico quando avvii l'istanza arrestata o ibernata.
- Rilasciamo l'indirizzo IP pubblico quando associ un indirizzo IP elastico all'istanza. Assegniamo un nuovo indirizzo IP pubblico quando annulli l'associazione dell'indirizzo IP elastico all'istanza.
- Se rilasciamo l'indirizzo IP pubblico dell'istanza ed essa dispone di un'interfaccia di rete secondaria, non assegniamo un nuovo indirizzo IP pubblico.
- Se rilasciamo l'indirizzo IP pubblico dell'istanza ed essa dispone di un indirizzo IP privato secondario associato a un indirizzo IP elastico, non assegniamo un nuovo indirizzo IP pubblico.

Se ti occorre un indirizzo IP pubblico persistente che puoi associare o dissociare in base alle tue esigenze, utilizza un indirizzo IP elastico.

Se utilizzi il DNS dinamico per mappare un nome DNS esistente a un indirizzo IP pubblico di una nuova istanza, potrebbero essere necessarie fino a 24 ore affinché l'indirizzo IP venga propagato in Internet. Come risultato, le nuove istanze potrebbero non ricevere traffico e quelle terminate continuerebbero a ricevere richieste. Per risolvere questo problema, utilizza un indirizzo IP elastico. Puoi allocare un tuo indirizzo IP elastico e associarlo all'istanza in uso. Per ulteriori informazioni, consulta Indirizzi IP elastici.

Se utilizzi Amazon VPC IP Address Manager (IPAM), puoi ottenere un blocco contiguo di indirizzi IPv4 pubblici AWS e utilizzarlo per allocare indirizzi IP elastici alle risorse. AWS L'utilizzo di blocchi di indirizzi IPv4 contigui può ridurre in modo significativo il sovraccarico di gestione degli elenchi di controllo degli accessi di sicurezza e semplificare l'assegnazione e il tracciamento degli indirizzi IP per le aziende che scalano in AWS. Per ulteriori informazioni, consulta Assegnare indirizzi IP elastici sequenziali da un pool IPAM nella Guida per l'utente di Amazon VPC IPAM.

Considerazioni

- AWS addebita tutti gli indirizzi IPv4 pubblici, inclusi gli indirizzi IPv4 pubblici associati alle istanze in esecuzione e gli indirizzi IP elastici. Per ulteriori informazioni, consulta la scheda Public IPv4 Address sulla pagina dei prezzi di Amazon VPC.
- Alle istanze che accedono ad altre istanze tramite l'indirizzo IP NAT pubblico vengono addebitati i costi per il trasferimento di dati Internet o regionali, a seconda che le istanze si trovino nella stessa regione o meno.

Ottimizzazione dell'indirizzo IPv4 pubblico

AWS addebiti per tutti gli indirizzi IPv4 pubblici, inclusi gli indirizzi IPv4 pubblici associati alle istanze in esecuzione e gli indirizzi IP Elastic. Per ulteriori informazioni, consulta la scheda Public IPv4 Address sulla pagina dei prezzi di Amazon VPC.

L'elenco seguente contiene le azioni che è puoi intraprendere per ottimizzare il numero di indirizzi IPv4 pubblici utilizzati:

- Usa un sistema di bilanciamento del carico elastico per bilanciare il traffico verso le tue istanze EC2 e disabilitare l'IP Auto-assign pubblico sull'ENI primario assegnato alle istanze. I bilanciatori del carico utilizzano un unico indirizzo IPv4 pubblico, in modo da ridurre il numero di indirizzi IPv4 pubblici. Potresti anche voler consolidare i bilanciatori del carico esistenti per ridurre ulteriormente il numero di indirizzi IPv4 pubblici.
- Se l'unico motivo per utilizzare un gateway NAT è accedere tramite SSH a un'istanza EC2 in una sottorete privata per la manutenzione o le emergenze, prendi in considerazione l'utilizzo dell'endpoint EC2 Instance Connect. Con l'endpoint EC2 Instance Connect, puoi connetterti a un'istanza da Internet senza che quest'ultima disponga di un indirizzo IPv4 pubblico.
- Se le istanze EC2 si trovano in una sottorete pubblica a cui sono assegnati indirizzi IP pubblici, valuta la possibilità di spostare le istanze in una sottorete privata, di rimuovere gli indirizzi IP pubblici e utilizzare un gateway NAT pubblico per consentire l'accesso da e verso le istanze EC2.

Esistono considerazioni relative ai costi per l'utilizzo dei gateway NAT. Utilizza questo metodo di calcolo per decidere se i gateway NAT sono convenienti. È possibile ottenere il `Number of public IPv4 addresses` necessario per questo calcolo creando un rapporto sui costi di AWS fatturazione e sull'utilizzo.

```
NAT gateway per hour + NAT gateway public IPs + NAT gateway transfer / Existing
 public IP cost
```

Dove:

- `NAT gateway per hour = $0.045 * 730 hours in a month * Number of Availability Zones the NAT gateways are in`
- `NAT gateway public IPs = $0.005 * 730 hours in a month * Number of IPs associated with your NAT gateways`
- `NAT gateway transfer = $0.045 * Number of GBs that will go through the NAT gateway in a month`
- `Existing public IP cost = $0.005 * 730 hours in a month * Number of public IPv4 addresses`

Se il totale è inferiore a 1, i gateway NAT sono più economici degli indirizzi IPv4 pubblici.

- AWS PrivateLinkUtilizzalo per connetterti privatamente a AWS servizi o servizi ospitati da altri AWS account anziché utilizzare indirizzi IPv4 e gateway Internet pubblici.
- Inserisci il tuo intervallo di indirizzi IP (BYOIP) AWS e utilizza l'intervallo per indirizzi IPv4 pubblici anziché utilizzare indirizzi IPv4 pubblici. Amazon-owned
- Disattiva l'assegnazione automatica di un indirizzo IPv4 pubblico aall'istanza avviata nelle sottoreti. Questa opzione è generalmente disabilitata per impostazione predefinita per i VPC quando crei una sottorete, ma dovresti controllare le sottoreti esistenti per assicurarti che sia disabilitata.
- Se disponi di istanze EC2 che non necessitano di indirizzi IPv4 pubblici, verifica che le interfacce di rete collegate alle istanze abbiano l'IP pubblico disabilitato. Auto-assign
- Configura gli endpoint di accelerazione in AWS Global Accelerator per le istanze EC2 in sottoreti private per consentire al traffico Internet di fluire direttamente verso gli endpoint nei tuoi VPC senza richiedere indirizzi IP pubblici. Puoi anche trasferire i tuoi indirizzi a AWS Global Accelerator e utilizzare i tuoi indirizzi IPv4 per gli indirizzi IP statici dell'acceleratore.

Indirizzi IPv6

Gli indirizzi IPv6 sono univoci a livello globale, e possono essere configurati per rimanere privati o essere raggiungibili via Internet. L'indirizzamento IPv6 pubblico e privato è disponibile in AWS:

- IPv6 privato: AWS considera gli indirizzi IPv6 privati quelli che non sono pubblicizzati e non possono essere pubblicizzati su Internet da. AWS
- IPv6 pubblico: AWS considera gli indirizzi IPv6 pubblici quelli pubblicizzati su Internet da. AWS

Per ulteriori informazioni sugli indirizzi IPv6 pubblici e privati, consulta Indirizzi IPv6 nella Guida per l'utente di Amazon VPC.

Tutti i tipi di istanza supportano gli indirizzi IPv6, ad eccezione dei seguenti: C1, M1, M2, M3 e T1.

Le tue istanze EC2 ricevono un indirizzo IPv6 se al VPC e alla sottorete è associato un blocco CIDR IPv6 e se una delle seguenti condizioni è vera:

- La tua sottorete è configurata per assegnare automaticamente un indirizzo IPv6 a un'istanza durante l'avvio. Per ulteriori informazioni, consulta la sezione Modifica dell'attributo di assegnazione degli indirizzi IP della sottorete.
- Assegni un indirizzo IPv6 alla tua istanza durante l'avvio.
- Assegni un indirizzo IPv6 all'interfaccia di rete primaria dell'istanza dopo l'avvio.
- Assegni un indirizzo IPv6 a un'interfaccia di rete nella stessa sottorete e colleghi l'interfaccia di rete all'istanza dopo l'avvio.

Quando l'istanza riceve un indirizzo IPv6 durante l'avvio, l'indirizzo viene associato all'interfaccia di rete primaria (index 0) dell'istanza. Puoi gestire gli indirizzi IPv6 per l'interfaccia di rete primaria delle istanze come segue:

- Assegna o annulla l'assegnazione di indirizzi IPv6 dall'interfaccia di rete. Il numero di indirizzi IPv6 che puoi assegnare a un'interfaccia di rete e il numero di interfacce di rete collegabili a un'istanza variano a seconda del tipo di istanza. Per ulteriori informazioni, consulta Numero massimo di indirizzi IP per interfaccia di rete.
- Abilita un indirizzo IPv6 primario. Un indirizzo IPv6 primario ti consente di evitare l'interruzione del traffico verso istanze o ENI. Per ulteriori informazioni, consulta Crea un'interfaccia di rete per la tua istanza EC2 o Gestire gli indirizzi IP per le interfacce di rete.

Un indirizzo IPv6 persiste quando arresti e avvii o iberni e avvii un'istanza e viene rilasciato quando la termini. Non è possibile riassegnare un indirizzo IPv6 mentre è già assegnato a un'altra interfaccia di rete: devi prima annullare l'assegnazione.

Puoi controllare se le istanze sono raggiungibili tramite i relativi indirizzi IPv6 controllando il routing della tua sottorete o utilizzando le regole ACL del gruppo di sicurezza e della rete. Per ulteriori informazioni, consulta Riservatezza del traffico Internet nella Guida per l'utente di Amazon VPC.

Per ulteriori informazioni sugli intervalli di indirizzi IPv6 riservati, vedere IANA IPv6 Address Registry e RFC4291. Special-Purpose https://tools.ietf.org/html/rfc4291

Indirizzi IP multipli

È possibile specificare più indirizzi IPv4 e IPv6 privati per le tue istanze. Il numero di interfacce di rete e di indirizzi IPv4 e IPv6 privati che si possono specificare per un'istanza dipende dal tipo di istanza. Per ulteriori informazioni, consulta Numero massimo di indirizzi IP per interfaccia di rete.

Casi d'uso

- Ospitare più siti Web su un solo server utilizzando più certificati SSL su un unico server e associando ciascun certificato a un indirizzo IP specifico.
- Gestire appliance di rete, come firewall o load balancer, che hanno più indirizzi IP per ogni interfaccia di rete.
- Reindirizzare il traffico interno verso un'istanza in standby in caso di esito negativo dell'istanza riassegnando l'indirizzo IP secondario all'istanza in standby.

Funzionamento degli indirizzi IP multipli

- Puoi assegnare un indirizzo IPv4 privato secondario a qualsiasi interfaccia di rete.
- Puoi assegnare più indirizzi IPv6 a un'interfaccia di rete che si trova in una sottorete a cui è associato un blocco CIDR IPv6.
- Devi scegliere l'indirizzo IPv4 secondario dall'intervallo del blocco CIDR IPv4 della sottorete dell'interfaccia di rete.
- Devi scegliere gli indirizzi IPv6 dall'intervallo del blocco CIDR IPv6 della sottorete dell'interfaccia di rete.
- È possibile associare i gruppi di sicurezza con le interfacce di rete e non ai singoli indirizzi IP. Pertanto, ogni indirizzo IP specificato in un'interfaccia di rete è soggetto al gruppo di sicurezza dell'interfaccia di rete.

- Gli indirizzi IP multipli possono essere assegnati e tolti alle interfacce di rete collegate a istanze in esecuzione o arrestate.
- Gli indirizzi IPv4 privati secondari assegnati a un'interfaccia di rete possono essere riassegnati a un'altra interfaccia se lo consenti in modo esplicito.
- Un indirizzo IPv6 non può essere riassegnato a un'altra interfaccia di rete; devi prima annullare l'assegnazione dell'indirizzo IPv6 dall'interfaccia di rete esistente.
- Se assegni più indirizzi IP a un'interfaccia di rete utilizzando gli strumenti a riga di comando o l'API, l'intera operazione non va a buon fine se uno degli indirizzi IP non può essere assegnato.
- Gli indirizzi IPv4 privati primari e secondari, gli indirizzi IP elastici e gli indirizzi IPv6 rimangono con l'interfaccia di rete quando l'interfaccia di rete secondaria quando viene scollegata da un'istanza o è collegata a un'istanza.
- Anche se non puoi scollegare l'interfaccia di rete primaria da un'istanza, puoi riassegnare l'indirizzo IPv4 privato secondario dell'interfaccia di rete primaria a un'altra interfaccia di rete.

Per ulteriori informazioni, consulta the section called “Indirizzi IP secondari”.

Nomi host per le istanze EC2

Quando crei un'istanza EC2, crea un nome host per quell'istanza. AWS Per ulteriori informazioni sui tipi di nomi host e su come viene eseguito il provisioning da. AWSHostname e domini delle istanze EC2 Amazon fornisce un server DNS che risolve i Amazon-provided nomi host in indirizzi IPv4 e IPv6. Il server DNS Amazon si trova alla base dell'intervallo di rete VPC più due. Per ulteriori informazioni, consulta Attributi DNS per il VPC nella Guida per l'utente di Amazon VPC.

Link-local indirizzi

Amazon EC2 riserva indirizzi IPv4 link-local specifici per servizi accessibili solo da un'istanza EC2. Questi servizi vengono eseguiti sull'host sottostante, non sull'istanza. Quando accedi agli indirizzi locali di collegamento riservati per questi servizi, stai comunicando con l'Xenhypervisor o il controller Nitro. L'host sottostante gestisce il traffico verso questi indirizzi riservati invece di inoltrarlo in base a percorsi configurati dal cliente. I gruppi di sicurezza e gli ACL di rete non filtrano questo traffico.

AWS non riserva tutti gli indirizzi IPv4 in. `169.254.0.0/16` Il traffico verso un indirizzo non riservato in questo intervallo segue il percorso VPC applicabile. I tuoi gruppi di sicurezza e gli ACL di rete possono filtrare questo traffico.

Link-local intervalli di indirizzi

- IPv4 — 169.254.0. 0/16 (da 169.254.0.0 a 169.254.255.255)
- IPv6: fe80::/10

Servizi a cui si accede utilizzando gli indirizzi link local

- Servizio di metadati delle istanze — `169.254.169.254`
- Amazon Route 53 Resolver(noto anche come server DNS Amazon) — `169.254.169.253`
- Servizio Amazon Time Sync — `169.254.169.123`
- AWS Server KMS

Gestisci gli indirizzi IPv4 per le istanze EC2

È possibile assegnare un indirizzo IPv4 pubblico all'istanza al momento dell'avvio. È possibile visualizzare gli indirizzi IPv4 per l'istanza nella console tramite la pagina Instances (Istanze) o Network Interfaces (Interfacce di rete).

Processi

- Assegnare un indirizzo IPv4 pubblico all'avvio
- Assegnare un indirizzo IPv4 privato all'avvio
- Visualizzare l'indirizzo IPv4 primario
- Visualizzare gli indirizzi IPv4 tramite i metadati dell'istanza

Assegnare un indirizzo IPv4 pubblico all'avvio

Ogni sottorete ha un attributo che determina se alle istanze in essa avviate viene assegnato un indirizzo IP pubblico. Per impostazione predefinita, le sottoreti non predefinite hanno questo attributo impostato su false, mentre le sottoreti predefinite lo hanno impostato su true. Quando avvii un'istanza, hai anche a disposizione una funzione di indirizzamento IPv4 pubblico per controllare se all'istanza è stato assegnato un indirizzo IPv4 pubblico; è possibile sostituire il comportamento predefinito dell'attributo di indirizzamento IP della sottorete. L'indirizzo IPv4 pubblico viene assegnato dal pool di Amazon degli indirizzi IPv4 pubblici e viene assegnato all'interfaccia di rete con indice di dispositivo pari a 0. Questa funzione dipende da alcune condizioni al momento dell'avvio dell'istanza.

Considerazioni

- Puoi annullare l'assegnazione dell'indirizzo IP pubblico alla tua istanza dopo l'avvio gestendo gli indirizzi IP associati a un'interfaccia di rete. Per ulteriori informazioni sugli indirizzi IPv4 pubblici, consulta Indirizzi IPv4 pubblici.
- Se specifichi più di un'interfaccia di rete, non potrai assegnare automaticamente un indirizzo IP pubblico. Inoltre, non è possibile sostituire l'impostazione della sottorete utilizzando la funzione di assegnamento automatico dell'IP pubblico se specifichi un'interfaccia di rete esistente per il dispositivo index 0.
- Che tu assegni un indirizzo IP pubblico all'istanza durante l'avvio o meno, puoi associare un indirizzo IP elastico all'istanza dopo che è stata avviata. Per ulteriori informazioni, consulta Indirizzi IP elastici. Puoi anche modificare il comportamento di indirizzamento IPv4 pubblico della sottorete. Per ulteriori informazioni, consulta Modifica dell'attributo di assegnazione degli indirizzi IPv4 pubblici della sottorete.

Console

Per assegnare un indirizzo IPv4 pubblico all'avvio

Segui la procedura per avviare un'istanza e, quando configuri le impostazioni di rete, scegli l'opzione IP Auto-assign pubblico.

AWS CLI

Per assegnare un indirizzo IPv4 pubblico all'avvio

Usa il comando run-instances con l'opzione `--associate-public-ip-address`.

```
--associate-public-ip-address
```

PowerShell

Per assegnare un indirizzo IPv4 pubblico all'avvio

Utilizza il New-EC2Instance cmdlet con il `-AssociatePublicIp` parametro.

```
-AssociatePublicIp $true
```

Assegnare un indirizzo IPv4 privato all'avvio

Puoi specificare un indirizzo IPv4 privato dall'intervallo di indirizzi IPv4 della sottorete o lasciare che sia Amazon EC2 a sceglierne uno per tuo conto. Questo indirizzo viene assegnato all'interfaccia di rete primaria.

Per assegnare indirizzi IPv4 dopo l'avvio, consulta the section called "Assegnare indirizzi IP secondari a un'istanza".

Console

Per assegnare un indirizzo IPv4 privato all'avvio

Segui la procedura per avviare un'istanza. Quando configuri le Impostazioni di rete, espandi la sezione Configurazione di rete avanzata e inserisci un valore per IP primario.

AWS CLI

Per assegnare un indirizzo IPv4 privato all'avvio

Usa il comando run-instances con l'opzione `--private-ip-address`.

```
--private-ip-addresses 10.251.50.12
```

Per consentire ad Amazon EC2 di scegliere l'indirizzo IP, ometti questa opzione.

PowerShell

Per assegnare un indirizzo IPv4 privato all'avvio

Utilizzare il New-EC2Instance cmdlet con il parametro. `-PrivateIpAddress`

```
-PrivateIpAddress 10.251.50.12
```

Per consentire ad Amazon EC2 di scegliere l'indirizzo IP, ometti questo parametro.

Visualizzare l'indirizzo IPv4 primario

L'indirizzo IPv4 pubblico viene mostrato come proprietà dell'interfaccia di rete nella console, ma è mappato sull'indirizzo IPv4 privato primario tramite NAT. Perciò, se ispezioni le proprietà dell'interfaccia di rete dell'istanza, ad esempio, tramite `ifconfig` (Linux) o `ipconfig` (Windows), l'indirizzo IPv4 pubblico non viene mostrato.

Console

Per visualizzare gli indirizzi IPv4 di un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Nella scheda Reti, trova Indirizzo IPv4 pubblico e Indirizzi IPv4 privati.
5. (Facoltativo) La scheda Reti contiene anche le interfacce di rete e gli indirizzi IP elastici dell'istanza.

AWS CLI

Per visualizzare l'indirizzo IPv4 primario di un'istanza

Utilizzare il comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[].Instances[].PrivateIpAddress" \
    --output text
```

Di seguito è riportato un output di esempio.

```
10.251.50.12
```

PowerShell

Per visualizzare l'indirizzo IPv4 primario di un'istanza

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.PrivateIpAddress
```

Di seguito è riportato un output di esempio.

```
10.251.50.12
```

Visualizzare gli indirizzi IPv4 tramite i metadati dell'istanza

Puoi ottenere gli indirizzi IPv4 dell'istanza recuperando i metadati di tale istanza. Per ulteriori informazioni, consulta Utilizzo dei metadati dell'istanza per gestire l'istanza EC2.

Per visualizzare gli indirizzi IPv4 tramite i metadati dell'istanza

1. Connettiti alla tua istanza. Per ulteriori informazioni, consulta Connettiti all'istanza EC2.
2. Eseguire uno dei seguenti comandi.

   IMDSv2

   Linux

   Esegui il seguente comando dall'istanza Linux.

   ```
   TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/local-ipv4
   ```

   Windows

   Esegui il seguente comando dall'istanza Windows.

   ```
   [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
   seconds" = "21600"} `
       -Method PUT -Uri http://169.254.169.254/latest/api/token
   ```

   ```
   Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
       -Method GET -Uri http://169.254.169.254/latest/meta-data/local-ipv4
   ```

   IMDSv1

   Linux

   Esegui il seguente comando dall'istanza Linux.

   ```
   curl http://169.254.169.254/latest/meta-data/local-ipv4
   ```

Windows

Esegui il seguente comando dall'istanza Windows.

```
Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4
```

3. Usa uno dei seguenti comandi per accedere all'indirizzo IP pubblico. Se esiste un indirizzo IP elastico associato all'istanza, il comando restituisce l'indirizzo IP elastico.

IMDSv2

Linux

Esegui il seguente comando dall'istanza Linux.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
 "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/public-ipv4
```

Windows

Esegui il seguente comando dall'istanza Windows.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/public-ipv4
```

IMDSv1

Linux

Esegui il seguente comando dall'istanza Linux.

```
curl http://169.254.169.254/latest/meta-data/public-ipv4
```

Windows

Esegui il seguente comando dall'istanza Windows.

```
Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4
```

Gestisci gli indirizzi IPv6 per le istanze EC2

Se il VPC e la sottorete hanno blocchi CIDR IPv6 a loro associati, puoi assegnare all'istanza un indirizzo IPv6 durante o dopo l'avvio. Puoi accedere agli indirizzi IPv6 delle istanze nella console dalla pagina Istanze o Interfacce di rete. Le seguenti attività configurano indirizzi IP per le istanze. Per configurare indirizzi IP per le interfacce di rete, consulta the section called "Gestire gli indirizzi IP".

Processi

- Assegnazione di un indirizzo IPv6 a un'istanza
- Visualizzare gli indirizzi IPv6 di un'istanza
- Visualizzare gli indirizzi IPv6 utilizzando i metadati dell'istanza
- Annullare l'assegnazione di un indirizzo IPv6 a un'istanza

Assegnazione di un indirizzo IPv6 a un'istanza

Puoi specificare un indirizzo IPv6 dall'intervallo di indirizzi IPv6 della sottorete o lasciare che sia Amazon EC2 a sceglierne uno per tuo conto. Questo indirizzo viene assegnato all'interfaccia di rete primaria. Tieni presente che i seguenti tipi di istanza non supportano gli indirizzi IPv6: C1, M1, M2, M3 e T1.

Console

Per assegnare un indirizzo IPv6 all'avvio

Segui la procedura per avviare un'istanza. Quando configuri le impostazioni di rete, scegli l'opzione Auto-assign IP IPv6. Se non visualizzi questa opzione, la sottorete selezionata non dispone di un intervallo CIDR IPv6 associato.

Assegnazione di un indirizzo IPv6 dopo l'avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).

3. Selezionare l'istanza e scegliere Actions (Operazioni), Networking (Reti), Manage IP addresses (Gestisci indirizzi IP).
4. Espandere l'interfaccia di rete. In IPv6 Addresses (Indirizzi IPv6) selezionare Assign new IP address (Assegna nuovo indirizzo IP).
5. Inserisci un indirizzo IPv6 dall'intervallo della sottorete o lascia il campo vuoto per consentire ad Amazon EC2 di scegliere l'indirizzo IPv6 per tuo conto. Se non visualizzi questa opzione, la sottorete dell'istanza non dispone di un intervallo CIDR IPv6 associato.
6. Selezionare Salva.

AWS CLI

Per assegnare un indirizzo IPv6 all'avvio

Usa il comando run-instances con l'opzione `--ipv6-addresses`. Il seguente esempio assegna due indirizzi IPv6.

```
--ipv6-addresses Ipv6Address=2001:db8::1234:5678:1.2.3.4
 Ipv6Address=2001:db8::1234:5678:5.6.7.8
```

Per lasciare che sia Amazon EC2 a scegliere gli indirizzi IPv6, usa l'opzione `--ipv6-address-count`. Il seguente esempio assegna due indirizzi IPv6.

```
--ipv6-address-count 2
```

Assegnazione di un indirizzo IPv6 dopo l'avvio

Usa il comando assign-ipv6-addresses. Il seguente esempio assegna due indirizzi IPv6.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8::1234:5678:1.2.3.4 2001:db8::1234:5678:5.6.7.8
```

Per lasciare che sia Amazon EC2 a scegliere gli indirizzi IPv6, usa l'opzione `--ipv6-address-count`. Il seguente esempio assegna due indirizzi IPv6.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-address-count 2
```

PowerShell

Per assegnare un indirizzo IPv6 all'avvio

Utilizzare il New-EC2Instance cmdlet con il parametro. `-Ipv6Address` Il seguente esempio assegna due indirizzi IPv6.

```
-Ipv6Address $ipv6addr1,$ipv6addr2
```

Definisci gli indirizzi IPv6 come indicato di seguito.

```
$ipv6addr1 = New-Object Amazon.EC2.Model.InstanceIpv6Address
$ipv6addr1.Ipv6Address = "2001:db8::1234:5678:1.2.3.4"
$ipv6addr2 = New-Object Amazon.EC2.Model.InstanceIpv6Address
$ipv6addr2.Ipv6Address = "2001:db8::1234:5678:5.6.7.8"
```

Per lasciare che sia Amazon EC2 a scegliere gli indirizzi IPv6, usa il parametro `-Ipv6AddressCount`. Il seguente esempio assegna due indirizzi IPv6.

```
-Ipv6AddressCount 2
```

Assegnazione di un indirizzo IPv6 dopo l'avvio

Utilizza il cmdlet Register-EC2Ipv6AddressList. Il seguente esempio assegna due indirizzi IPv6.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address "2001:db8::1234:5678:1.2.3.4","2001:db8::1234:5678:5.6.7.8"
```

Per lasciare che sia Amazon EC2 a scegliere gli indirizzi IPv6, usa il parametro `-Ipv6AddressCount`. Il seguente esempio assegna due indirizzi IPv6.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6AddressCount 2
```

Visualizzare gli indirizzi IPv6 di un'istanza

Puoi visualizzare gli indirizzi IPv6 delle istanze.

Console

Per visualizzare gli indirizzi IPv6 di un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Nella scheda Networking (Reti) individuare gli IPv6 addresses (Indirizzi IPv6).

AWS CLI

Per visualizzare l'indirizzo IPv6 di un'istanza

Utilizzare il comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[].Ipv6Address" \
    --output text
```

Di seguito è riportato un output di esempio.

```
2001:db8::1234:5678:1.2.3.4
```

PowerShell

Per visualizzare l'indirizzo IPv6 di un'istanza

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.Ipv6Address
```

Di seguito è riportato un output di esempio.

```
2001:db8::1234:5678:1.2.3.4
```

Visualizzare gli indirizzi IPv6 utilizzando i metadati dell'istanza

Una volta stabilita la connessione all'istanza, puoi recuperare gli indirizzi IPv6 utilizzando i metadati dell'istanza. Per prima cosa, devi ottenere l'indirizzo MAC dell'istanza da `http://169.254.169.254/latest/meta-data/network/interfaces/macs/`.

IMDSv2

Linux

Esegui il seguente comando dall'istanza Linux.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/ipv6s
```

Windows

Esegui i seguenti cmdlet dall'istanza Windows.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/ipv6s
```

IMDSv1

Linux

Esegui il seguente comando dall'istanza Linux.

```
curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/ipv6s
```

Windows

Esegui il seguente cmdlet dall'istanza Windows.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/network/interfaces/
macs/mac-address/ipv6s
```

Annullare l'assegnazione di un indirizzo IPv6 a un'istanza

È possibile annullare l'assegnazione di un indirizzo IPv6 da un'istanza in qualsiasi momento.

Console

Per annullare l'assegnazione di un indirizzo IPv6 a un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza e scegliere Actions (Operazioni), Networking (Reti), Manage IP addresses (Gestisci indirizzi IP).
4. Espandere l'interfaccia di rete. In IPv6 Addresses (Indirizzi IPv6), selezionare Unassign (Annulla l'assegnazione) accanto all'indirizzo IPv6.
5. Selezionare Salva.

AWS CLI

Per annullare l'assegnazione di un indirizzo IPv6 a un'istanza

Usa il comando unassign-ipv6-addresses.

```
aws ec2 unassign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8::1234:5678:1.2.3.4
```

PowerShell

Per annullare l'assegnazione di un indirizzo IPv6 a un'istanza

Utilizza il cmdlet Unregister-EC2Ipv6AddressList.

```
Unregister-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address 2001:db8::1234:5678:1.2.3.4
```

Indirizzi IP secondari per le istanze EC2

Il primo indirizzo IPv4 assegnato a un'interfaccia di rete è noto come indirizzo IP primario. Gli indirizzi IP secondari sono indirizzi IPv4 aggiuntivi assegnati a un'interfaccia di rete. Per ulteriori informazioni, consulta the section called "Indirizzi IP multipli".

Puoi anche assegnare più indirizzi IPv6 a un'istanza. Per ulteriori informazioni, consulta the section called "Indirizzi IPv6".

Processi

- Assegnare indirizzi IP secondari a un'istanza
- Configurare il sistema operativo per l'utilizzo di indirizzi IP secondari
- Annullare l'assegnazione di un indirizzo IP secondario a un'istanza

Assegnare indirizzi IP secondari a un'istanza

Puoi assegnare indirizzi IP secondari all'interfaccia di rete di un'istanza quando la avvii o quando è in esecuzione.

Console

Per assegnare un indirizzo IP secondario all'avvio

1. Segui la procedura per avviare un'istanza. Quando configuri le Impostazioni di rete, espandi la sezione Configurazione di rete avanzata.
2. In IP secondario, scegli Assegnazione automatica e inserisci il numero di indirizzi IP che Amazon EC2 deve assegnare. In alternativa, scegli Assegnazione manuale e inserisci gli indirizzi IPv4.
3. Completa i passaggi restanti per avviare l'istanza.

Per assegnare un indirizzo IP secondario dopo l'avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza e scegliere Actions (Operazioni), Networking (Reti), Manage IP addresses (Gestisci indirizzi IP).
4. Espandere l'interfaccia di rete.

5. Per aggiungere un indirizzo IPv4, in Indirizzi IPv4, scegli Assegna un nuovo indirizzo IP. Inserisci un indirizzo IPv4 dall'intervallo della sottorete o lascia il campo vuoto per consentire ad Amazon EC2 di sceglierne uno per tuo conto.
6. Selezionare Salva.

AWS CLI

Per assegnare un indirizzo IP secondario all'avvio

Usa il comando run-instances con l'opzione `--secondary-private-ip-addresses`.

```
--secondary-private-ip-addresses 10.251.50.12
```

Per lasciare che sia Amazon EC2 a scegliere l'indirizzo IP, usa l'opzione `--secondary-private-ip-address-count`. Il seguente esempio assegna un indirizzo IP secondario.

```
--secondary-private-ip-address-count 1
```

In alternativa, puoi creare un'interfaccia di rete. Per ulteriori informazioni, consulta the section called "Creazione di un'interfaccia di rete".

Per assegnare un indirizzo IP secondario dopo l'avvio

Usa il comando assign-private-ip-addresses con l'opzione `--private-ip-addresses`.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-ids eni-1234567890abcdef0 \
    --private-ip-addresses 10.251.50.12
```

Per lasciare che sia Amazon EC2 a scegliere l'indirizzo IPv4, usa il parametro `--secondary-private-ip-address-count`. Il seguente esempio assegna un indirizzo IPv4.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-ids eni-1234567890abcdef0 \
    --secondary-private-ip-address-count 1
```

PowerShell

Per assegnare un indirizzo IP secondario all'avvio

Devi creare un'interfaccia di rete. Per ulteriori informazioni, consulta the section called "Creazione di un'interfaccia di rete".

Per assegnare un indirizzo IP secondario dopo l'avvio

Utilizzare il Register-EC2PrivateIpAddress cmdlet con il parametro. `-PrivateIpAddress`

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -PrivateIpAddress 10.251.50.12
```

Per lasciare che sia Amazon EC2 a scegliere gli indirizzi IPv4, usa il parametro `-SecondaryPrivateIpAddressCount`. Il seguente esempio assegna un indirizzo IPv4.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -SecondaryPrivateIpAddressCount 1
```

Configurare il sistema operativo per l'utilizzo di indirizzi IP secondari

Dopo aver assegnato un indirizzo IP secondario all'istanza, devi configurare il sistema operativo dell'istanza affinché riconosca l'indirizzo IPv4 privato aggiuntivo.

Istanze Linux

- Se utilizzi Amazon Linux, il pacchetto ec2-net-utils può occuparsi di questo passaggio al posto tuo. Configura altre interfacce di rete da collegare mentre l'istanza è in esecuzione, aggiorna gli indirizzi IPv4 secondari durante il rinnovo della locazione DHCP e le relative regole di routing. Puoi aggiornare immediatamente l'elenco di interfacce utilizzando uno dei seguenti comandi, a seconda del sistema operativo in uso: `sudo systemctl restart systemd-networkd` (AL2023) o `sudo service network restart` (Amazon Linux 2). Puoi visualizzare l'elenco aggiornato utilizzando il seguente comando: `ip addr li`. Se preferisci il controllo manuale della configurazione di rete, puoi rimuovere il pacchetto ec2-net-utils. Per ulteriori informazioni, consulta Configurazione dell'interfaccia di rete mediante ec2-net-utils.
- Se utilizzi un'altra distribuzione Linux, consulta la relativa documentazione. Cerca le informazioni sulla configurazione di altre interfacce di rete e di indirizzi IPv4 secondari. Se l'istanza ha due o più interfacce nella stessa sottorete, cerca le informazioni sull'utilizzo delle regole di routing per risolvere il routing asimmetrico.

Istanze Windows

Per ulteriori informazioni, consulta Configura indirizzi IPv4 privati secondari per istanze Windows.

Annullare l'assegnazione di un indirizzo IP secondario a un'istanza

Se non hai più bisogno di un indirizzo IP secondario, puoi annullarne l'assegnazione all'istanza o all'interfaccia di rete. Quando viene annullata l'assegnazione di un indirizzo IPv4 privato secondario a un'interfaccia di rete, viene dissociato anche l'indirizzo IP elastico (se presente).

Console

Per annullare l'assegnazione a un'istanza di un indirizzo IPv4 privato secondario

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona un'istanza, scegli Operazioni, Reti, Gestisci indirizzi IP.
4. Espandere l'interfaccia di rete. Per gli Indirizzi IPv4 seleziona Annulla l'assegnazione per l'indirizzo IPv4 a cui annullare l'assegnazione.
5. Selezionare Salva.

AWS CLI

Per annullare l'assegnazione di un indirizzo IP privato secondario

Usa il comando unassign-private-ip-addresses.

```
aws ec2 unassign-private-ip-addresses \
    --network-interface eni-1234567890abcdef0\
    --private-ip-addresses 10.251.50.12
```

PowerShell

Per annullare l'assegnazione di un indirizzo IP privato secondario

Utilizza il cmdlet Unregister-EC2PrivateIpAddress.

```
Unregister-EC2PrivateIpAddress `
    -NetworkInterface eni-1234567890abcdef0 `
    -PrivateIpAddress 10.251.50.12
```

Configura indirizzi IPv4 privati secondari per istanze Windows

Puoi specificare più indirizzi IPv4 privati per le tue istanze. Dopo aver assegnato un indirizzo IPv4 privato secondario a un'istanza, devi configurare il sistema operativo dell'istanza per riconoscere l'indirizzo IPv4 privato secondario.

> **Note**
>
> Queste istruzioni fanno riferimento a Windows Server 2022. L'implementazione di queste fasi potrebbe variare in base al sistema operativo dell'istanza Windows.

Processi

- Prerequisiti
- Fase 1: configurazione degli indirizzi IP statici nell'istanza
- Fase 2: configurazione di un indirizzo IP privato secondario per l'istanza
- Fase 3: configurazione delle applicazioni per l'utilizzo dell'indirizzo IP privato secondario

Prerequisiti

- Assegna l'indirizzo IPv4 privato secondario all'interfaccia di rete dell'istanza. Puoi assegnare l'indirizzo IPv4 privato secondario all'interfaccia di rete quando avvii l'istanza o quando è in esecuzione. Per ulteriori informazioni, consulta Assegnare indirizzi IP secondari a un'istanza.

Fase 1: configurazione degli indirizzi IP statici nell'istanza

Per abilitare l'istanza Windows all'utilizzo di più indirizzi IP, devi configurare l'istanza per l'utilizzo degli indirizzi IP statici anziché di un server DHCP.

> **Important**
>
> Quando configuri gli indirizzi IP statici nell'istanza, l'indirizzo IP deve corrispondere esattamente a quanto visualizzato nella console, nella CLI o nell'API. Se immetti questi indirizzi IP in modo errato, l'istanza potrebbe diventare irraggiungibile.

Per configurare gli indirizzi IP statici su un'istanza Windows

1. Connettiti alla tua istanza.
2. Cercare l'indirizzo IP, una subnet mask e gli indirizzi gateway di default per l'istanza eseguendo le fasi seguenti:

   - Esegui il seguente comando in PowerShell:

     ```
     ipconfig /all
     ```

     Esamina l'output e annota i valori visualizzati nei campi Indirizzo IPv4, Maschera di sottorete, Gateway di default e Server DNS per l'interfaccia di rete. L'output dovrebbe essere simile all'esempio seguente:

     ```
     ...

     Ethernet adapter Ethernet 4:

        Connection-specific DNS Suffix  . : us-west-2.compute.internal
        Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
        Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
        IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Lease Obtained. . . . . . . . . . : Monday, April 8, 2024 12:19:29 PM
        Lease Expires . . . . . . . . . . : Monday, April 8, 2024 4:49:30 PM
        Default Gateway . . . . . . . . . : 10.200.0.1
        DHCP Server . . . . . . . . . . . : 10.200.0.1
        DHCPv6 IAID . . . . . . . . . . . : 151166011
        DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-
     E7
        DNS Servers . . . . . . . . . . . : 10.200.0.2
        NetBIOS over Tcpip. . . . . . . . : Enabled
     ```

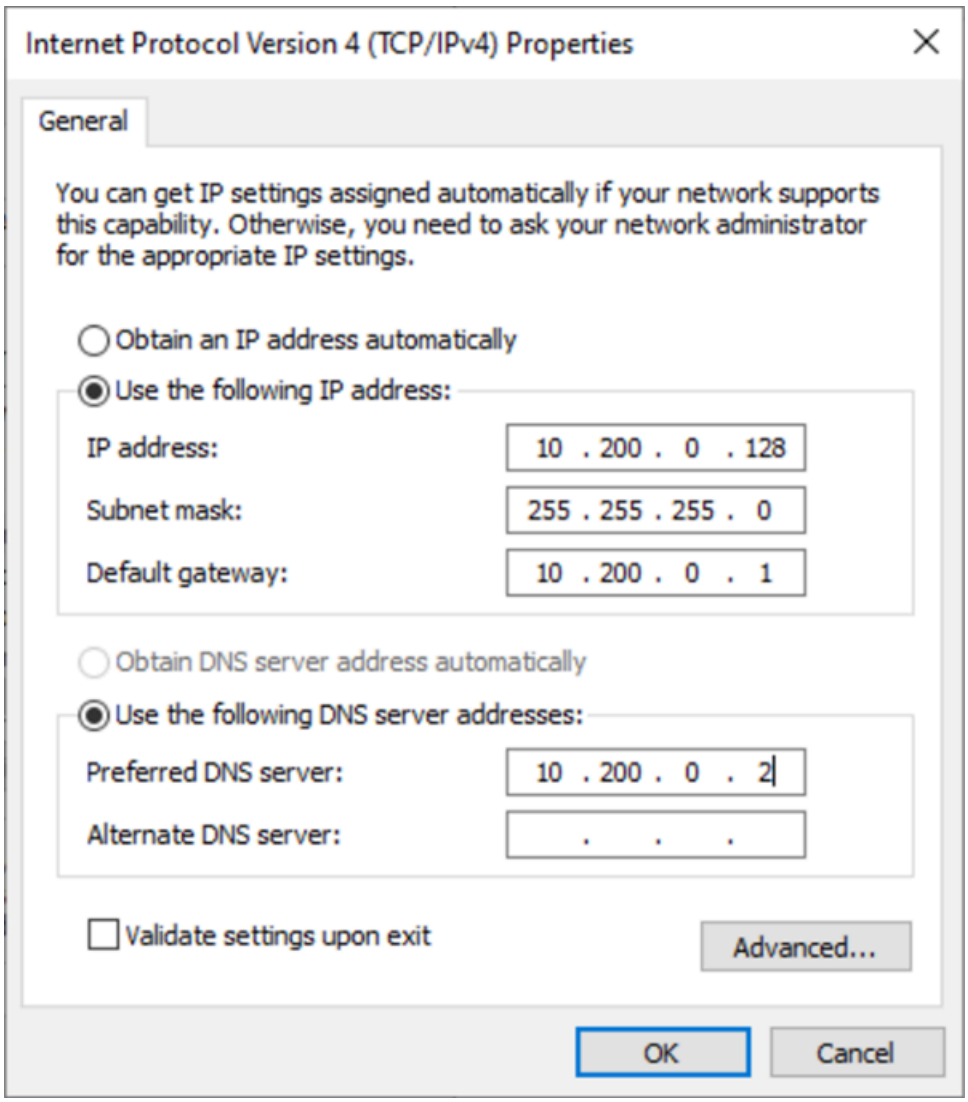
3. Aprire il Centro connessioni di rete e condivisione eseguendo il seguente comando in PowerShell:

   ```
   & $env:SystemRoot\system32\control.exe ncpa.cpl
   ```

4. Aprire il menu contestuale (fare clic con il pulsante destro del mouse) per l'interfaccia di rete (connessione alla rete locale o Ethernet) e scegliere Proprietà.
5. Scegli Internet Protocol Version 4 (TCP/IPv4), Proprietà.
6. Nella finestra di dialogo Proprietà del protocollo Internet versione 4 (TCP/IPv4), scegliete Usa il seguente indirizzo IP, immettete i seguenti valori, quindi scegliete OK.

Campo	Valore
IP address (Indirizzo IP)	Indirizzo IPv4 annotato nella precedente fase 2.
Maschera sottorete	Subnet mask annotata nella precedente fase 2.
Default gateway (Gateway predefinito)	Indirizzo del gateway di default annotato nella precedente fase 2.
Preferred DNS server (Server DNS preferito)	Server DNS annotato nella precedente fase 2.
Alternate DNS server (Server DNS alternativo)	Server DNS alternativo annotato nella precedente fase 2. Se nell'output non è visualizzato alcun server DNS alternativo, lasciare vuoto questo campo.

> **Important**
>
> Se si imposta l'indirizzo IP su un qualsiasi valore diverso dall'indirizzo IP corrente, la connettività all'istanza andrà perduta.



Si perderà la connettività RDP all'istanza Windows per alcuni secondi mentre l'istanza viene convertita dall'uso di DHCP all'uso degli indirizzi statici. L'istanza conserva le stesse informazioni sugli indirizzi IP di prima, ma ora queste informazioni sono statiche e non sono gestite da DHCP.

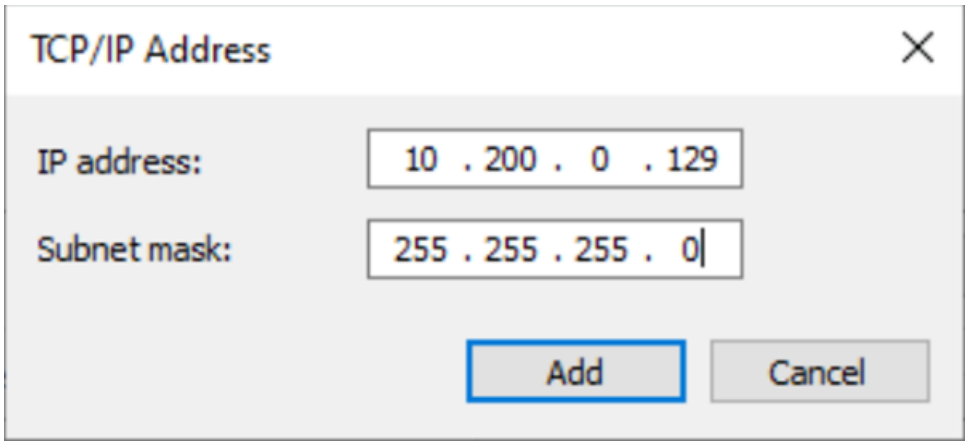
Fase 2: configurazione di un indirizzo IP privato secondario per l'istanza

Dopo aver configurato gli indirizzi IP statici sull'istanza Windows, prepara un indirizzo IP privato secondario.

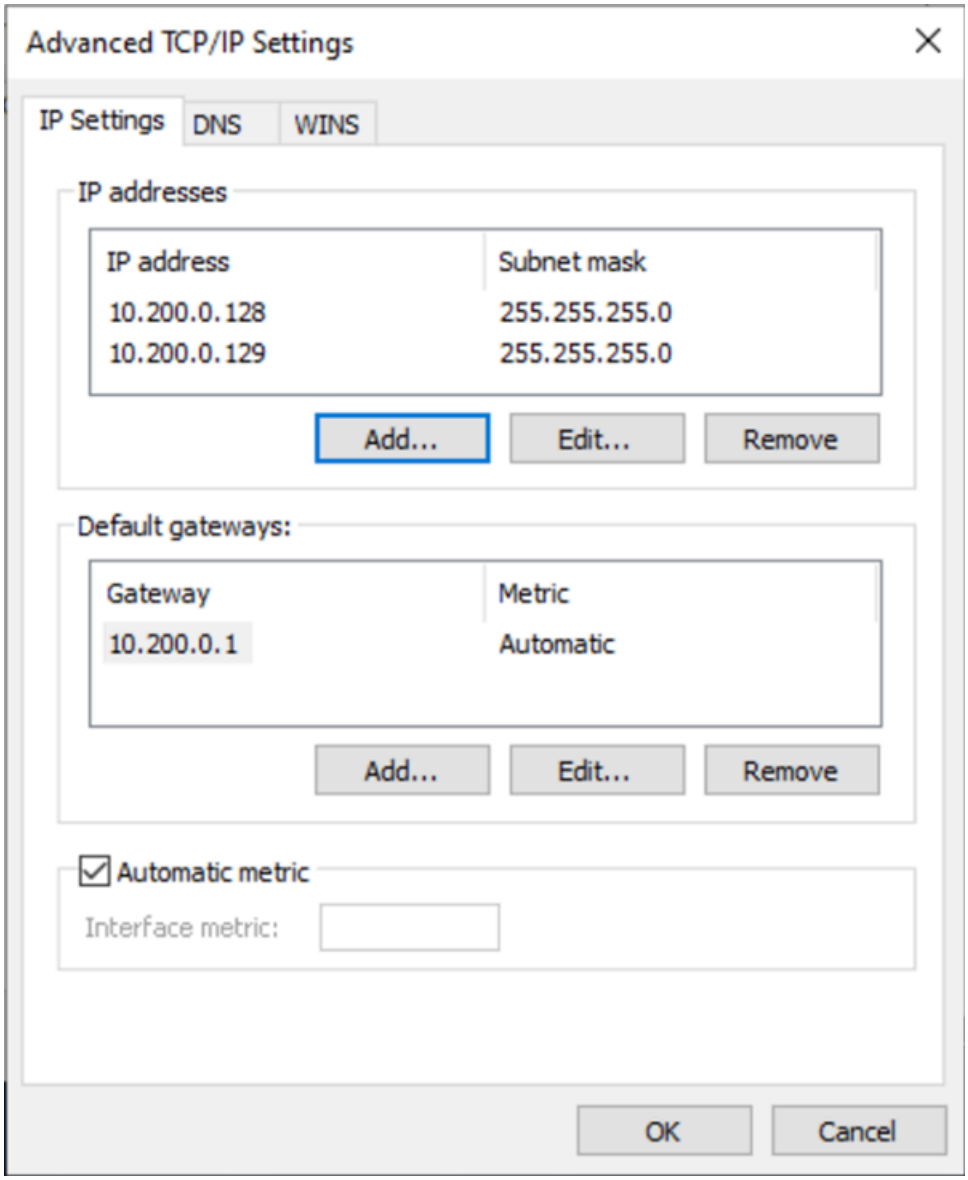
Per configurare un indirizzo IP secondario

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, selezionare Instances (Istanze) e selezionare l'istanza.
3. In Networking (Rete), prendere nota dell'indirizzo IP secondario.
4. Connettiti alla tua istanza.
5. Nell'istanza di Windows scegliere Start, Control Panel (Pannello di controllo).
6. Scegliere Network and Internet (Rete e Internet), Network and Sharing Center (Centro connessioni di rete e condivisione).
7. Selezionare l'interfaccia di rete (connessione alla rete locale o Ethernet) e scegliere Proprietà.
8. Nella pagina delle proprietà della connessione alla rete locale, scegli Protocollo Internet versione 4 (TCP/IPv4), Proprietà, Avanzate.
9. Scegliere Aggiungi.
10. Nella finestra di dialogo TCP/IP Indirizzo, digitate l'indirizzo IP privato secondario per l'indirizzo IP. Per Subnet mask (Maschera sottorete), immettere la stessa subnet mask specificata per l'indirizzo IP privato principale nella Fase 1: configurazione degli indirizzi IP statici nell'istanza, quindi scegliere Add (Aggiungi).



11. Verificare le impostazioni dell'indirizzo IP e scegliere OK.



12. Scegliere OK, Close (Chiudi).
13. Per confermare che l'indirizzo IP secondario è stato aggiunto al sistema operativo, esegui il `ipconfig /all` comando in PowerShell. L'output visualizzato dovrebbe essere simile al seguente:

```
Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
   Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

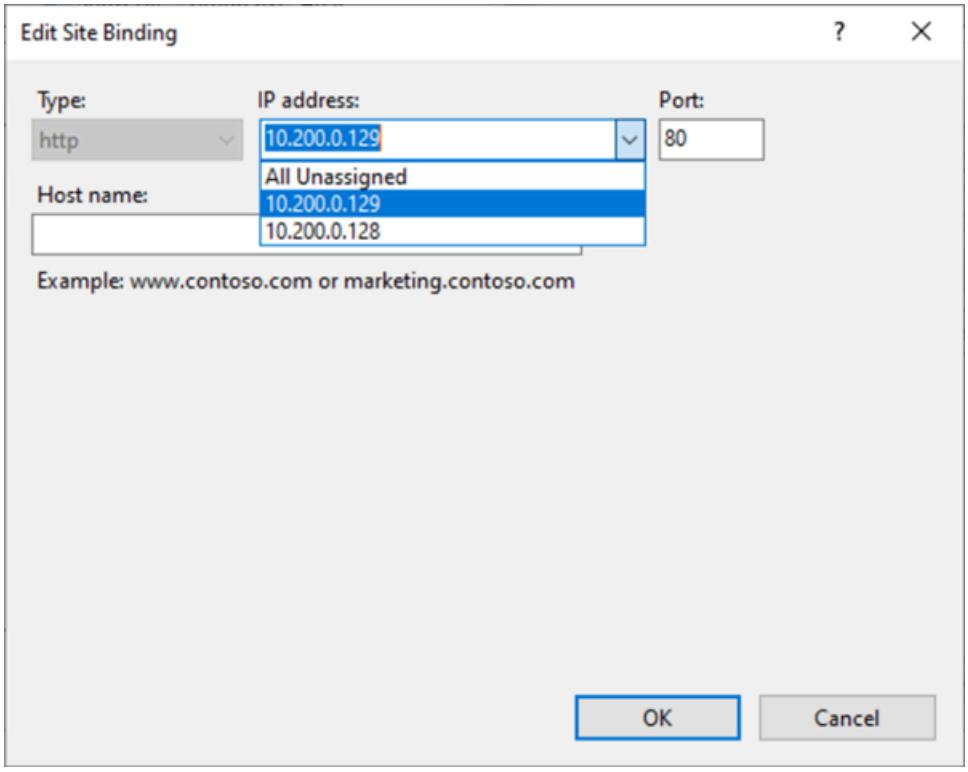
```
   Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 10.200.0.129(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.200.0.1
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Fase 3: configurazione delle applicazioni per l'utilizzo dell'indirizzo IP privato secondario

Puoi configurare qualsiasi applicazione per l'utilizzo dell'indirizzo IP privato secondario. Ad esempio, se l'istanza esegue un sito Web su IIS, puoi configurare IIS per l'uso dell'indirizzo IP privato secondario.

Per configurare IIS per l'utilizzo dell'indirizzo IP privato secondario

1. Connettiti alla tua istanza.
2. Aprire Internet Information Services (IIS) Manager (Gestione Internet Information Services [IIS]).
3. Nel riquadro Connections (Connessioni) espandere Sites (Siti).
4. Aprire il menu contestuale (pulsante destro del mouse) per il sito Web e scegliere Edit Bindings (Modifica binding).
5. Nella finestra di dialogo Site Bindings (Binding sito), per Type (Tipo) scegliere http, Edit (Modifica).
6. Nella finestra di dialogo Edit Site Binding (Modifica binding sito), selezionare l'indirizzo IP privato secondario in IP address (Indirizzo IP). Per impostazione di default, ogni sito Web accetta richieste HTTP da tutti gli indirizzi IP.



7. Scegliere OK, Close (Chiudi).

Hostname e domini delle istanze EC2

Comprendere gli hostname e i domini delle istanze EC2 è importante per gestire e accedere in modo efficace alle istanze Amazon EC2. Ogni istanza EC2 può avere diversi tipi di hostname, privati e pubblici, che servono a scopi diversi e seguono convenzioni di denominazione specifiche.

Questo argomento spiega la struttura degli hostname delle istanze EC2, come sono costruiti e i diversi tipi di hostname disponibili. Scoprirai come visualizzare e modificare le impostazioni dei nomi host, capire quando utilizzare ciascun tipo e apprendere le best practice per la gestione dei nomi host nel tuo AWS ambiente.

Indice

- Comprensione degli hostname e dei domini delle istanze EC2
- Tipi di hostname

Comprensione degli hostname e dei domini delle istanze EC2

Un indirizzo di istanza EC2 è composto da diversi componenti. Di seguito è riportato un esempio di un indirizzo di istanza EC2 che utilizza l'indirizzo IPv4 privato dell'istanza:

```
   IP address         Domain name
   #--------# #-----------------------#
ip-10-24-34-0.us-west-2.compute.internal
#-----------#
  Hostname
#-------------------------------------#
    Fully qualified domain name (FQDN)
```

Dove:

- Indirizzo IP: l'indirizzo IPv4 primario dell'interfaccia di rete principale associata a un'istanza.
- Hostname: il nome locale di una specifica istanza EC2 (utilizzato dal sistema operativo e per l'identificazione della rete locale)
- Nome di dominio: la parte del FQDN che fornisce AWS
- Nome di dominio completo (FQDN): l'indirizzo completo che include sia l'hostname che il nome di dominio. Si tratta dell'identificatore univoco completo e globale utilizzato per raggiungere l'istanza in tutte le reti.

A seconda del tipo di hostname scelto per l'istanza o l'interfaccia di rete principale collegata all'istanza, i formati dell'hostname e del nome di dominio saranno diversi dall'esempio precedente. Questa sezione spiega le opzioni del tipo di hostname.

Tipi di hostname

AWS fornisce due tipi di nomi host: privati e pubblici. La tabella seguente confronta le principali differenze tra gli hostname privati e pubblici, incluso il modo in cui si risolvono, come sono configurati e quando utilizzare ciascun tipo.

	Hostname privati	Hostname pubblici
Risoluzione DNS	Gli hostname privati abilitano FQDN privati non accessibili da Internet pubblico. Gli hostname privati	Gli hostname pubblici abilitano FQDN pubblici accessibili da Internet pubblico. Gli hostname pubblici

	Hostname privati	Hostname pubblici
	consentono solo alle richieste di risolversi a indirizzi GUA IPv4 e IPv6 privati all'interno del VPC.	consentono alle richieste di risolversi a GUA IPv4 e IPv6 privati all'interno del VPC e IP pubblici da Internet (DNS split-horizon).
Configurazione	Gli hostname privati vengono configurati a livello di istanza.	Gli hostname pubblici sono configurati a livello di interfaccia di rete.
Quando utilizzarlo	• Per gli hostname che si risolvono solo all'interno del tuo VPC, per la comunicazione interna • Per mantenere privato lo schema di denominazione interno • Per semplificare la gestione delle risorse interne senza considerazioni DNS esterne	• Per accedere alle istanze su IPv4 e IPv6 da Internet • Per consentire una migrazione agevole da ambienti IPv4 a IPv6

Indice

- Hostname pubblici
- Hostname privati

Hostname pubblici

Puoi utilizzare gli hostname pubblici per accedere alle istanze EC2 utilizzando hostname che si risolvono all'indirizzo pubblico IPv4 o IPv6 dell'istanza e facilitano la transizione a IPv6.

Gli hostname pubblici consentono di:

- Accedere alle istanze EC2 sia su IPv4 che su IPv6, per una maggiore flessibilità nel modo in cui ti connetti alle risorse.
- Migrare da ambienti IPv4 a IPv6 in base alle esigenze. Puoi, ad esempio, disaccoppiare le migrazioni di database e applicazioni, riducendo la complessità e il rischio.
- Utilizza più opzioni di hostname (IPv4-only IPv6-only, e dual-stack) che si risolvono automaticamente negli indirizzi IP appropriati.

- Usufruisci di una maggiore sicurezza con il DNS split-horizon, che risolve gli hostname a indirizzi IP privati quando vengono richiesti dall'interno del tuo VPC.

Indice

- Tipi di hostname pubblici e quando utilizzarli
- Visualizzazione di hostname pubblici
- Modifica i tipi di hostname pubblici

Tipi di hostname pubblici e quando utilizzarli

Per utilizzare gli hostname pubblici, devi modificare un'interfaccia di rete esistente. Questa sezione descrive le tre opzioni relative al tipo di hostname pubblico e aiuta a decidere quale utilizzare:

- Dual-stack - Nome basato su IP
  - Questa è l'opzione migliore se stai migrando o intendi migrare da IPv4 a IPv6. Questa opzione consente la connettività sia su IPv4 che su IPv6, offrendo flessibilità ai client che potrebbero utilizzare entrambi i protocolli e consente ai client di mantenere lo stesso hostname durante la migrazione a IPv6.
  - Le richieste dall'interno del VPC vengono risolte sia all'indirizzo IPv4 privato che a IPv6 Global Unicast Address (GUA). Le richieste provenienti da Internet si risolvono sia all'indirizzo GUA IPv4 pubblico che all'indirizzo GUA IPv6 dell'interfaccia di rete.
  - Esempio
    - Quando scegli questa opzione, verrà generato un FQDN dual-stack per questa interfaccia di rete. Questo è un esempio del FQDN che verrà generato:
      - f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdp O.ap-southeast-2.ip.aws
    - Dove:
      - f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdpO è l'hostname che è una rappresentazione di base36 dell'indirizzo IPv6 pubblico primario (f5lnz-0khrm-nt2u3-gyqqt-nbdl5) sull'interfaccia di rete insieme a una rappresentazione di base36 dell'indirizzo IPv4 pubblico primario (q3cdpO) sull'interfaccia di rete.
      - f5lnz-0khrm-nt2u3-gyqqt-nbdl5 viene risolto dal resolver DNS Amazon all'indirizzo GUA IPv6. FFFF:1407:4:f000:81d:2689:1066:4489 Questo è il primo GUA IPv6 assegnato all'interfaccia di rete.

        - Q3CDpo viene risolto nell'indirizzo IPv4 di 52.54.55.56. Questo è l'indirizzo IPv4 pubblico collegato all'interfaccia di rete primaria.
        - ap-southeast-2 è la regione della sottorete in cui si trova l'interfaccia di rete.
        - ip.aws è il dominio fornito da. AWS
- IPv6 - Nome basato su IP
    - Questa è una buona opzione se hai già effettuato la migrazione a IPv6 e hai bisogno della connettività solo su IPv6.
    - Le richieste provenienti dall'interno del VPC o da Internet si risolvono all'indirizzo GUA IPv6 dell'interfaccia di rete.
    - Esempio
        - Quando scegli questa opzione, verrà generato un FQDN per questa interfaccia di rete. Questo è un esempio del FQDN che verrà generato:
            - f5lnz-0khrm-nt2u3-gyqqt-nbdl5.ap-southeast-2.ip.aws
        - Dove:
            - f5lnz-0khrm-nt2u3-gyqqt-nbdl5 è un hostname che è una rappresentazione in base36 dell'indirizzo IPv6 pubblico primario sull'interfaccia di rete.
            - f5lnz-0khrm-nt2u3-gyqqt-nbdl5 viene risolto dal resolver DNS Amazon nell'indirizzo GUA IPv6. FFFF:1407:4:f000:81d:2689:1066:4489 Questo è il primo GUA IPv6 assegnato all'interfaccia di rete.
            - ap-southeast-2 è la regione della sottorete in cui si trova l'interfaccia di rete.
            - ip.aws è il dominio fornito da. AWS
- IPv4 - Nome basato su IP
    - Questa è una buona opzione se l'istanza che utilizza questa interfaccia di rete deve mantenere l'accesso IPv4 durante la transizione a IPv6 o se le applicazioni o i sistemi in esecuzione sull'istanza supportano solo IPv4. Questa è l'opzione migliore se devi solo mantenere la connettività IPv4 e i tuoi carichi di lavoro non richiedono il supporto IPv6. Ad esempio, se stai effettuando la migrazione a IPv6, potresti decidere di mantenere alcune applicazioni su IPv4 mentre altre passano a IPv6.
    - Le richieste dall'interno del VPC si risolvono all'indirizzo IPv4 primario privato dell'interfaccia di rete. Le richieste provenienti da Internet si risolvono all'indirizzo IPv4 pubblico dell'interfaccia di rete.
    - Esempio

- Se scegli questa opzione, verrà generato un nome host IPv4-enabled pubblico per questa interfaccia di rete. Questo è un esempio del nome DNS che verrà generato:
  - ec2-52-54-55-66.ap-southeast-2.compute.amazonaws.com
- Dove:
  - ec2-52-54-55-66 è un nome host derivato dall'indirizzo IPv4 pubblico primario dell'interfaccia di rete, utilizzando il formato ec2- seguito dall'indirizzo IP con punti sostituiti da trattini.
  - ec2-52-54-55-66 si risolve nell'indirizzo IPv4 52.54.55.66. Questo è l'indirizzo IPv4 pubblico collegato all'interfaccia di rete primaria.
  - ap-southeast-2 è la regione della sottorete in cui si trova l'interfaccia di rete.
  - compute.amazonaws.com è il dominio fornito da for public AWS hostname IPv4-based .

> **Important**
>
> Negli esempi precedenti, puoi vedere che gli indirizzi IP vengono utilizzati per generare l'hostname. Se modifichi l'indirizzo IPv4 privato principale o il primo GUA IPv6 assegnato all'interfaccia di rete, la parte dell'hostname che si traduce nell'indirizzo IP cambierà e l'hostname pubblico generato in precedenza non sarà più valido. Inoltre, la modifica dell'indirizzo pubblico IPv4 primario impone un aggiornamento a valle del Servizio di metadati di istanza (IMDS) nella Guida per l'utente di Amazon EC2, quindi i metadati IMDS dell'istanza EC2 vengano aggiornati automaticamente.

Visualizzazione di hostname pubblici

Se il VPC in cui si trova l'interfaccia di rete non ha entrambi sia EnableDnsHostnames che EnableDnsSupport abilitati, non viene definito o generato alcun tipo di hostname.

Console

Puoi visualizzare gli hostname pubblici di un'istanza o di un'interfaccia di rete primaria.

Per visualizzare il tipo di hostname e i nomi DNS di un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona la casella di controllo relativa all'istanza.

4. Nella scheda Rete, in Hostname e DNS, trova quanto segue:

   - Tipo di hostname pubblico
   - DNS pubblico
   - IPv4-only Nome basato su IP
   - IPv6-only - Nome basato su IP
   - Dualstack: nome basato su IP

Per visualizzare il tipo di hostname e i nomi DNS di un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Interfacce di rete.
3. Nel campo di ricerca, inserisci l'ID dell'istanza. Seleziona l'ID dell'interfaccia di rete per aprirne la pagina dei dettagli.
4. In Hostname e DNS, trova quanto segue:

   - Tipo di hostname pubblico
   - Nome DNS pubblico
   - Nome DNS IPv4 pubblico
   - Nome DNS IPv6 pubblico
   - Nome DNS Dualstack pubblico

AWS CLI

Per visualizzare il tipo di hostname e i nomi DNS di un'interfaccia di rete

Utilizza il comando describe-network-interfaces.

```
aws ec2 describe-network-interfaces \
    --network-interface-id eni-1234567890abcdef0 \
    --query NetworkInterfaces[].PublicIpDnsNameOptions
```

Di seguito è riportato un output di esempio. Poiché il tipo di hostname è `public-dual-stack-dns-name`, l'hostname DNS è lo stesso di `PublicDualStackDnsName`.

```
[
```

```
    {
        "DnsHostnameType": "public-dual-stack-dns-name",
        "PublicIpv4DnsName": "ec2-52-54-55-66.ap-
southeast-2.compute.amazonaws.com",
        "PublicIpv6DnsName": "f5lnz-0khrm-nt2u3-gyqqt-nbdl5.ap-
southeast-2.ip.aws",
        "PublicDualStackDnsName": "f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdp0.ap-
southeast-2.ip.aws"
    }
]
```

PowerShell

Per visualizzare il tipo di hostname e i nomi DNS di un'interfaccia di rete

Utilizza il cmdlet Get-EC2NetworkInterface.

```
(Get-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0).PublicIpDnsNameOptions
```

Di seguito è riportato un output di esempio. Poiché il tipo di hostname è `public-dual-stack-dns-name`, l'hostname DNS è lo stesso di `PublicDualStackDnsName`.

```
DnsHostnameType        : public-dual-stack-dns-name
PublicDualStackDnsName : f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdp0.ap-southeast-2.ip.aws
PublicIpv4DnsName      : ec2-52-54-55-66.ap-southeast-2.compute.amazonaws.com
PublicIpv6DnsName      : f5lnz-0khrm-nt2u3-gyqqt-nbdl5.ap-southeast-2.ip.aws
```

Modifica i tipi di hostname pubblici

Le opzioni relative al tipo di hostname pubblico dipendono dagli indirizzi IP associati all'interfaccia di rete:

- Se l'interfaccia di rete ha solo un indirizzo IPv4 pubblico, il tipo di hostname deve essere IPv4 - Nome basato su IP.
- Se l'interfaccia di rete ha solo un indirizzo IPv6, il tipo di hostname deve essere IPv6 - Nome basato su IP.
- Se l'interfaccia di rete ha sia un indirizzo IPv4 pubblico che un indirizzo IPv6, il tipo di nome host può essere Dual-stack : nome basato su IP.

Prerequisiti

- L'interfaccia di rete deve avere un indirizzo IPv4 pubblico associato o un indirizzo IPv6.
- Il VPC in cui si trova l'interfaccia di rete deve avere EnableDnsHostnames e EnableDnsSupport abilitati. Consulta la sezione View and update DNS attributes for your VPC nella Guida per l'utente di Amazon VPC.

Console

Per modificare il tipo di hostname pubblico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Interfacce di rete.
3. Nel campo di ricerca, inserisci l'ID dell'istanza. Seleziona la casella di controllo relativa all'interfaccia di rete.

   In alternativa, dalla pagina dei dettagli dell'istanza, scegli la scheda Rete e seleziona l'ID dell'interfaccia di rete per l'indice 0 del dispositivo.
4. Scegli Azioni, Modifica il tipo di hostname pubblico.
5. Seleziona un'opzione:

   - Dual-stack - Nome basato su IP: un nome host pubblico dual-stack per un'interfaccia di rete. Le richieste dall'interno del VPC vengono risolte sia all'indirizzo IPv4 privato che a IPv6 Global Unicast Address. Le richieste provenienti da Internet si risolvono sia all'indirizzo GUA IPv4 pubblico che all'indirizzo GUA IPv6 dell'interfaccia di rete.
   - IPv4 - Nome basato su IP: un nome host IPv4-enabled pubblico per un'interfaccia di rete. Le richieste dall'interno del VPC si risolvono all'indirizzo IPv4 primario privato dell'interfaccia di rete. Le richieste provenienti da Internet si risolvono all'indirizzo IPv4 pubblico dell'interfaccia di rete.
   - IPv6 - Nome basato su IP: un nome host IPv6-enabled pubblico per un'interfaccia di rete. Le richieste provenienti dall'interno del VPC o da Internet si risolvono all'indirizzo GUA IPv6 dell'interfaccia di rete.
6. Scegli Modifica.

AWS CLI

Per modificare il tipo di hostname pubblico

Utilizza il comando modify-public-ip-dns-name-options.

```
aws ec2 modify-public-ip-dns-name-options \
    --network-interface-id eni-1234567890abcdef0 \
    --hostname-type public-dual-stack-dns-name
```

Di seguito è riportato un output di esempio.

```
{
    "Successful": true
}
```

PowerShell

Per modificare il tipo di hostname pubblico

Utilizza il cmdlet Edit-EC2PublicIpDnsNameOption.

```
Edit-EC2PublicIpDnsNameOption `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -HostNameType public-dual-stack-dns-name
```

Hostname privati

In questa sezione sono descritti i tipi di hostname privati dell'istanza di Amazon EC2 disponibili quando le istanze vengono avviate nelle sottoreti VPC.

L'hostname privato distingue le istanze EC2 sulla rete. Puoi utilizzare l'hostname privato di un'istanza se, ad esempio, desideri eseguire script per comunicare con alcune o tutte le istanze della rete.

Indice

- Tipi di hostname privati
- Dove trovare i nomi delle risorse e i nomi IP
- Scegliere tra nomi di risorse e nomi IP

- Modifica delle opzioni di denominazione basate sulle risorse per Amazon EC2

Tipi di hostname privati

Esistono due tipi di hostname privati per l'hostname del sistema operativo guest quando le istanze EC2 vengono avviate in un VPC:

- IP name (Nome IP): lo schema di denominazione legacy in cui, quando si avvia un'istanza, l'indirizzo IPv4 privato dell'istanza è incluso nel nome host dell'istanza. Il nome IP esiste per tutta la durata dell'istanza EC2. Se utilizzato come nome host DNS privato, restituirà solo l'indirizzo IPv4 privato (record A).
- Resource name (Nome risorsa): quando avvii un'istanza, il campo EC2 instance ID (ID istanza EC2) è incluso nel nome host dell'istanza. Il nome risorsa esiste per tutta la durata dell'istanza EC2. Se utilizzato come nome host DNS privato, può restituire sia l'indirizzo IPv4 privato (record A) che l'indirizzo Unicast globale IPv6 (record and/or AAAA).

Il nome host del sistema operativo guest dell'istanza EC2 dipende dalle impostazioni della sottorete:

- Se l'istanza viene avviata in una IPv4-only sottorete, è possibile selezionare il nome IP o il nome della risorsa.
- Se l'istanza viene avviata in una sottorete dual-stack (IPv4+IPv6), puoi selezionare il nome IP o il nome risorsa.
- Se l'istanza viene avviata in una IPv6-only sottorete, il nome della risorsa viene utilizzato automaticamente.

Indice

- Nome IP
- Nome risorsa
- Differenza tra nome IP e nome risorsa

Nome IP

Quando avvii un'istanza EC2 con Hostname type (Tipo di nome host) uguale a IP name (Nome IP), il nome host del sistema operativo guest è configurato per utilizzare l'indirizzo IPv4 privato.

- Formato per un'istanza in us-east-1: *`private-ipv4-address`*`.ec2.internal`

- Ad esempio: *ip-10-24-34-0*.ec2.internal
- Formato per un'istanza in qualsiasi altra AWS regione: *private-ipv4-address.region*.compute.internal
- Ad esempio: *ip-10-24-34-0.us-west-2*.compute.internal

Nome risorsa

Quando si avviano istanze EC2 nelle IPv6-only sottoreti, per impostazione predefinita viene selezionato il tipo Hostname del nome della risorsa. Quando avvii un'istanza in IPv4-only o sottoreti dual-stack (IPv4+IPv6), puoi selezionare il nome della risorsa. Dopo aver avviato un'istanza, puoi gestire la configurazione del nome host. Per ulteriori informazioni, consulta Modifica delle opzioni di denominazione basate sulle risorse per Amazon EC2.

Quando avvii un'istanza EC2 con Hostname type (Tipo di nome host) di Resource name (Nome risorsa), il nome host del sistema operativo guest è configurato per utilizzare l'ID dell'istanza EC2.

- Formato per un'istanza in us-east-1: *ec2-instance-id*.ec2.internal
- Ad esempio: *i-0123456789abcdef*.ec2.internal
- Formato AWS per un'istanza in qualsiasi altra regione: *ec2-instance-id.region*.compute.internal
- Ad esempio: *i-0123456789abcdef.us-west-2*.compute.internal

Differenza tra nome IP e nome risorsa

Le query DNS per i nomi IP e nomi risorsa coesistono per garantire la compatibilità con le versioni precedenti e consentire la migrazione dai nomi host basati su IP alla denominazione basata su risorse. Per i nomi host DNS privati basati su nomi IP, non è possibile configurare se una query di record DNS A per l'istanza riceve una risposta o meno. Le query del record DNS A ricevono sempre una risposta indipendentemente dalle impostazioni del nome host del sistema operativo guest.
Al contrario, per i nomi host DNS privati basati sul nome della risorsa, è possibile configurare se rispondere o meno alle query DNS AAAA and/or DNS DNS per l'istanza. È possibile configurare il comportamento della risposta quando si avvia un'istanza o si modifica una sottorete. Per ulteriori informazioni, consulta Modifica delle opzioni di denominazione basate sulle risorse per Amazon EC2.

Dove trovare i nomi delle risorse e i nomi IP

Puoi visualizzare i tipi di nome host, nome delle risorse e nome IP nella console Amazon EC2.

Indice

- Creazione di un'istanza EC2
- Quando si visualizzano i dettagli di un'istanza EC2 esistente

Creazione di un'istanza EC2

Quando crei un'istanza EC2, a seconda del tipo di sottorete selezionato, l'opzione Hostname type (Tipo di nome host) di Resource name (Nome risorsa) potrebbe essere disponibile oppure potrebbe essere selezionata e non modificabile. In questa sezione vengono descritti gli scenari in cui vengono visualizzati i tipi di nome host nome risorsa e nome IP.

Scenario 1

Crei un'istanza EC2 nella procedura guidata (vediAvviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console) e, quando configuri i dettagli, scegli una sottorete che hai configurato. IPv6-only

In questo caso, l'opzione Hostname type (Tipo di nome host) di Resource name (Nome risorsa) è selezionata automaticamente e non è modificabile. Le opzioni DNS Hostname (Nome host DNS) di Enable IP name IPv4 (A record) DNS requests (Abilita richieste DNS IPv4 [record A] basate sul nome IP) e di Enable resource-based IPv4 (A record) DNS requests (Abilita richieste DNS IPv4 [record A] basate sulle risorse) sono deselezionate automaticamente e non sono modificabili. L'opzione Enable resource-based IPv6 (AAAA record) DNS requests (Abilita richieste DNS IPv6 [record AAAA] basate sulle risorse) è selezionata di default ma è modificabile. Se l'opzione è selezionata, le richieste DNS al nome risorsa verranno risolte all'indirizzo IPv6 (record AAAA) di questa istanza EC2.

Scenario 2

Crea un'istanza EC2 nella procedura guidata (consulta la sezione Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console) e, quando configuri i dettagli, scegli una sottorete configurata con un intervallo CIDR IPv4 o un intervallo CIDR IPv4 e IPv6 ("dual stack").

L'opzione Enable IP name IPv4 (A record) DNS requests (Abilita richieste DNS IPv4 [record A] basate sul nome IP) è selezionata automaticamente e non può essere modificata. Ciò significa che le richieste al nome IP risolveranno l'indirizzo IPv4 (record A) di questa istanza EC2.

Le opzioni sono predefinite per le configurazioni della sottorete, ma puoi modificare le opzioni per l'istanza a seconda delle impostazioni della sottorete:

- Hostname type (Tipo di nome host): determina se desideri che il nome host del sistema operativo guest dell'istanza EC2 sia il nome risorsa o il nome IP. Il valore predefinito è IP name (Nome IP).
- Enable resource-based IPv4 (A record) DNS requests (Abilita richieste DNS IPv4 [record A] basate sulle risorse): determina se le richieste al nome risorsa vengono risolte con l'indirizzo IPv4 privato (record A) di questa istanza EC2. Questa opzione non è selezionata di default.
- Enable resource-based IPv6 (AAAA record) DNS requests (Abilita richieste DNS IPv6 [record AAAA] basate sulle risorse): determina se le richieste al nome risorsa vengono risolte con l'indirizzo GUA IPv6 (record AAAA) di questa istanza EC2. Questa opzione non è selezionata di default.

Quando si visualizzano i dettagli di un'istanza EC2 esistente

Puoi visualizzare i valori del nome host per un'istanza EC2 esistente nella scheda Details (Dettagli) dell'istanza EC2:

- Hostname type (Tipo di nome host): il nome host nel formato del nome IP o del nome risorsa.
- Private IP DNS name (IPv4 only) (Nome DNS IP privato [solo IPv4]): il nome IP che verrà sempre risolto all'indirizzo IPv4 privato dell'istanza.
- Private resource DNS name (Nome DNS risorsa privato): il nome risorsa che può essere risolto ai record DNS selezionati per l'istanza.
- Answer private resource DNS name (Rispondi al nome DNS delle risorse private): il nome risorsa risolve i record DNS IPv4 (A), IPv6 (AAAA) o IPv4 e IPv6 (A e AAAA).

Inoltre, se ti connetti all'istanza EC2 direttamente tramite SSH e inserisci il comando `hostname`, visualizzerai il nome host nel formato nome IP o nome risorsa.

Scegliere tra nomi di risorse e nomi IP

Quando avvii un'istanza EC2 (consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console), se scegli l'opzione Hostname type (Tipo di nome host) di Resource name (Nome risorsa), l'istanza EC2 viene avviata con un nome host nel formato del nome risorsa. In questi casi, anche il record DNS per l'istanza EC2 può indicare il nome risorsa. Ciò offre la flessibilità di scegliere se tale nome host si risolve all'indirizzo IPv4, all'indirizzo IPv6 o sia all'indirizzo IPv4 sia all'indirizzo IPv6 dell'istanza. Se prevedi di utilizzare IPv6 in futuro o se stai già utilizzando sottoreti dual-stack, è meglio usare l'opzione Hostname type (Tipo di nome host) di Resource name (Nome risorsa) in modo tale da modificare la risoluzione DNS per i nomi host delle istanze senza apportare modifiche ai record DNS stessi. Il nome risorsa consente di aggiungere e rimuovere la risoluzione DNS IPv4 e IPv6 su un'istanza EC2.

Se invece scegli un Hostname type (Tipo di nome host) di IP name (Nome IP) e lo utilizzi come nome host DNS, esso può risolvere solo all'indirizzo IPv4 dell'istanza. Non risolverà all'indirizzo IPv6 dell'istanza anche se all'istanza sono associati sia un indirizzo IPv4 sia un indirizzo IPv6.

Modifica delle opzioni di denominazione basate sulle risorse per Amazon EC2

Puoi modificare il tipo di nome host e le configurazioni del nome host DNS per le sottoreti, il che influisce su tutti i successivi lanci di istanze in quell'oggetto, oppure puoi modificarli per un'istanza EC2 dopo averla avviata.

Opzioni di denominazione basate su risorse

- Tipo di hostname: determina l'impostazione predefinita per il sistema operativo guest dell'istanza EC2 avviata nella sottorete. Si tratta del nome della risorsa o del nome IP.
- Abilita le richieste IPv4 (record A) del nome host DNS: determina se il DNS relativo requests/queries al nome della risorsa si risolve nell'indirizzo IPv4 privato (record A) dell'istanza EC2.
- Abilita le richieste IPv6 (record AAAA) del nome host DNS: determina se il requests/queries DNS relativo al nome della risorsa si risolve nell'indirizzo IPv6 (record AAAA) dell'istanza EC2.

Sottoreti

La modifica delle impostazioni della sottorete non modifica la configurazione delle istanze EC2 già avviate nella sottorete.

Console

Per modificare le opzioni per una sottorete

Apri la console Amazon VPC e seleziona la sottorete. Scegli Operazioni, Modifica impostazioni della sottorete. Modifica le impostazioni in base alle esigenze e poi salva le modifiche.

AWS CLI

Per modificare le opzioni per una sottorete

Utilizza il comando modify-subnet-attribute.

```
aws ec2 modify-subnet-attribute \
    --subnet-id subnet-0abcdef1234567890 \
    --private-dns-hostname-type-on-launch resource-name \
    --enable-resource-name-dns-a-record-on-launch \
```

```
    --enable-resource-name-dns-aaaa-record-on-launch
```

PowerShell

Per modificare le opzioni per una sottorete

Utilizza il cmdlet Edit-EC2SubnetAttribute.

```
Edit-EC2SubnetAttribute `
    -SubnetId subnet-0abcdef1234567890 `
    -PrivateDnsHostnameTypeOnLaunch ResourceName `
    -EnableResourceNameDnsAAAARecordOnLaunch $true `
    -EnableResourceNameDnsARecordOnLaunch $true
```

Istanze EC2

Considerazioni

- Per modificare il tipo di hostname, devi prima arrestare l'istanza. Non è necessario interrompere un'istanza per modificare le altre due opzioni.
- Poiché non è possibile arrestare un'istanza con un volume root di archivio dell'istanza, puoi configurare il tipo di hostname e le opzioni dell'hostname DNS solo all'avvio dell'istanza. Solo i seguenti tipi di istanza supportano volumi root dell'archivio dell'istanza: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

Console

Per modificare le opzioni del tipo di hostname e dell'hostname DNS per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Se hai intenzione di modificare l'impostazione Use resource based naming as guest OS hostname (Usa denominazione basata sulle risorse come nome host del sistema operativo guest), prima devi arrestare l'istanza EC2. In caso contrario, puoi ignorare questo passaggio.

   Per arrestare l'istanza, selezionare l'istanza e scegliere Instance state (Stato istanza), Stop instance (Arresta istanza).
3. Selezionare l'istanza, quindi scegliere Actions (Operazioni), Instance settings (Impostazioni dell'istanza), Change resource based naming options (Modifica delle opzioni di denominazione basate sulle risorse).

- Use resource based naming as guest OS hostname (Usa denominazione basata sulle risorse come nome host del sistema operativo guest): determina se desideri che il nome host del sistema operativo guest dell'istanza EC2 sia il nome risorsa o il nome IP.
- Rispondi alle richieste IPv4 (record A) del nome host DNS: determina se il DNS del nome della risorsa si risolve nell' requests/queries indirizzo IPv4 privato di questa istanza EC2.
- Rispondi alle richieste di nome host DNS IPv6 (record AAAA): determina se il DNS del nome della risorsa viene risolto nell'indirizzo IPv6 (record AAAA) requests/queries di questa istanza EC2.

4. Scegli Save (Salva).
5. Dopo aver arrestato l'istanza, avviarla di nuovo.

AWS CLI

Per modificare le opzioni del tipo di hostname e dell'hostname DNS per un'istanza

Utilizza il comando modify-private-dns-name-options.

```
aws ec2 modify-private-dns-name-options \
    --instance-id i-1234567890abcdef0 \
    --private-dns-hostname-type resource-name \
    --enable-resource-name-dns-a-record \
    --enable-resource-name-dns-aaaa-record
```

PowerShell

Per modificare le opzioni del tipo di hostname e dell'hostname DNS per un'istanza

Utilizza il cmdlet Edit-EC2PrivateDnsNameOption.

```
Edit-EC2PrivateDnsNameOption `
    -InstanceId i-1234567890abcdef0 `
    -PrivateDnsHostnameType ResourceName `
    -EnableResourceNameDnsAAAARecord $true`
    -EnableResourceNameDnsARecord $true
```

Trasferire i propri indirizzi IP (BYOIP) in Amazon EC2

È possibile trasferire una parte o tutto l'intervallo di indirizzi IPv4 o IPv6 indirizzabili pubblicamente dalla rete on-premises al proprio account Account AWS. Continui a controllare l'intervallo di indirizzi e puoi pubblicizzare l'intervallo di indirizzi su Internet tramite AWS. Dopo aver importato l'intervallo di indirizzi in Amazon EC2, questo viene visualizzato nel tuo Account AWS pool di indirizzi.

> **Note**
>
> Questa documentazione descrive come portare il proprio intervallo di indirizzi IP da utilizzare solo in Amazon EC2. Per inserire il tuo intervallo di indirizzi IP da utilizzare AWS Global Accelerator, consulta Bring your own IP address (BYOIP) nella Developer Guide. AWS Global Accelerator Per utilizzare il tuo intervallo di indirizzi IP Amazon VPC IP Address Manager, consulta il Tutorial: Bring your IP address to IPAM nella Amazon VPC IPAM User Guide.

Quando inserisci un intervallo di indirizzi IP a AWS, AWS verifica che tu controlli l'intervallo di indirizzi IP. Esistono due metodi da utilizzare per verificare il controllo dell'intervallo:

- Se il tuo intervallo di indirizzi IP è registrato in un registro Internet che supporta RDAP (come ARIN, RIPE e APNIC), puoi verificare il controllo del tuo dominio con un X.509 certificato utilizzando la procedura descritta in questa pagina. Il certificato deve essere valido solo per la durata del processo di provisioning. È possibile rimuovere il certificato dal record dei Regional Internet Registry (RIR) dopo aver completato il provisioning.
- Indipendentemente dal fatto che il registro internet supporti RDAP, è possibile utilizzare IPAM di Amazon VPC per verificare il controllo del dominio con un record TXT DNS. La procedura è documentata in Tutorial: trasferisci i tuoi indirizzi IP su IPAM nella Guida per l'utente di IPAM di Amazon VPC.

Per ulteriori informazioni, consulta l' AWS Online Tech Talk Deep Dive su Bring Your Own IP.

Indice

- Definizioni BYOIP
- Requisiti e quote
- Disponibilità regionale

- Disponibilità delle zone locali
- Prerequisiti di BYOIP in Amazon EC2
- Onboarding dell'intervallo di indirizzi da utilizzare in Amazon EC2
- Utilizzo dell'intervallo di indirizzi BYOIP in Amazon EC2

Definizioni BYOIP

- X.509 Self-sign certificato: uno standard di certificato più comunemente utilizzato per crittografare e autenticare i dati all'interno di una rete. È un certificato utilizzato da per AWS convalidare il controllo sullo spazio IP da un record RDAP. Per ulteriori informazioni sui X.509 certificati, vedere RFC 3280.
- Autonomous System Number (ASN): identificatore univoco globale che definisce un gruppo di prefissi IP gestiti da uno o più operatori di rete che mantengono un'unica policy di instradamento chiaramente definita.
- Registro Internet regionale (RIR): un'organizzazione che gestisce l'allocazione e la registrazione di indirizzi IP e ASN in una regione del mondo.
- Registry Data Access Protocol (RDAP): un protocollo di sola lettura per interrogare i dati di registrazione correnti all'interno di un RIR. Le voci all'interno del database RIR interrogato vengono denominate "record RDAP". Alcuni tipi di record devono essere aggiornati dai clienti tramite un RIR-provided meccanismo. Questi record vengono interrogati AWS per verificare il controllo di uno spazio di indirizzi nel RIR.
- Autorizzazione origine percorso (ROA): un oggetto creato dai RIR per i clienti allo scopo di autenticare la pubblicità IP, in sistemi autonomi particolari. Per una panoramica, consulta Route Origin Authorizations (ROAs) sul sito Web ARIN.
- Registro Internet locale (LIR): organizzazioni come i provider di servizi Internet che allocano un blocco di indirizzi IP da un RIR per i propri clienti.

Requisiti e quote

- L'intervallo di indirizzi deve essere registrato presso il Regional Internet Registry (RIR) personale. Consultare il RIR per eventuali policy relative alle aree geografiche. Il BYOIP attualmente supporta la registrazione nell'American Registry for Internet Numbers (ARIN), nel Réseaux IP Européens Network Coordination Centre (RIPE) o nel Network Information Centre (APNIC). Asia-Pacific Deve

essere registrato in un'entità aziendale o istituzionale e non può essere registrato per una persona fisica.

- L'intervallo di indirizzi IPv4 più specifico che puoi portare è /24.
- L'intervallo di indirizzi IPv6 più specifico che puoi inserire è /48 per i CIDR pubblicizzati pubblicamente e /60 per i CIDR che non lo sono. ???
- I ROA non sono richiesti per gli intervalli CIDR che non sono pubblicizzabili pubblicamente, ma i record RDAP devono ancora essere aggiornati.
- È possibile raggruppare ogni intervallo di indirizzi in una regione alla volta. AWS
- Puoi aggiungere al tuo account un totale di cinque intervalli di indirizzi BYOIP IPv4 e IPv6 per regione. AWS AWS Non è possibile modificare le quote per i CIDR BYOIP utilizzando la console Service Quotas, ma è possibile richiedere un aumento delle quote contattando il Centro assistenza come descritto nelle quote di servizio nella. AWS AWS Riferimenti generali di AWS
- Non puoi condividere il tuo intervallo di indirizzi IP con altri account utilizzando a AWS RAM meno che non utilizzi Amazon VPC IP Address Manager (IPAM) e integri l'IPAM con le organizzazioni. AWS Per ulteriori informazioni, consulta Integrare l'IPAM con AWS le organizzazioni nella Amazon VPC IPAM User Guide.
- Gli indirizzi nell'intervallo di indirizzi IP deve avere una cronologia pulita. È opportuno esaminare la reputazione dell'intervallo di indirizzi IP e riservarti il diritto di rifiutare un intervallo di indirizzi IP se contiene un indirizzo IP che ha scarsa reputazione o è associato a un comportamento dannoso.
- Lo spazio di indirizzi legacy, ovvero lo spazio di indirizzi IPv4 distribuito dal registro centrale della Internet Assigned Numbers Authority (IANA) prima della formazione del sistema Regional Internet Registry (RIR), richiede ancora un oggetto ROA corrispondente.
- Per i LIR, è comune che usino un processo manuale per aggiornare i record. L'implementazione può richiedere giorni, a seconda del LIR.
- Per un blocco CIDR di grandi dimensioni sono necessari un singolo oggetto ROA e un record RDAP. Puoi trasferire più blocchi CIDR più piccoli da quell'intervallo a AWS, anche tra più AWS regioni, utilizzando un singolo oggetto e record.
- Il BYOIP non è supportato per le zone di lunghezza d'onda o attive. AWS Outposts
- Non apportare modifiche manuali al BYOIP nel RADb o in qualsiasi altro IRR. Il BYOIP aggiornerà automaticamente il RADb. Qualsiasi modifica manuale che includa l'ASN BYOIP causerà un errore nell'operazione di provisioning del BYOIP.
- Dopo aver inserito un intervallo di indirizzi IPv4 AWS, è possibile utilizzare tutti gli indirizzi IP dell'intervallo, incluso il primo indirizzo (l'indirizzo di rete) e l'ultimo indirizzo (l'indirizzo di trasmissione).

Disponibilità regionale

La funzionalità BYOIP è attualmente disponibile in tutte le regioni AWS commerciali ad eccezione delle regioni cinesi.

Disponibilità delle zone locali

Una zona locale è un'estensione di una AWS regione in prossimità geografica degli utenti. Le zone locali sono raggruppate in "gruppi di confini di rete". In AWS, un gruppo di confini di rete è un insieme di zone di disponibilità (AZ), zone locali o zone di lunghezza d'onda da cui AWS pubblicizza un indirizzo IP pubblico. Le zone locali possono avere gruppi di confini di rete diversi rispetto alle AZ di una AWS regione per garantire una latenza o una distanza fisica minima tra la AWS rete e i clienti che accedono alle risorse in tali zone.

Puoi eseguire il provisioning di intervalli di indirizzi BYOIPv4 e pubblicizzarli nei seguenti gruppi di confini di rete di zone locali utilizzando l'opzione `--network-border-group`:

- af-south-1-los-1
- ap-northeast-1-tpe-1
- ap-south-1-ccu-1
- ap-south-1-del-1
- ap-southeast-1-bkk-1
- ap-southeast-1-mnl-1
- ap-southeast-2-akl-1
- ap-southeast-2-per-1
- eu-central-1-ham-1
- eu-central-1-ist-1
- eu-central-1-waw-1
- eu-north-1-cph-1
- eu-north-1-hel-1
- me-south-1-mct-1
- us-east-1-atl-2
- us-east-1-bos-1
- us-east-1-bue-1
- us-east-1-chi-2

- us-east-1-dfw-2
- us-east-1-iah-2
- us-east-1-lim-1
- us-east-1-mci-1
- us-east-1-mia-2
- us-east-1-msp-1
- us-east-1-nyc-1
- us-east-1-nyc-2
- us-east-1-phl-1
- us-east-1-qro-1
- us-east-1-scl-1
- us-west-2-den-1
- us-west-2-hnl-1
- us-west-2-las-1
- us-west-2-lax-1
- us-west-2-pdx-1
- us-west-2-phx-2
- us-west-2-sea-1

Se hai abilitato delle zone locali (consulta Enable a Local Zone), puoi scegliere un gruppo di confine di rete per le zone locali quando effettui il provisioning e pubblicizzi un CIDR BYOIPv4. Scegliete attentamente il gruppo di confini di rete come EIP e la AWS risorsa a cui è associata deve risiedere nello stesso gruppo di confini di rete.

> **Note**
>
> Al momento non è possibile effettuare il provisioning o pubblicizzare intervalli di indirizzi BYOIPv6 nelle zone locali, ad eccezione di, che supporta sia BYOIPv4 che BYOIPv6. `eu-central-1-ist-1`

Nella zona `eu-central-1-ist-1` locale, la pubblicità e il prelievo sono operazioni asincrone il cui completamento può richiedere fino a cinque giorni lavorativi. Quando pubblicizzi un intervallo di

indirizzi, il suo stato cambia da `provisioned` a `pending-advertising`, quindi a `advertised` dopo il completamento dell'operazione. Quando lo ritiri, lo stato cambia da `advertised` a `pending-withdrawal`, poi di nuovo a. `provisioned` Puoi monitorare lo stato di avanzamento di queste operazioni tramite la AWS Console o la CLI.

Se utilizzi il tuo codice ASN (BYOASN), puoi specificarlo quando pubblicizzi il tuo intervallo di indirizzi. Non è possibile modificare l'ASN associato al CIDR dopo l'annuncio. Per modificare l'ASN, ritira il CIDR e ripeti la pubblicità.

> **Important**
>
> Non è possibile annullare un annuncio o un prelievo in sospeso. È necessario attendere il completamento dell'operazione prima di iniziare l'operazione successiva.

Prerequisiti di BYOIP in Amazon EC2

Il processo di onboarding per BYOIP prevede due fasi, per le quali è necessario eseguire tre passaggi. Questi passaggi corrispondono ai passaggi descritti nel diagramma seguente. In questa documentazione sono inclusi i passaggi manuali; tuttavia, per aiutarti a eseguire questi passaggi, è possibile che il tuo RIR offra servizi gestiti.

> **Tip**
>
> Le attività in questa sezione richiedono un terminale Linux e possono essere eseguite utilizzando Linux AWS CloudShell, o il sottosistema Windows per Linux.

Indice

- Panoramica di
- Crea una chiave privata e genera un certificato X.509
- Carica il X.509 certificato nel record RDAP del tuo RIR
- Creazione di un oggetto ROA nel RIR

Panoramica di

Fase di preparazione

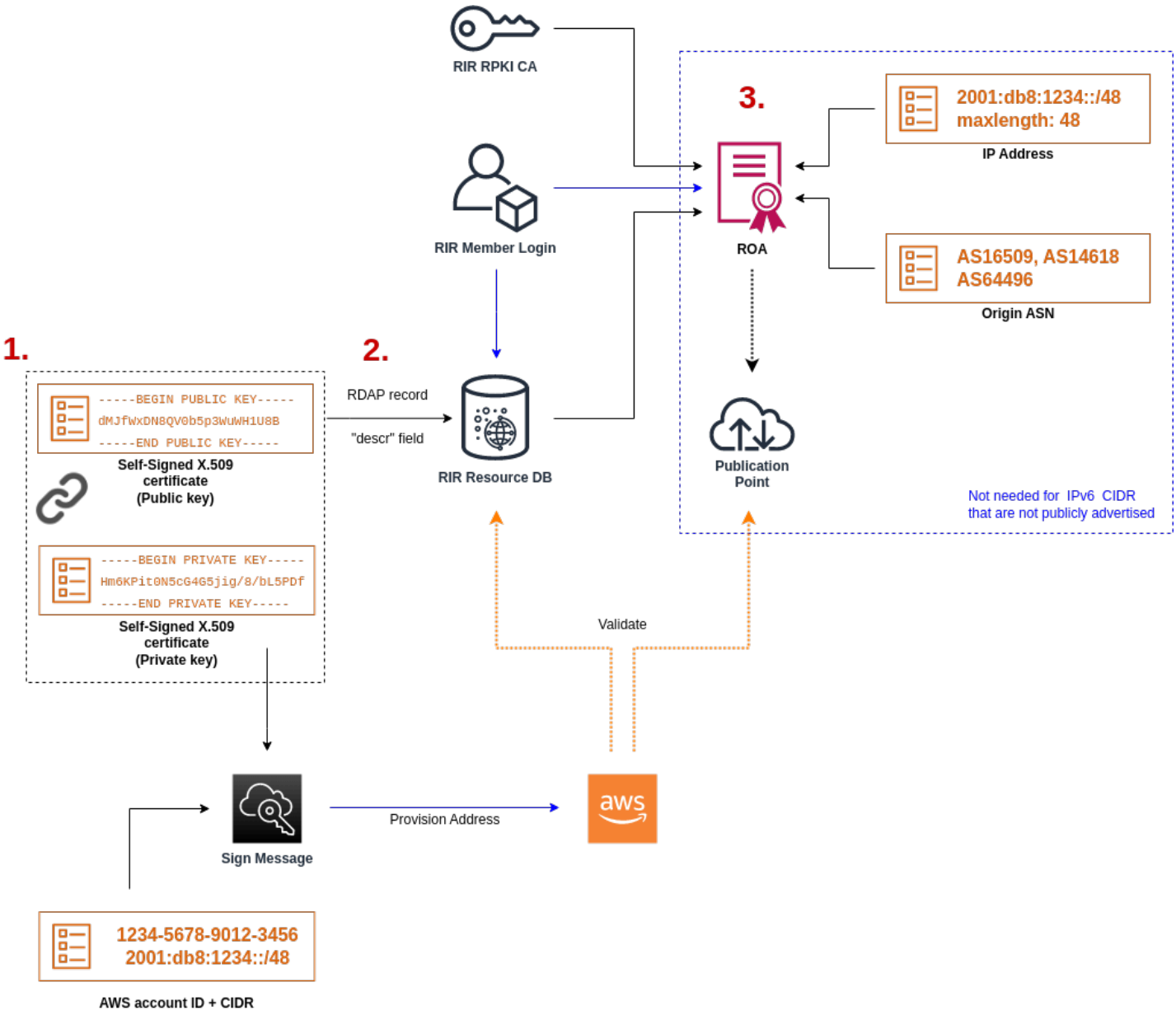
[1] Crea una chiave privata e usala per generare un X.509 certificato autofirmato per scopi di autenticazione. Questo certificato viene utilizzato solo durante la fase di provisioning. È possibile rimuovere il certificato dal record dei Regional Internet Registry (RIR) dopo aver completato il provisioning

Fase di configurazione RIR

[2] Carica il certificato autofirmato nei commenti dei record RDAP.

[3] Crea un oggetto ROA nel RIR. Il ROA definisce l'intervallo di indirizzi desiderato, i numeri ASN (Autonomous System Number) (ASN) autorizzati a pubblicizzare l'intervallo di indirizzi e una data di scadenza da registrare con l'RPKI (Resource Public Key Infrastructure) del tuo RIR.

> **Note**
>
> Non è richiesto un ROA per lo spazio di indirizzi IPv6 non pubblicizzabile pubblicamente.



Per attivare più intervalli di indirizzi non contigui, devi ripetere questo processo con ogni intervallo di indirizzi. Tuttavia, non è necessario ripetere le fasi di preparazione e configurazione RIR se si divide un blocco contiguo in diverse regioni. AWS

L'attivazione di un intervallo di indirizzi non ha alcun effetto sugli intervalli di indirizzi attivati in precedenza.

Crea una chiave privata e genera un certificato X.509

Utilizzate la procedura seguente per creare un X.509 certificato autofirmato e aggiungerlo al record RDAP per il vostro RIR. Questa coppia di chiavi viene utilizzata per autenticare l'intervallo di indirizzi con il RIR. I comandi openssl richiedono OpenSSL versione 1.0.2 o successive.

Copia i comandi seguenti e sostituisci solo i valori segnaposto (testo in corsivo colorato).

Questa procedura segue le best practice per crittografare la chiave RSA privata e richiedere una passphrase per accedervi.

1. Genera una chiave privata RSA a 2048 bit come segue.

```
$ openssl genpkey -aes256 -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out
 private-key.pem
```

Il parametro `-aes256` specifica l'algoritmo utilizzato per crittografare la chiave privata. Il comando restituisce l'output seguente, inclusi i prompt per impostare una passphrase:

```
......+++
.+++
Enter PEM pass phrase: xxxxxxx
Verifying - Enter PEM pass phrase: xxxxxxx
```

Puoi scaricare la chiave pubblica utilizzando il comando seguente:

```
$ openssl pkey -in private-key.pem -text
```

Questo restituisce un prompt della passphrase e il contenuto della chiave, che deve essere simile al seguente:

```
Enter pass phrase for private-key.pem: xxxxxxx
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDFBXHRI4HVKAhh
3seiciooizCRTbJe1+YsxNTja4XyKypVGIFWDGhZs44FCHlPOOSVJ+NqP74w96oM
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zHOSEpNmY2fMxISBxewlxR
FAniwmSd/8TDvHJMY9FvAIvWuTsv5l0tJKk+a91K4+tO3UdDR7Sno5WXExfsBrW3
g1ydo3TBsx8i5/YiVOcNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRsOlAhJ
DnZPNeweboo+K3Q3lwbgbmOKD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrMSn2
BzsPVuDLAgMBAAECggEACiJUj2hfJkKv47Dc3es3Zex67A5uDVjXmxfox2Xhdupn
```

```
fAcNqAptV6fXt0SPUNbhUxbBKNbshoJGufFwXPli1SXnpzvkdU4Hyco4zgbhXFsE
RNYjYfOGzTPwdBLpNMB6k3Tp4RHse6dNrlH0jDhpioL8cQEBdBJyVF5X0wymEbmV
mC0jgH/MxsBAPWW6ZKicg9ULMlWiAZ3MRAZPjHHgpYkAAsUWKAbCBwVQcVjGO59W
jfZjzTX5pQtVVH68ruciH88DTZCwjCkjBhxg+OIkJBLE5wkh82jIHSivZ63flwLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQKBgQDjwlC/3jxp8zJy6P8o
JQKv7TdvMwUj4VSWOHZBHLv4evJaaia0uQjIo1UDa8AYitqhX1NmCCehGH8yuXj/
v6V3CzMKDkmRr1NrONnSz5QsndQ04Z6ihAQlPmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEvONK+xwUKzi9c
L/OzBq5yOIC1Pz2T85gOe1i8kwZws+xlpG6uBT6lmIJELd0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGeOBohmF0phTHkrWKBxXiyT0oS8zjnJlEn8ysIpGgO28jjr
LpaHNZ/MXQKBgQDfLNcnS0LzpsS2aK0tzyZU8SMyqVHOGMxj7quhneBq2T6FbiLD
T9TVlYaGNZ0j71vQaLI19qOubWymbautH0Op5KV8owdf4+bf1/NJaPIOzhDUSIjD
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycaAW9lItu8aBrMndnQKBgQDb
nNp/JyRwqjOrNljk7DHEs+SD39kHQzzCfqd+dnTPv2sc06+cpym3yulQcbokULpy
fmRo3bin/pvJQ3aZX/Bdh9woTXqhXDdrrSwWInVYMQPyPk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtixlWtheKRYkQmzQZXbWdIhYyI3QKBgD+F/6wcZ85QW8nAUykA
3WrSIx/3cwDGdm4NRGct8ZOZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUt7bNK0AUVLh
dMJfWxDN8QV0b5p3WuWH1U8B
-----END PRIVATE KEY-----
Private-Key: (2048 bit)
modulus:
    00:c5:05:71:d1:23:81:d5:28:08:61:de:c7:a2:72:
    2a:28:8b:30:91:4d:b2:5e:d7:e6:2c:c4:d4:e3:6b:
    85:f2:2b:2a:55:18:81:56:0c:68:59:b3:8e:05:08:
    79:4f:38:e4:95:27:e3:6a:3f:be:30:f7:aa:0c:ec:
    33:d2:df:1a:3d:91:a4:32:64:11:67:d9:81:29:d8:
    40:6a:e6:f7:f7:d3:b2:87:35:19:99:65:49:a4:9f:
    4c:c7:39:21:29:36:66:36:7c:cc:48:48:1c:5e:c2:
    5c:51:14:09:e2:c2:64:9d:ff:c4:c3:bc:72:4c:63:
    d1:6f:00:8b:d6:b9:3b:2f:e6:5d:2d:24:a9:3e:6b:
    dd:4a:e3:eb:4e:dd:47:43:47:b4:a7:a3:95:97:13:
    17:ec:06:b5:b7:83:5c:9d:a3:74:c1:b3:1f:22:e7:
    f6:22:54:e7:0d:02:9c:bb:81:ed:bf:16:2c:18:dd:
    a0:97:24:1e:ab:ea:7b:85:e8:7f:26:46:02:38:af:
    8b:e4:31:1b:0e:94:08:49:0e:76:4f:35:ec:1e:6e:
    8a:3e:2b:74:37:97:06:e0:6e:63:8a:0f:fc:fd:b2:
    f9:3c:37:ff:a1:51:30:6d:21:7d:1f:46:d6:c6:f8:
    f2:c8:c3:7c:56:44:71:ab:31:29:f6:07:3b:0f:56:
    e0:cb
publicExponent: 65537 (0x10001)
privateExponent:
    0a:22:54:8f:68:5f:26:42:af:e3:b0:dc:dd:eb:37:
    65:ec:7a:ec:0e:6e:0d:58:d7:9b:17:e8:c7:65:e1:
```

```
    76:ea:67:7c:07:0d:a8:0a:6d:57:a7:d7:b7:44:8f:
    50:d6:e1:53:16:c1:28:d6:ec:86:82:46:b9:f1:70:
    5c:f9:62:d5:25:e7:a7:3b:e4:75:4e:07:c9:ca:38:
    ce:06:e1:5c:5b:04:44:d6:23:61:f3:86:cd:33:f0:
    74:12:e9:34:c0:7a:93:74:e9:e1:11:ec:7b:a7:4d:
    ae:51:f4:8c:38:69:8a:82:fc:71:01:01:74:12:72:
    54:5e:57:d3:0c:a6:11:b9:95:98:2d:23:80:7f:cc:
    c6:c0:40:3d:65:ba:64:a8:9c:83:d5:0b:32:55:a2:
    01:9d:cc:44:06:4f:8c:71:e0:a5:89:00:02:c5:16:
    28:06:c2:07:05:50:71:58:c6:3b:9f:56:8d:f6:63:
    cd:35:f9:a5:0b:55:54:7e:bc:ae:e7:22:1f:cf:03:
    4d:90:b0:8c:29:23:06:1c:60:f8:e2:24:24:12:c4:
    e7:09:21:f3:68:c8:1d:28:af:67:ad:df:97:02:f0:
    cf:e1:34:f8:78:44:2d:26:49:ae:7d:8c:63:a2:71:
    9a:29:37:a8:d3:54:38:5f:d9:fb:79:ac:76:3d:a5:
    b9
prime1:
    00:e3:c2:50:bf:de:3c:69:f3:32:72:e8:ff:28:25:
    02:af:ed:37:6f:33:05:23:e1:54:96:38:76:41:1c:
    bb:f8:7a:f2:5a:6a:26:b4:b9:08:c8:a3:55:03:6b:
    c0:18:8a:da:a1:5f:53:66:08:27:a1:18:7f:32:b9:
    78:ff:bf:a5:77:0b:33:0a:0e:49:91:af:53:6b:38:
    d9:d2:cf:94:2c:9d:d4:34:e1:9e:a2:84:04:25:3e:
    62:7d:ea:0e:30:2a:d8:28:0b:b0:18:a7:23:f4:83:
    56:be:e3:fb:23:6f:5f:a8:dd:84:08:e2:90:ff:17:
    bd:5c:fa:a6:b3:b4:7e:cf:47
prime2:
    00:dd:73:6d:f2:36:64:f7:f8:9c:a9:b5:fd:1f:2a:
    31:2f:38:d2:be:c7:05:0a:ce:2f:5c:2f:f3:b3:06:
    ae:72:38:80:b5:3f:3d:93:f3:98:0e:7b:58:bc:93:
    06:70:b3:ec:65:a4:6e:ae:05:3e:a5:98:82:44:2d:
    dd:24:e7:d1:72:ba:93:6e:e1:d3:ef:5f:94:83:e8:
    61:aa:77:1e:23:93:d2:af:23:be:2e:b0:67:8e:06:
    88:66:17:4a:61:4c:79:2b:58:a0:71:5e:2c:93:d2:
    84:bc:ce:39:c9:94:49:fc:ca:c2:29:1a:03:b6:f2:
    38:eb:2e:96:87:35:9f:cc:5d
exponent1:
    00:df:2c:d7:27:4b:42:f3:a6:c4:b6:68:ad:2d:cf:
    26:54:f1:23:32:a9:51:ce:18:cc:63:ee:ab:a1:9d:
    e0:6a:d9:3e:85:6e:22:c3:4f:d4:d5:95:86:86:35:
    9d:23:ef:5b:d0:68:b2:35:f6:a3:ae:6d:6c:a6:6d:
    ab:ad:1f:43:a9:e4:a5:7c:a3:07:5f:e3:e6:df:d7:
    f3:49:68:f2:0e:ce:10:d4:48:88:c3:42:8d:35:59:
    6d:f5:67:d5:c3:49:18:4a:15:39:d6:ce:60:a3:05:
```

```
    d7:88:71:a8:f2:cd:fd:74:60:ab:32:71:a0:16:f6:
    52:2d:bb:c6:81:ac:c9:dd:9d
exponent2:
    00:db:9c:da:7f:27:24:70:aa:33:ab:36:58:e4:ec:
    31:c4:b3:e4:83:df:d9:07:43:3c:c2:7e:a7:7e:76:
    74:cf:bf:6b:1c:d3:af:9c:a7:29:b7:ca:e9:50:71:
    ba:24:50:ba:72:7e:64:68:dd:b8:a7:fe:9b:c9:43:
    76:99:5f:f0:5d:87:dc:28:4d:7a:a1:5c:37:6b:ad:
    2c:16:22:75:58:31:03:f2:3e:4f:1f:fc:3f:66:20:
    e2:69:e4:55:16:33:01:c3:53:ec:21:21:94:b1:b0:
    47:84:fa:3b:62:c6:55:ad:85:e2:91:62:44:26:cd:
    06:57:6d:67:48:85:8c:88:dd
coefficient:
    3f:85:ff:ac:1c:67:ce:50:5b:c9:c0:53:29:00:dd:
    6a:d2:23:1f:f7:73:00:c6:76:6e:0d:44:67:2d:f1:
    93:99:8d:31:e3:8b:2f:68:8c:c3:83:d4:be:e2:32:
    14:50:ff:79:37:85:4b:22:9f:92:c3:32:9f:eb:c9:
    61:86:c7:8b:88:68:b6:ad:e3:49:22:0b:b4:f8:23:
    ae:83:33:b3:f9:f5:eb:aa:77:3d:f0:d0:f0:fe:55:
    4f:a1:ec:64:a2:be:fb:05:0d:dc:92:52:de:db:34:
    ad:00:51:52:e1:74:c2:5f:5b:10:cd:f1:05:74:6f:
    9a:77:5a:e5:87:d5:4f:01
```

Custodisci la tua chiave privata in un luogo sicuro quando non è in uso.

2. Genera un X.509 certificato utilizzando la chiave privata creata nel passaggio precedente. In questo esempio, il certificato scade tra 365 giorni; dopo tale data diventa inaffidabile. Assicurarsi di impostare la scadenza in modo appropriato. Il certificato deve essere valido solo per la durata del processo di provisioning. È possibile rimuovere il certificato dal record dei Regional Internet Registry (RIR) dopo aver completato il provisioning. Il comando `tr -d "\n"` rimuove i caratteri di nuova riga (interruzioni di riga) dall'output. Quando richiesto, è necessario fornire un nome comune, ma gli altri campi possono essere lasciati vuoti.

```
$ openssl req -new -x509 -key private-key.pem -days 365 | tr -d "\n" >
 certificate.pem
```

Viene restituito un output simile al seguente:

```
Enter pass phrase for private-key.pem: xxxxxxx
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:example.com
Email Address []:
```

> **Note**
>
> Il nome comune non è necessario per il AWS provisioning. Può essere qualsiasi nome di dominio interno o pubblico.

Puoi verificare il certificato utilizzando il comando seguente:

```
$ cat certificate.pem
```

L'output deve essere una PEM-encoded stringa lunga senza interruzioni di riga, preceduta da `-----BEGIN CERTIFICATE-----` e seguita da. `-----END CERTIFICATE-----`

Carica il X.509 certificato nel record RDAP del tuo RIR

Aggiungere il certificato creato in precedenza al record RDAP per il RIR. Assicurati di includere le stringhe `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` prima e dopo la porzione codificata. Tutto questo contenuto deve trovarsi su un'unica linea lunga. La procedura per l'aggiornamento di RDAP dipende dal RIR:

- Per ARIN, utilizza il portale Account Manager per aggiungere il certificato nella sezione "Commenti pubblici" per l'oggetto "Informazioni di rete" che rappresenta l'intervallo di indirizzi. Non aggiungerlo alla sezione commenti dell'organizzazione.
- Per RIPE, aggiungi il certificato come nuovo campo "descr" all'oggetto "inetnum" o "inet6num" che rappresenta il tuo intervallo di indirizzi. Di solito si trovano nella sezione "Le mie risorse" del portale

del database RIPE. Non aggiungerlo alla sezione commenti della tua organizzazione o al campo "commenti" degli oggetti sopra indicati.

- Per APNIC, aggiungi il certificato modificando le osservazioni nel record “inetnum” o “inet6num”.

Puoi rimuovere il certificato dal record dei Registri Internet Regional (RIR) dopo aver completato la fase di provisioning riportata di seguito.

Creazione di un oggetto ROA nel RIR

Crea un oggetto ROA per autorizzare Amazon ASN 16509 e 14618 a pubblicizzare l'intervallo di indirizzi, così come gli ASN che sono attualmente autorizzati a pubblicizzare l'intervallo di indirizzi. Per il AWS GovCloud (US) Regions, autorizza solo l'ASN 8987. Per lo AWS European Sovereign Cloud, autorizza gli ASN 16509 e 214101. È necessario impostare la lunghezza massima alle dimensioni del CIDR che si desidera importare. Il prefisso IPv4 più specifico che puoi importare è /24. L'intervallo di indirizzi IPv6 più specifico che puoi portare è /48 per i CIDR pubblicizzabili pubblicamente e /60 per i CIDR non pubblicizzabili pubblicamente.

> **Important**
>
> Quando crei un oggetto ROA per Amazon VPC IP Address Manager (IPAM), per i CIDR IPv4 devi impostare la lunghezza massima di un prefisso di indirizzo IP su `/24`. Per i CIDR IPv6, se vengono aggiunti a un pool pubblicizzabile, la lunghezza massima di un prefisso dell'indirizzo IP deve essere `/48`. Ciò garantisce la massima flessibilità per suddividere il tuo indirizzo IP pubblico tra le regioni. AWS IPAM applica la lunghezza massima impostata. Per ulteriori informazioni sugli indirizzi BYOIP su IPAM, consulta il Tutorial: portare i CIDR di indirizzi BYOIP su IPAM nella Guida per l'utente di IPAM di Amazon VPC.

Potrebbe essere necessarie fino a 24 ore prima che il ROA diventi disponibile su Amazon. Per ulteriori informazioni, consulta il tuo RIR:

- Richieste — ROA ARIN
- — Gestire i ROA RIPE
- APNIC – Gestione delle route

Quando esegui la migrazione degli annunci pubblicitari da un carico di lavoro locale a AWS, devi creare un ROA per l'ASN esistente prima di creare il RoA per gli ASN di Amazon. In caso contrario, potresti avere un impatto sul routing e sugli annunci pubblicitari esistenti.

> **Important**
>
> Affinché Amazon possa pubblicizzare e continuare a pubblicizzare il tuo intervallo di indirizzi IP, i ROA per gli ASN di Amazon devono essere conformi alle precedenti linee guida. Se i ROA non sono validi o conformi alle linee guida sopra descritte, Amazon si riserva il diritto di interrompere la pubblicizzazione dell'intervallo di indirizzi IP.

> **Note**
>
> Questo passaggio non è richiesto per lo spazio di indirizzi IPv6 non pubblicizzabile pubblicamente.

Onboarding dell'intervallo di indirizzi da utilizzare in Amazon EC2

Il processo di onboarding per BYOIP prevede le seguenti attività, a seconda delle esigenze.

Processi

- Fornisci un intervallo di indirizzi pubblicizzato in AWS
- Effettuare il provisioning di un intervallo di indirizzi IPv6 non pubblicizzabile pubblicamente
- Pubblicizza l'intervallo di indirizzi tramite AWS
- Annullamento del provisioning dell'intervallo di indirizzi
- Convalida del BYOIP

Fornisci un intervallo di indirizzi pubblicizzato in AWS

Quando fornisci un intervallo di indirizzi da utilizzare con AWS, confermi di controllare l'intervallo di indirizzi e autorizzi Amazon a pubblicizzarlo. Verifichiamo inoltre che tu abbia il controllo dell'intervallo di indirizzi tramite un messaggio di autorizzazione firmato. Questo messaggio è firmato con la coppia di X.509 chiavi autofirmate utilizzata per aggiornare il record RDAP con il certificato. X.509 AWS richiede un messaggio di autorizzazione con firma crittografica da presentare al RIR. Il RIR autentica

la firma basandosi sul certificato aggiunto a RDAP e controlla i dettagli dell'autorizzazione rispetto al ROA.

Eseguire il provisioning dell'intervallo di indirizzi

1. Composizione di un messaggio

   Comporre il messaggio di autorizzazione in testo normale. Il formato del messaggio è il seguente, in cui la data è la data di scadenza del messaggio:

   ```
   1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
   ```

   Sostituire il numero di account, l'intervallo di indirizzi e la data di scadenza con i valori desiderati per creare un messaggio analogo al seguente:

   ```
   text_message="1|aws|0123456789AB|198.51.100.0/24|20211231|SHA256|RSAPSS"
   ```

   Questo non deve essere confuso con un messaggio ROA, che ha un aspetto simile.

2. Firma di messaggi

   Firmare il messaggio di testo normale utilizzando la chiave privata creata in precedenza. La firma restituita da questo comando è una stringa lunga che sarà necessario utilizzare nel passaggio successivo.

   > **Important**
   >
   > Si consiglia di copiare e incollare questo comando. Ad eccezione del contenuto del messaggio, non modificare o sostituire nessuno dei valori.

   ```
   signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt
    rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform PEM
    | openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
   ```

3. Provisioning dell'indirizzo

   Utilizzate il comando AWS CLI https://docs.aws.amazon.com/cli/latest/reference/ec2/provision-byoip-cidr.html provision-byoip-cidr per effettuare il provisioning dell'intervallo di indirizzi.

L'opzione `--cidr-authorization-context` utilizza le stringhe di messaggio e firma create in precedenza.

> **Important**
>
> È necessario specificare la AWS regione in cui eseguire il provisioning dell'intervallo BYOIP se è diverso da quello di Configure the. AWS CLI `Default region name`

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --region us-east-1
```

Il provisioning di un intervallo di indirizzi è un'operazione asincrona, perciò la chiamata ritorna immediatamente, mentre l'intervallo di indirizzi non è pronto per l'utilizzo finché lo stato non passa da `pending-provision` a `provisioned`.

4. Monitoraggio dell'avanzamento

   Sebbene la maggior parte del provisioning venga completata entro due ore, il completamento del processo di provisioning per gli intervalli pubblicizzabili pubblicamente può richiedere fino a una settimana. Utilizza il comando describe-byoip-cidrs per monitorarne l'avanzamento, come in questo esempio:

   ```
   aws ec2 describe-byoip-cidrs --max-results 5 --region us-east-1
   ```

   Se si verificano problemi durante il provisioning e lo stato passa a `failed-provision`, eseguire nuovamente il comando `provision-byoip-cidr` dopo che i problemi sono stati risolti.

Effettuare il provisioning di un intervallo di indirizzi IPv6 non pubblicizzabile pubblicamente

Per impostazione predefinita, viene eseguito il provisioning di un intervallo di indirizzi affinché sia pubblicizzabile pubblicamente su Internet. Puoi eseguire il provisioning di un intervallo di indirizzi IPv6 che non sarà pubblicizzabile pubblicamente. Per le route che non sono pubblicamente pubblicizzabili, il processo di provisioning viene generalmente completato in pochi minuti. Quando si associa un blocco CIDR IPv6 da un intervallo di indirizzi non pubblici a un VPC, è possibile accedere al CIDR

IPv6 solo tramite opzioni di connettività ibrida che supportano l'IPv6, come VPN o Amazon VPC Transit Gateway. Direct Connect AWS Site-to-Site https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html

Non è richiesto un ROA per effettuare il provisioning di un intervallo di indirizzi non pubblici.

> **Important**
>
> - Puoi specificare solo se un intervallo di indirizzi sarà pubblicizzabile pubblicamente durante il provisioning. Non puoi modificare lo stato pubblicizzabile in un secondo momento.
> - Amazon VPC non supporta i CIDR con indirizzo locale univoco (ULA). Tutti VPC devono avere CIDR IPv6 univoci. Due VPC non possono avere lo stesso intervallo CIDR IPv6.

Per effettuare il provisioning di un intervallo di indirizzi IPv6 che non sarà pubblicizzabile pubblicamente, utilizza il seguente comando: provision-byoip-cidr.

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --no-publicly-advertisable --
region us-east-1
```

Pubblicizza l'intervallo di indirizzi tramite AWS

Dopo aver eseguito il provisioning, l'intervallo di indirizzi è pronto per essere pubblicizzato. Deve essere pubblicizzato l'intervallo di indirizzi esatto oggetto del provisioning. Non può essere pubblicizzata solo una parte dell'intervallo di indirizzi oggetto del provisioning.

Se hai eseguito il provisioning di un intervallo di indirizzi IPv6 che non verrà pubblicizzato pubblicamente, non è necessario completare questa fase.

Ti consigliamo di smettere di pubblicizzare l'intervallo di indirizzi o parte dell'intervallo da altre località prima di pubblicizzarlo tramite. AWS Se si continua a pubblicizzare l'intervallo di indirizzi IP o qualsiasi parte dell'intervallo da altri percorsi, non possiamo sostenere l'operazione in modo affidabile e risolvere eventuali problemi. Nello specifico, non siamo in grado di garantire che il traffico verso l'intervallo di indirizzi o qualsiasi parte dell'intervallo entrerà nella tua rete.

Per ridurre al minimo i tempi di inattività, puoi configurare AWS le tue risorse in modo da utilizzare un indirizzo del tuo pool di indirizzi prima che venga pubblicizzato e contemporaneamente interrompere la pubblicità dalla posizione corrente e iniziare a pubblicizzarlo tramite. AWS Per ulteriori informazioni

sull'allocazione di un indirizzo IP elastico da un pool di indirizzi, consulta Allocare un indirizzo IP elastico.

Limitazioni

- È possibile eseguire il comando advertise-byoip-cidr al massimo una volta ogni 10 secondi, anche se è necessario specificare ogni volta i diversi intervalli di indirizzi.
- È possibile eseguire il comando withdraw-byoip-cidr al massimo una volta ogni 10 secondi, anche se è necessario specificare i diversi intervalli di indirizzi ogni volta.

Per pubblicizzare l'intervallo di indirizzi, utilizzare il seguente comando advertise-byoip-cidr.

```
aws ec2 advertise-byoip-cidr --cidr address-range --region us-east-1
```

Per smettere di pubblicizzare un intervallo di indirizzi, utilizza il comando withdraw-byoip-cidr seguente.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

> **Note**
>
> Nella zona `eu-central-1-ist-1` locale, la pubblicità e il prelievo sono asincroni. L'intervallo di indirizzi passa allo `pending-withdrawal` stato `pending-advertising` or prima del completamento dell'operazione. Per ulteriori informazioni, vedere Disponibilità https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-byoip.html#byoip-zone-avail delle zone locali.

Annullamento del provisioning dell'intervallo di indirizzi

Per smettere di utilizzare l'intervallo di indirizzi con AWS, rilascia innanzitutto gli indirizzi IP elastici e dissocia tutti i blocchi CIDR IPv6 ancora allocati dal pool di indirizzi. Quindi interrompi la pubblicità dell'intervallo di indirizzi e, infine, annulla il provisioning dell'intervallo di indirizzi.

Non puoi annullare il provisioning di una parte dell'intervallo di indirizzi. Se desideri utilizzare un intervallo di indirizzi più specifico con AWS, rimuovi l'intero intervallo di indirizzi ed esegui il provisioning di un intervallo di indirizzi più specifico.

(IPv4) Per rilasciare ciascun indirizzo IP elastico, utilizza il seguente comando release-address.

```
aws ec2 release-address --allocation-id eipalloc-12345678abcabcabc --region us-east-1
```

(IPv6) Per annullare l'associazione di un blocco CIDR IPv6, utilizza il seguente comando disassociate-vpc-cidr-block.

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-12345abcd1234abc1
 --region us-east-1
```

Per smettere di pubblicizzare un intervallo di indirizzi, utilizza il comando withdraw-byoip-cidr seguente.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Per annullare il provisioning di un intervallo di indirizzi, utilizza il comando deprovision-byoip-cidr seguente.

```
aws ec2 deprovision-byoip-cidr --cidr address-range --region us-east-1
```

L'annullamento del provisioning di un intervallo di indirizzi può richiedere fino a un giorno.

Convalida del BYOIP

1. Convalida della coppia di chiavi x.509 autofirmata

   Verifica che il certificato sia stato caricato e sia valido tramite il comando whois.

   Per ARIN, usa `whois -h whois.arin.net r + 2001:0DB8:6172::/48` per cercare il record RDAP dell'intervallo di indirizzi. Controlla la sezione `Public Comments` per verificare `NetRange` (intervallo di rete) nell'output del comando. Il certificato deve essere aggiunto nella sezione `Public Comments` dell'intervallo di indirizzi.

   Puoi esaminare i `Public Comments` contenenti il certificato usando il comando seguente:

   ```
   whois -h whois.arin.net r + 2001:0DB8:6172::/48 | grep Comments | grep BEGIN
   ```

   Questo restituisce un output con il contenuto della chiave, che deve essere simile al seguente:

   ```
   Public Comments:
   -----BEGIN CERTIFICATE-----
   ```

```
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Per RIPE, usa `whois -r -h whois.ripe.net` *`2001:0DB8:7269::/48`* per cercare il record RDAP dell'intervallo di indirizzi. Controlla la sezione `descr` per esaminare l'oggetto `inetnum` (intervallo di rete) nell'output del comando. Il certificato deve essere aggiunto come nuovo campo `descr` dell'intervallo di indirizzi.

Puoi esaminare i `descr` contenenti il certificato usando il comando seguente:

```
whois -r -h whois.ripe.net 2001:0DB8:7269::/48 | grep descr | grep BEGIN
```

Questo restituisce un output con il contenuto della chiave, che deve essere simile al seguente:

```
descr:
-----BEGIN CERTIFICATE-----MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8
RDAHSP+I1TowDQYJKoZIhvcNAQELBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAg
MCEF1Y2tsYW5kMREwDwYDVQQHDAhBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIF
dlYiBTZXJ2aWNlczETMBEGA1UECwwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPS
VAgRGVtbzAeFw0yMTEyMDcyMDI0NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNV
BAYTAk5aMREwDwYDVQQIDAhBdWNrbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDA
aBgNVBAoME0FtYXpvbiBXZWIgU2VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW
```

```
8xEzARBgNVBAMMCkJZT0lQIERlbW8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwg
gEKAoIBAQCfmacvDp0wZ0ceiXXcR/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanA
EskgAseyFypwEEQr4CJijI/5hp9prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3
stsI5QesHVRwOaXUdprAnndaTugmDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq
35wU/x+wXlAqBXg4MZK2KoUu27kYt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp
1ZnVIc7NqnhdeIW48QaYjhMlUEfxdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2r
GlHWkJsbhr0VEUyAGu1bwkgcdww3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBS
tFyujN6SYBr2glHpGt0XGF7GbGTAfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0
XGF7GbGTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6Y
Lhz521lfyVfxY0t6o3410bQAeAF08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyL
xngwMYN0XY5tVhDQqk4/gmDNEKSZy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9
wySL507XQz76Uk5cFypBOzbnk35UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8
mBGqVpPpey+dXpzzzv1iBKN/VY4ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGC
vRDl/qdO/GIDJi77dmZWkh/ic90MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoN
PyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Per APNIC, usa `whois -h whois.apnic.net` *`2001:0DB8:6170::/48`* per cercare il record RDAP dell'intervallo di indirizzi BYOIP. Controlla la sezione `remarks` per esaminare l'oggetto `inetnum` (intervallo di rete) nell'output del comando. Il certificato deve essere aggiunto come nuovo campo `remarks` dell'intervallo di indirizzi.

Puoi esaminare i `remarks` contenenti il certificato usando il comando seguente:

```
whois -h whois.apnic.net 2001:0DB8:6170::/48 | grep remarks | grep BEGIN
```

Questo restituisce un output con il contenuto della chiave, che deve essere simile al seguente:

```
remarks:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
```

```
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

2. Convalida della creazione di un oggetto ROA

   Convalida la corretta creazione degli oggetti ROA utilizzando l'API dati RIPEstat. Assicurati di testare l'intervallo di indirizzi rispetto agli ASN Amazon 16509 e 14618, oltre agli ASN attualmente autorizzati a pubblicizzare l'intervallo di indirizzi. Per farlo AWS GovCloud (US) Regions, esegui il test con ASN 8987. Per lo AWS European Sovereign Cloud, esegui il test con gli ASN 16509 e 214101.

   Puoi ispezionare gli oggetti ROA da diversi ASN Amazon con il tuo intervallo di indirizzi usando il comando seguente:

   ```
   curl --location --request GET "https://stat.ripe.net/data/rpki-validation/data.json?
   resource=ASN&prefix=CIDR
   ```

   In questo output di esempio, la risposta ha il risultato di `"status": "valid"` per l'ASN Amazon 16509. Indica che l'oggetto ROA dell'intervallo di indirizzi è stato creato correttamente:

   ```
   {
       "messages": [],
       "see_also": [],
       "version": "0.3",
       "data_call_name": "rpki-validation",
       "data_call_status": "supported",
       "cached": false,
       "data": {
           "validating_roas": [
               {
                   "origin": "16509",
                   "prefix": "2001:0DB8::/32",
                   "max_length": 48,
                   "validity": "valid"
   ```

```
            },
            {
                "origin": "14618",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            },
            {
                "origin": "64496",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            }
        ],
        "status": "valid",
        "validator": "routinator",
        "resource": "16509",
        "prefix": "2001:0DB8::/32"
    },
    "query_id": "20230224152430-81e6384e-21ba-4a86-852a-31850787105f",
    "process_time": 58,
    "server_id": "app116",
    "build_version": "live.2023.2.1.142",
    "status": "ok",
    "status_code": 200,
    "time": "2023-02-24T15:24:30.773654"
}
```


Lo stato "`unknown`" indica che l'oggetto ROA dell'intervallo di indirizzi non è stato creato. Lo stato "`invalid_asn`" indica che l'oggetto ROA dell'intervallo di indirizzi non è stato creato correttamente.

Utilizzo dell'intervallo di indirizzi BYOIP in Amazon EC2

Puoi visualizzare e utilizzare gli intervalli di indirizzi IPv4 e IPv6 di cui hai effettuato il provisioning nell'account. Per ulteriori informazioni, consulta the section called "Onboarding dell'intervallo di indirizzi".

Intervalli di indirizzi IPv4

Puoi creare un indirizzo IP elastico dal tuo pool di indirizzi IPv4 e utilizzarlo con AWS le tue risorse, come istanze EC2, gateway NAT e Network Load Balancer.

Per visualizzare informazioni sui pool di indirizzi IPv4 di cui hai effettuato il provisioning nell'account, utilizza il comando describe-public-ipv4-pools riportato di seguito.

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

Per creare un indirizzo IP elastico dal pool di indirizzi IPv4, utilizza il comando allocate-address. Puoi utilizzare l'opzione `--public-ipv4-pool` per specificare l'ID del pool di indirizzi restituito da `describe-byoip-cidrs`. Oppure, puoi utilizzare l'opzione `--address` per specificare un indirizzo dall'intervallo di indirizzi di cui è stato effettuato il provisioning.

Intervalli di indirizzi IPv6

Per visualizzare informazioni sui pool di indirizzi IPv6 di cui hai effettuato il provisioning nell'account, utilizza il comando describe-ipv6-pools riportato di seguito.

```
aws ec2 describe-ipv6-pools --region us-east-1
```

Per creare un VPC e specificare un blocco CIDR IPv6 dal pool di indirizzi IPv6, utilizza il seguente comando create-vpc. Per consentire ad Amazon di scegliere il blocco CIDR IPv6 dal pool di indirizzi IPv6, ometti l'opzione `--ipv6-cidr-block`.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --ipv6-cidr-block ipv6-cidr --ipv6-
pool pool-id --region us-east-1
```

Per associare un blocco CIDR IPv6 dal pool di indirizzi IPv6 a un VPC, utilizza il seguente comando associate-vpc-cidr-block. Per consentire ad Amazon di scegliere il blocco CIDR IPv6 dal pool di indirizzi IPv6, ometti l'opzione `--ipv6-cidr-block`.

```
aws ec2 associate-vpc-cidr-block --vpc-id vpc-123456789abc123ab --ipv6-cidr-block ipv6-
cidr --ipv6-pool pool-id --region us-east-1
```

Per visualizzare i VPC e le informazioni relative al pool di indirizzi IPv6 associato, utilizza il comando describe-vpcs. Per visualizzare informazioni sui blocchi CIDR IPv6 associati da un pool di indirizzi IPv6 specifico, utilizza il seguente comando get-associated-ipv6-pool-cidrs.

```
aws ec2 get-associated-ipv6-pool-cidrs --pool-id pool-id --region us-east-1
```

Se annulli l'associazione del blocco CIDR IPv6 dal VPC, viene rilasciato nuovamente nel pool di indirizzi IPv6.

Indirizzi IP elastici

Un indirizzo IP elastico è un indirizzo IPv4 statico progettato per il cloud computing dinamico. Un indirizzo IP elastico viene assegnato al tuo AWS account ed è tuo fino a quando non lo rilasci. Mediante un indirizzo IP elastico, è possibile mascherare il guasto di un'istanza o di un software rimappando rapidamente l'indirizzo per un'altra istanza presente nell'account. In alternativa, è possibile specificare l'indirizzo IP elastico in un record DNS del dominio, in modo che il dominio punti all'istanza specificata. Per ulteriori informazioni, consulta la documentazione del registrar di dominio.

Un indirizzo IP elastico è un indirizzo IPv4 pubblico raggiungibile da Internet. Se devi collegarti a un'istanza in uso che non dispone di un indirizzo IPv4 pubblico, puoi associare un indirizzo IP elastico all'istanza per abilitare la comunicazione con Internet.

Indice

- Prezzi degli indirizzi IP elastici
- Nozioni di base sull'indirizzo IP elastico
- Quota degli indirizzi IP elastici
- Associazione di un indirizzo IP elastico a un'istanza
- Trasferisci un indirizzo IP elastico tra Account AWS
- Rilascio di un indirizzo IP elastico
- Creazione di un record DNS inverso per l'e-mail su Amazon EC2

Prezzi degli indirizzi IP elastici

È previsto un addebito per tutti gli indirizzi IP elastici, indipendentemente dal fatto che siano in uso (allocati a una risorsa, come un'istanza EC2) o inattivi (creati nell'account ma non allocati).

AWS addebiti per tutti gli indirizzi IPv4 pubblici, inclusi gli indirizzi IPv4 pubblici associati alle istanze in esecuzione e gli indirizzi IP elastici. Per ulteriori informazioni, consulta la scheda Public IPv4 Address sulla pagina dei prezzi di Amazon VPC.

Nozioni di base sull'indirizzo IP elastico

Le caratteristiche di base di un indirizzo IP elastico sono le seguenti:

- Un indirizzo IP elastico è statico e non cambia nel tempo.

- Un indirizzo IP elastico può essere utilizzato solo in una regione specifica e non può essere spostato in una regione diversa.
- Un indirizzo IP elastico proviene dal pool Amazon di indirizzi IPv4 o da un pool di indirizzi IPv4 personalizzati trasferiti su Account AWS. IPv6 non supporta gli indirizzi IP elastici.
- Per utilizzare un indirizzo IP elastico bisogna prima allocarne uno al proprio account e associarlo con la propria istanza o con un'interfaccia di rete.
- Quando si associa un indirizzo IP elastico a un'istanza, viene associato anche all'interfaccia di rete primaria dell'istanza. Quando si associa un indirizzo IP elastico a un'interfaccia di rete collegata a un'istanza, viene associato anche all'istanza.
- Quando associ un indirizzo IP elastico viene a un'istanza o alla sua interfaccia di rete principale, se l'istanza possiede già un indirizzo IPv4 pubblico associato, quell'indirizzo IPv4 pubblico viene reinserito nel pool di Amazon degli indirizzi IPv4 pubblici. L'indirizzo IP elastico viene invece associato all'istanza. Non è possibile riutilizzare l'indirizzo IPv4 pubblico che è stato precedentemente associato all'istanza e non è possibile convertire quell'indirizzo IPv4 pubblico in un indirizzo IP elastico. Per ulteriori informazioni, consulta Indirizzi IPv4 pubblici.
- È possibile disassociare un indirizzo IP elastico da una risorsa e associarlo nuovamente con una risorsa differente. Per evitare comportamenti imprevisti, assicurarsi che tutte le connessioni attive alla risorsa denominata nell'associazione esistente siano chiuse prima di apportare la modifica. Dopo aver associato l'indirizzo IP elastico a una risorsa diversa, è possibile riaprire le connessioni alla risorsa appena associata.
- Un indirizzo IP elastico disassociato rimane allocato al proprio account fino all'esplicito rilascio. Ti vengono addebitati tutti gli indirizzi IP elastici presenti nel tuo account, indipendentemente dal fatto che siano associati o meno a un'istanza. Per ulteriori informazioni, consulta la scheda Public IPv4 Address sulla pagina dei prezzi di Amazon VPC.
- Quando un indirizzo IP elastico viene associato a un'istanza che in precedenza aveva un indirizzo IPv4 pubblico, l'hostname del DNS pubblico dell'istanza cambia per abbinare l'indirizzo IP elastico.
- Risolveremo un hostname del DNS pubblico per l'indirizzo IPv4 pubblico o per l'indirizzo IP elastico dell'istanza al di fuori della rete della stessa e per l'indirizzo IPv4 privato dell'istanza all'interno della rete dell'istanza.
- Quando assegni un indirizzo IP elastico da un pool di indirizzi IP che hai aggiunto al tuo AWS account, non viene conteggiato ai fini dei limiti degli indirizzi IP Elastic. Per ulteriori informazioni, consulta Quota degli indirizzi IP elastici.
- Quando si allocano gli indirizzi IP elastici, è possibile associare gli indirizzi IP elastici a un gruppo di confine di rete. Questa è la posizione da cui pubblicizziamo il blocco CIDR. L'impostazione del

gruppo di confine di rete limita il blocco CIDR a questo gruppo. Se non si specifica il gruppo di confine di rete, viene impostato il gruppo di confine contenente tutte le zone di disponibilità nella regione (ad esempio `us-west-2`).

- Un indirizzo IP elastico può essere utilizzato solo in un gruppo di confine di rete specifico.

Quota degli indirizzi IP elastici

Per impostazione predefinita, tutti Account AWS hanno una quota di cinque (5) indirizzi IP elastici per regione, poiché gli indirizzi Internet pubblici (IPv4) sono una risorsa pubblica limitata. Consigliamo fortemente l'utilizzo di un indirizzo IP elastico, per la possibilità di rimappare l'indirizzo su un'altra istanza in caso di fallimento dell'istanza. Inoltre, permette l'utilizzo di hostname DNS per tutte le altre comunicazioni internodo.

Se si ritiene che l'architettura richieda ulteriori indirizzi IP elastici, è possibile chiedere un aumento delle quote direttamente dalla console Service Quotas. Per richiedere un aumento della quota, è possibile richiedere un aumento a livello di account. Per ulteriori informazioni, consulta Service Quotas di Amazon EC2.

Associazione di un indirizzo IP elastico a un'istanza

Dopo aver assegnato un indirizzo IP elastico, puoi associarlo a una AWS risorsa, come un'istanza EC2, un gateway NAT o un Network Load Balancer. Per associare un indirizzo IP Elastic a una AWS risorsa diversa in un secondo momento, puoi dissociarlo dalla risorsa corrente e quindi associarlo alla nuova risorsa.

Processi

- Allocare un indirizzo IP elastico
- Associazione di un indirizzo IP elastico
- Annullare l'associazione di un indirizzo IP elastico

Allocare un indirizzo IP elastico

Puoi allocare un indirizzo IP elastico per l'utilizzo in una Regione. È previsto un addebito per tutti gli indirizzi IP elastici, indipendentemente dal fatto che siano in uso (associati a una risorsa, come un'istanza EC2) o inattivi (creati nell'account ma non associati).

Console

Per allocare un indirizzo IP elastico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Network & Security (Rete e sicurezza) e poi Elastic IPs (IP elastici).
3. Scegliere Allocate Elastic IP address (Alloca indirizzo IP elastico).
4. (Facoltativo) Quando si assegna un indirizzo IP elastico (EIP), si sceglie il gruppo di confini di rete in cui allocare l'EIP. Un gruppo di confini di rete è un insieme di zone di disponibilità (AZ), zone locali o zone di lunghezza d'onda da cui AWS pubblicizza un indirizzo IP pubblico. Le zone locali e le zone a lunghezza d'onda possono avere gruppi di confini di rete diversi rispetto alle AZ di una regione per garantire una latenza o una distanza fisica minima tra la AWS rete e i clienti che accedono alle risorse in tali zone.

   > **Important**
   >
   > È necessario allocare un EIP nello stesso gruppo di confini di rete della AWS risorsa che verrà associata all'EIP. Un EIP in un gruppo di confini di rete può essere pubblicizzato solo nelle zone di quel gruppo di confini di rete e non in altre zone rappresentate da altri gruppi di confini di rete.

   Se hai abilitato le zone locali o le zone Wavelength (per ulteriori informazioni, consulta Abilitazione di una zona locale o Abilitazione delle zone Wavelength), puoi scegliere un gruppo di confini di rete per AZ, zone locali o zone Wavelength. Scegli con attenzione il gruppo di confini di rete poiché l'EIP e la risorsa AWS a cui è associata devono risiedere nello stesso gruppo di confini di rete. Puoi utilizzare la console EC2 per visualizzare il gruppo di confini di rete in cui si trovano le tue zone di disponibilità, zone locali o zone Wavelength. In genere, tutte le zone di disponibilità in una regione appartengono allo stesso gruppo di confini di rete, mentre le zone locali o le zone Wavelength Zone appartengono a gruppi di confini di rete separati.

   Se non hai abilitato le zone locali o le zone Wavelength, quando allochi un EIP, il gruppo di confini di rete che rappresenta tutte le AZ della regione (ad esempio, `us-west-2`) è predefinito e non potrai modificarlo. Ciò significa che l'EIP assegnato a questo gruppo di confini di rete verrà pubblicizzato in tutte le AZ della regione in cui ti trovi.

5. Per Public IPv4 address pool (Pool di indirizzi IPv4 pubblici) scegliere una delle seguenti opzioni:

   - Amazon's pool of IPv4 addresses (Pool di indirizzi IPv4 di Amazon) — Se desideri che un indirizzo IPv4 venga allocato dal pool di indirizzi IP di Amazon.
   - Indirizzo IPv4 pubblico che importi nel tuo account AWS : se desideri allocare un indirizzo pubblico IPv4 non contiguo (non sequenziale) da un pool di indirizzi IP che hai importato nel tuo account AWS . Questa opzione è disattivata se non disponi di pool di indirizzi IP. Per ulteriori informazioni su come aggiungere il proprio intervallo di indirizzi IP al proprio AWS account, vedere. Trasferire i propri indirizzi IP (BYOIP) in Amazon EC2
   - Pool di indirizzi IPv4 di proprietà del cliente: se desideri allocare un indirizzo IPv4 da un pool creato dalla tua rete locale per l'utilizzo con un Outpost. AWS Questa opzione è disabilitata se non si dispone di un Outpost AWS .
   - Allocazione utilizzando un pool IPv4 IPAM: se desideri allocare indirizzi IP elastici sequenziali da un blocco IPv4 pubblico contiguo in un pool IPAM. L'allocazione di indirizzi IP elastici sequenziali può ridurre in modo significativo il sovraccarico di gestione degli elenchi di controllo degli accessi di sicurezza e semplificare l'allocazione e il tracciamento degli indirizzi IP per le aziende che scalano in AWS. Per ulteriori informazioni, consulta Allocare indirizzi IP elastici sequenziali da un pool IPAM nella Guida per l'utente di Amazon VPC IPAM.
6. (Facoltativo) Per aggiungere un tag, scegli Aggiungi nuovo tag e immetti una chiave e un valore di tag.

AWS CLI

Per allocare un indirizzo IP elastico

Utilizzare il comando allocate-address della AWS CLI .

Nel seguente esempio, Amazon EC2 seleziona un indirizzo dal pool di indirizzi Amazon.

```
aws ec2 allocate-address
```

Nell'esempio seguente, Amazon EC2 seleziona un indirizzo dal pool specificato che hai utilizzato utilizzando BYOIP. AWS

```
aws ec2 allocate-address \
```

```
    --public-ipv4-pool ipv4pool-ec2-012345abcdef67890
```

Il seguente esempio specifica un indirizzo dal pool IPv4 IPAM specificato.

```
aws ec2 allocate-address \
    --ipam-pool-id ipam-pool-1234567890abcdef0 \
    --address 192.0.2.0
```

PowerShell

Per allocare un indirizzo IP elastico

Utilizza il cmdlet New-EC2Address.

Nel seguente esempio, Amazon EC2 seleziona un indirizzo dal pool di indirizzi Amazon.

```
New-EC2Address
```

Nell'esempio seguente, Amazon EC2 seleziona un indirizzo dal pool specificato che hai utilizzato utilizzando BYOIP. AWS

```
New-EC2Address `
    -PublicIpv4Pool ipv4pool-ec2-012345abcdef67890
```

Il seguente esempio specifica un indirizzo dal pool IPv4 IPAM specificato.

```
New-EC2Address `
    -IpamPoolId ipam-pool-1234567890abcdef0 `
    -Address 192.0.2.0
```

Associazione di un indirizzo IP elastico

Se si sta cercando di associare un indirizzo IP elastico a un'istanza in modo da consentire la comunicazione con Internet, occorre accertarsi che l'istanza si trovi in una sottorete pubblica. Per ulteriori informazioni, consulta Permetti l'accesso a Internet tramite un gateway Internet nella Guida per l'utente di Amazon VPC.

Console

Per associare un indirizzo IP elastico a un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico creato e scegliere Actions (Operazioni), Associate address (Associa indirizzo IP elastico).
4. Per Resource type (Tipo di risorsa), scegliere Instance (Istanza).
5. Ad esempio, scegliere l'istanza con cui associare l'indirizzo IP elastico. È inoltre possibile immettere del testo per cercare un'istanza specifica.
6. (Facoltativo) Per Private IP address (Indirizzo IP privato), specificare un indirizzo IP privato a cui associare l'indirizzo IP elastico.
7. Seleziona Associate (Associa).

Per associare un indirizzo IP elastico a un'interfaccia di rete.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico creato e scegliere Actions (Operazioni), Associate address (Associa indirizzo IP elastico).
4. Per il Resource type (Tipo di risorsa), scegli Network interface (Interfaccia di rete).
5. Per Network interface (Interfaccia di rete), scegliere l'interfaccia di rete con cui associare l'indirizzo IP elastico. È inoltre possibile immettere del testo per cercare un'interfaccia di rete specifica.
6. (Facoltativo) Per Private IP address (Indirizzo IP privato), specificare un indirizzo IP privato a cui associare l'indirizzo IP elastico.
7. Seleziona Associate (Associa).

AWS CLI

Per associare un indirizzo IP elastico

Usa il comando associate-address. https://docs.aws.amazon.com/cli/latest/reference/ec2/associate-address.html AWS CLI

```
aws ec2 associate-address \
    --instance-id i-0b263919b6498b123 \
    --allocation-id eipalloc-64d5890a
```

PowerShell

Per associare un indirizzo IP elastico

Utilizza il cmdlet Register-EC2Address.

```
Register-EC2Address `
    -InstanceId i-0b263919b6498b123 `
    -AllocationId eipalloc-64d5890a
```

Annullare l'associazione di un indirizzo IP elastico

È possibile annullare l'associazione di un indirizzo IP elastico da un'istanza o un'interfaccia di rete in qualsiasi momento. Dopo aver annullato l'associazione dell'indirizzo IP elastico, puoi associarlo a un'altra risorsa.

Console

Per annullare l'associazione e riassociare un indirizzo IP elastico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico per il quale annullare l'associazione, quindi selezionare Actions (Operazioni), Disassociate Elastic IP address (Annulla associazione indirizzo IP elastico).
4. Selezionare Disassociate (Annulla associazione).

AWS CLI

Per annullare l'associazione di un indirizzo IP elastico

Utilizzate il comando disassociate-address. https://docs.aws.amazon.com/cli/latest/reference/ec2/disassociate-address.html AWS CLI

```
aws ec2 disassociate-address --association-id eipassoc-12345678
```

PowerShell

Per annullare l'associazione di un indirizzo IP elastico

Utilizza il cmdlet Unregister-EC2Address.

```
Unregister-EC2Address -AssociationId eipassoc-12345678
```

Trasferisci un indirizzo IP elastico tra Account AWS

È possibile trasferire un indirizzo IP elastico da uno Account AWS all'altro. Ciò può essere utile nelle seguenti situazioni:

- Disaster recovery: esegue nuovamente la mappatura degli indirizzi IP in modo rapido per i carichi di lavoro su Internet rivolti al pubblico durante gli eventi di emergenza.
- Ristrutturazione organizzativa: sposta rapidamente un carico di lavoro da uno Account AWS all'altro. Un trasferimento di indirizzi evita la necessità di attendere che i nuovi indirizzi IP elastici vengano autorizzati dai gruppi di sicurezza e dagli ACL di rete.
- Amministrazione centralizzata della sicurezza: utilizza un account di AWS sicurezza centralizzato per tracciare e trasferire gli indirizzi IP elastici di cui è stata verificata la conformità alla sicurezza.

Prezzi

Il trasferimento degli indirizzi IP elastici è gratuito.

Processi

- Abilitare il trasferimento di indirizzi IP elastici
- Accettazione di un indirizzo IP elastico trasferito
- Disabilitazione del trasferimento di indirizzi IP elastici

Abilitare il trasferimento di indirizzi IP elastici

Questa sezione descrive come accettare un indirizzo IP elastico trasferito. Prendi nota delle seguenti limitazioni relative all'abilitazione degli indirizzi IP elastici per il trasferimento:

- Puoi trasferire gli indirizzi IP elastici da qualsiasi Account AWS (account di origine) a qualsiasi altro Account AWS nello stesso Regione AWS (account di trasferimento). Non puoi trasferire indirizzi IP elastici in un'altra Regione.
- Quando si trasferisce un indirizzo IP elastico, viene eseguito un handshake in due passaggi tra gli Account AWS. Quando l'account di origine inizia il trasferimento, gli account di trasferimento hanno sette giorni per accettare il trasferimento dell'indirizzo IP elastico. Durante questi sette giorni, l'account di origine può visualizzare il trasferimento in sospeso (ad esempio nella AWS console o utilizzando il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-address-transfers.html describe-address-transfers). Dopo sette giorni, il trasferimento scade e la proprietà dell'indirizzo IP elastico ritorna all'account di origine.
- I trasferimenti accettati sono visibili all'account di origine (ad esempio nella AWS console o utilizzando il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-address-transfers.html describe-address-transfers) per 14 giorni dopo l'accettazione dei trasferimenti.
- AWS non notifica agli account di trasferimento le richieste di trasferimento di indirizzi IP elastici in sospeso. Il proprietario dell'account di origine deve notificare al proprietario dell'account di trasferimento che esiste una richiesta di trasferimento di indirizzo IP elastico che deve accettare.
- Tutti i tag che sono associati a un indirizzo IP elastico da trasferire vengono reimpostati al termine del trasferimento.
- Non puoi trasferire gli indirizzi IP elastici assegnati dai pool di indirizzi IPv4 pubblici che porti ai tuoi Account AWS , comunemente denominati pool di indirizzi Bring Your Own IP (BYOIP).
- Non è possibile trasferire indirizzi IP elastici allocati da un pool pubblico e Amazon-provided contiguo di Amazon VPC IP Address Manager (IPAM) IPv4. Invece, l'IPAM consente di condividere i pool IPAM tra AWS account integrando l'IPAM con le organizzazioni e utilizzandolo. AWS AWS RAM Per ulteriori informazioni, consulta Allocare indirizzi IP elastici sequenziali da un pool IPAM nella Guida per l'utente di Amazon VPC IPAM.
- Se si tenta di trasferire un indirizzo IP elastico a cui è associato un record DNS inverso, è possibile iniziare il processo di trasferimento, ma l'account di trasferimento non sarà in grado di accettare il trasferimento finché il record DNS associato non verrà rimosso.
- Se hai abilitato e configurato AWS Outposts, potresti aver allocato indirizzi IP elastici da un pool di indirizzi IP (CoIP) di proprietà del cliente. Non è possibile trasferire indirizzi IP elastici allocati dai CoIP. Tuttavia, puoi utilizzare AWS RAM per condividere un CoIP con un altro account. Per ulteriori informazioni, vedere gli indirizzi Customer-owned IP nella Guida per l'AWS Outposts utente.
- Puoi utilizzare Amazon VPC IPAM per monitorare il trasferimento di indirizzi IP elastici agli account di un'organizzazione da AWS Organizations. Per ulteriori informazioni, consulta Visualizza la

cronologia degli indirizzi IP. Se un indirizzo IP elastico viene trasferito all' Account AWS esterno dell'organizzazione, la cronologia di controllo IPAM dell'indirizzo IP elastico viene persa.

Questa sezione deve essere completata dall'account di origine.

Console

Abilitazione del trasferimento di indirizzi IP elastici

1. Assicurati di utilizzare l' AWS account sorgente.
2. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
3. Nel riquadro di navigazione, scegli IP elastici.
4. Seleziona uno o più indirizzi IP elastici per abilitare il trasferimento e scegli Actions (Azioni), Enable transfer (Abilita trasferimento).
5. Se stai trasferendo più indirizzi IP elastici, vedrai l'opzione Transfwer type (Tipo di trasferimento). Scegli una delle seguenti opzioni:
   - Scegli Account singolo se stai trasferendo gli indirizzi IP elastici su un singolo AWS account.
   - Scegli Account multipli se stai trasferendo gli indirizzi IP Elastic su più AWS account.
6. In Transfer account ID (ID degli account di trasferimento), inserisci gli ID degli account AWS a cui desideri trasferire gli indirizzi IP elastici.
7. Conferma il trasferimento inserendo **`enable`** nella casella di testo.
8. Seleziona Invia.
9. Per accettare il trasferimento, consulta Accettazione di un indirizzo IP elastico trasferito. Per disabilitare il trasferimento, consulta Disabilitazione del trasferimento di indirizzi IP elastici.

AWS CLI

Abilitazione del trasferimento di indirizzi IP elastici

Usa il comando enable-address-transfer.

```
aws ec2 enable-address-transfer \
    --allocation-id eipalloc-09ad461b0d03f6aaf \
    --transfer-account-id 123456789012
```

PowerShell

Abilitazione del trasferimento di indirizzi IP elastici

Utilizza il cmdlet Enable-EC2AddressTransfer.

```
Enable-EC2AddressTransfer `
    -AllocationId eipalloc-09ad461b0d03f6aaf `
    -TransferAccountId 123456789012
```

Accettazione di un indirizzo IP elastico trasferito

Questa sezione descrive come accettare un indirizzo IP elastico trasferito.

Quando si trasferisce un indirizzo IP elastico, viene eseguito un handshake in due passaggi tra gli Account AWS. Quando l'account di origine inizia il trasferimento, gli account di trasferimento hanno sette giorni per accettare il trasferimento dell'indirizzo IP elastico. Durante questi sette giorni, l'account di origine può visualizzare il trasferimento in sospeso (ad esempio nella AWS console o utilizzando il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-address-transfers.html describe-address-transfers). Dopo sette giorni, il trasferimento scade e la proprietà dell'indirizzo IP elastico ritorna all'account di origine.

Quando si accettano i trasferimenti, è bene prendere nota delle seguenti eccezioni che potrebbero verificarsi e delle modalità di risoluzione:

- AddressLimitExceeded: se il tuo account di trasferimento ha superato la quota di indirizzi IP elastici, l'account di origine può abilitare il trasferimento dell'indirizzo IP elastico, ma questa eccezione si verifica quando l'account di trasferimento tenta di accettare il trasferimento. Per impostazione predefinita, tutti AWS gli account sono limitati a 5 indirizzi IP elastici per regione. Consulta Quota degli indirizzi IP elastici per le istruzioni su come aumentare il limite.
- InvalidTransfer.AddressCustomPtrSet: se tu o qualcuno della tua organizzazione avete configurato l'indirizzo IP elastico che state tentando di trasferire per utilizzare la ricerca DNS inversa, l'account di origine può abilitare il trasferimento per l'indirizzo IP elastico, ma questa eccezione si verifica quando l'account di trasferimento tenta di accettare il trasferimento. Per risolvere questo problema, l'account di origine deve rimuovere il record DNS per l'indirizzo IP elastico. Per ulteriori informazioni, consulta Creazione di un record DNS inverso per l'e-mail su Amazon EC2.
- InvalidTransfer.AddressAssociated: se un indirizzo IP elastico è associato a un'istanza ENI o EC2, l'account di origine può abilitare il trasferimento per l'indirizzo IP elastico, ma questa eccezione si

verifica quando l'account di trasferimento tenta di accettare il trasferimento. Per risolvere questo problema, l'account di origine deve dissociare l'indirizzo IP elastico. Per ulteriori informazioni, consulta Annullare l'associazione di un indirizzo IP elastico.

Per eventuali altre eccezioni, contatta il Supporto.

Questa procedura deve essere completata dall'account di trasferimento.

Console

Accettazione del trasferimento di un indirizzo IP elastico

1. Assicurati di utilizzare l'account di trasferimento.
2. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
3. Nel riquadro di navigazione, scegli IP elastici.
4. Scegli Actions (Operazioni), Accept transfer (Accetta trasferimento).
5. Quando viene accettato il trasferimento, nessun tag associato all'indirizzo IP elastico da trasferire viene trasferito con l'indirizzo IP elastico. Se desideri definire un tag Name (Nome) per l'indirizzo IP elastico che stai accettando, seleziona Create a tag with a key of 'Name' and a value that you specify (Crea un tag con una chiave "Nome" e un valore da specificare).
6. Inserisci l'indirizzo IP elastico da trasferire.
7. Se stai accettando più indirizzi IP elastici trasferiti, scegli Add address (Aggiungi indirizzo) per inserire un indirizzo IP elastico aggiuntivo.
8. Seleziona Invia.

AWS CLI

Accettazione del trasferimento di un indirizzo IP elastico

Usa il comando accept-address-transfer.

```
aws ec2 accept-address-transfer --address 100.21.184.216
```

PowerShell

Accettazione del trasferimento di un indirizzo IP elastico

Utilizza il cmdlet Approve-EC2AddressTransfer.

```
Approve-EC2AddressTransfer -Address 100.21.184.216
```

Disabilitazione del trasferimento di indirizzi IP elastici

Questa sezione descrive come disabilitare un trasferimento di IP elastici dopo averlo abilitato.

Questi passaggi devono essere completati dall'account di origine che ha abilitato il trasferimento.

Console

Come disabilitare il trasferimento degli indirizzi IP elastici

1. Assicurati di utilizzare l'origine Account AWS.
2. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
3. Nel riquadro di navigazione, scegli IP elastici.
4. Nell'elenco delle risorse degli IP elastici, assicurati di avere abilitato la proprietà che mostra la colonna Transfer status (Stato del trasferimento).
5. Seleziona uno o più indirizzi IP elastici con Transfer status (Stato del trasferimento) impostato su Pending (In sospeso) e scegli Actions (Azioni), Disable transfer (Disabilita trasferimento).
6. Conferma inserendo **`disable`** nella casella di testo.
7. Seleziona Invia.

AWS CLI

Disabilitazione del trasferimento di indirizzi IP elastici

Usa il comando disable-address-transfer.

```
aws ec2 disable-address-transfer --allocation-id eipalloc-09ad461b0d03f6aaf
```

PowerShell

Disabilitazione del trasferimento di indirizzi IP elastici

Utilizza il cmdlet Disable-EC2AddressTransfer.

```
Disable-EC2AddressTransfer -AllocationId eipalloc-09ad461b0d03f6aaf
```

Rilascio di un indirizzo IP elastico

Se non hai più bisogno di un indirizzo IP Elastic, ti consigliamo di rilasciarlo. L'indirizzo IP elastico da rilasciare non deve essere attualmente associato a una AWS risorsa.

Console

per rilasciare un indirizzo IP elastico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Elastic IPs (IP elastici).
3. Selezionare l'indirizzo IP elastico da rilasciare e scegliere Actions (Operazioni), Release Elastic IP address (Rilascia indirizzo IP elastico).
4. Scegliere Release (Rilascia).

AWS CLI

per rilasciare un indirizzo IP elastico

Usa il comando release-address AWS CLI .

```
aws ec2 release-address --allocation-id eipalloc-64d5890a
```

PowerShell

per rilasciare un indirizzo IP elastico

Utilizza il cmdlet Remove-EC2Address.

```
Remove-EC2Address -AllocationId eipalloc-64d5890a
```

Se rilasci l'indirizzo IP elastico, dovresti riuscire a recuperarlo. Si applicano le regole seguenti:

- Non è possibile recuperare un indirizzo IP elastico se è stato allocato a un altro account AWS ; in caso contrario, si supererà il limite di indirizzi IP elastici.

- Non è possibile recuperare i tag associati all'indirizzo IP elastico.

AWS CLI

Per recuperare un indirizzo IP elastico

Usa il comando allocate-address.

```
aws ec2 allocate-address \
    --domain vpc \
    --address 203.0.113.3
```

PowerShell

Per recuperare un indirizzo IP elastico

Utilizza il cmdlet New-EC2Address.

```
New-EC2Address `
    -Address 203.0.113.3 `
    -Domain vpc `
    -Region us-east-1
```

Creazione di un record DNS inverso per l'e-mail su Amazon EC2

Se si intende inviare messaggi e-mail a terzi da un'istanza EC2, consigliamo di eseguire il provisioning di uno o più indirizzi IP elastici e assegnare record DNS inversi statici agli indirizzi IP elastici utilizzati per inviare l'e-mail. Questo può aiutarti a evitare che la tua email venga contrassegnata come spam da alcune organizzazioni antispam. AWS collabora con gli ISP e le organizzazioni antispam su Internet per ridurre la possibilità che le email inviate da questi indirizzi vengano contrassegnate come spam.

Considerazioni

- Prima di creare un record DNS inverso, devi impostare un corrispondente record DNS di inoltro (tipo di record A) che si risolva in un indirizzo IP elastico nel tuo account. Come best practice, includi tutti gli indirizzi IP elastici per i quali intendi creare record DNS inversi nel record DNS di inoltro.

- Se un record DNS inverso viene associato a un indirizzo IP elastico, l'indirizzo IP elastico è bloccato per l'account e non potrà essere rilasciato dall'account finché non verrà rimosso il record.
- Se ci hai contattato Supporto per configurare il DNS inverso per un indirizzo IP elastico, puoi rimuovere il DNS inverso, ma non puoi rilasciare l'indirizzo IP elastico perché è bloccato da. Supporto Per sbloccare l'indirizzo IP elastico, contatta Supporto AWS. Una volta sbloccato l'indirizzo IP elastico, è possibile rilasciarlo.
- [AWS GovCloud (US) Region] Non è possibile creare un registro DNS. AWS deve assegnare i registri DNS inversi statici per tuo conto. Apri un caso di supporto per rimuovere i limiti di DNS inversi e di invio di e-mail. Devi fornire i record di indirizzi IP elastici e DNS inversi.

Creazione di un record DNS inverso

Puoi creare un record DNS inverso per l'indirizzo IP elastico seguendo questi passaggi.

Console

Per creare un record DNS inverso

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli IP elastici.
3. Seleziona l'indirizzo IP elastico e scegli Actions (Operazioni), quindi Update reverse DNS (Aggiorna DNS inverso).
4. Per Reverse DNS Domain Name (Nome di dominio di DNS inverso), inserire il nome di dominio.
5. Immettere **`update`** per confermare.
6. Scegliere Update (Aggiorna).

AWS CLI

Per creare un record DNS inverso

Utilizza il comando modify-address-attribute.

```
aws ec2 modify-address-attribute \
    --allocation-id eipalloc-abcdef01234567890 \
    --domain-name example.com
```

Di seguito è riportato un output di esempio.

```
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.net.",
            "PtrRecordUpdate": {
                "Value": "example.com.",
                "Status": "PENDING"
            }
        }
    ]
}
```

PowerShell

Per creare un record DNS inverso

Utilizza il cmdlet Edit-EC2AddressAttribute.

```
Edit-EC2AddressAttribute `
    -AllocationId 'eipalloc-abcdef01234567890' `
    -DomainName 'example.com' |
Format-List `
    AllocationId, PtrRecord, PublicIp,
    @{Name='PtrRecordUpdate';Expression={$_.PtrRecordUpdate | Format-List | Out-
String}}
```

Di seguito è riportato un output di esempio.

```
AllocationId    : eipalloc-abcdef01234567890
PtrRecord       : example.net.
PublicIp        : 192.0.2.0
PtrRecordUpdate :
                  Reason :
                  Status : PENDING
                  Value  : example.com.
```

Rimozione di un registro DNS inverso

Puoi rimuovere un record DNS inverso dal tuo indirizzo IP elastico nel modo seguente.

Se ricevi il seguente errore, puoi inviare una richiesta di rimozione delle restrizioni all'invio di email per Supporto ricevere assistenza.

```
The address cannot be released because it is locked to your account.
```

Console

Per rimuovere un registro DNS inverso

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli IP elastici.
3. Seleziona l'indirizzo IP elastico e scegli Actions (Operazioni), quindi Update reverse DNS (Aggiorna DNS inverso).
4. Per Reverse DNS Domain Name (Nome di dominio di DNS inverso), rimuovi il nome di dominio.
5. Immettere **`update`** per confermare.
6. Scegliere Update (Aggiorna).

AWS CLI

Per rimuovere un registro DNS inverso

Utilizza il comando reset-address-attribute.

```
aws ec2 reset-address-attribute \
    --allocation-id eipalloc-abcdef01234567890 \
    --attribute domain-name
```

Di seguito è riportato un output di esempio.

```
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
```

```
            "PtrRecord": "example.com.",
            "PtrRecordUpdate": {
                "Value": "example.net.",
                "Status": "PENDING"
            }
        }
    ]
}
```

PowerShell

Per rimuovere un registro DNS inverso

Utilizza il cmdlet Reset-EC2AddressAttribute.

```
Reset-EC2AddressAttribute `
    -AllocationId 'eipalloc-abcdef01234567890' `
    -Attribute domain-name |
Format-List `
    AllocationId, PtrRecord, PublicIp,
    @{Name='PtrRecordUpdate';Expression={$_.PtrRecordUpdate | Format-List | Out-
String}}
```

Di seguito è riportato un output di esempio.

```
AllocationId    : eipalloc-abcdef01234567890
PtrRecord       : example.com.
PublicIp        : 192.0.2.0
PtrRecordUpdate :
                  Reason :
                  Status : PENDING
                  Value  : example.net.
```

Interfacce di rete elastiche

Un'interfaccia di rete elastica è un componente di rete logico in un VPC che rappresenta una scheda di rete virtuale. È possibile creare e configurare un'interfaccia di rete e collegarla alle istanze che avvii nella stessa zona di disponibilità. Gli attributi di un'interfaccia di rete dipendono dal fatto che sia collegata a o scollegata da un'istanza e quindi ricollegata a un'altra istanza. Quando trasferisci un'istanza di rete da un'istanza a un'altra, il traffico di rete viene reindirizzato dall'istanza originale a quella nuova.

Nota che questa AWS risorsa viene definita interfaccia di rete nell'API Console di gestione AWS di Amazon EC2. Pertanto, in questa documentazione utilizziamo "interfaccia di rete" anziché "interfaccia di rete elastica". Il termine "interfaccia di rete" in questa documentazione significa sempre "interfaccia di rete elastica".

Attributi dell'interfaccia di rete

Un'interfaccia di rete può includere i seguenti attributi:

- Un indirizzo IPv4 privato primario dall'intervallo di indirizzi IPv4 della sottorete
- Un indirizzo IPv6 primario dall'intervallo di indirizzi IPv6 della sottorete
- Indirizzi IPv4 privati secondari dall'intervallo di indirizzi IPv4 della sottorete
- Un indirizzo IP elastico (IPv4) per ogni indirizzo IPv4 privato
- Un indirizzo IPv4 pubblico
- Indirizzi IPv6 secondari
- Gruppi di sicurezza
- Un indirizzo MAC
- Un source/destination contrassegno
- Una descrizione

Monitoraggio del traffico

Puoi abilitare il log del flusso di un VPC sull'interfaccia di rete in modo che vengano acquisite le informazioni sul traffico a livello di interfaccia di rete. Dopo aver creato un log di flusso, puoi visualizzarne e recuperarne i dati in Amazon CloudWatch Logs. Per ulteriori informazioni, consulta Log di flusso VPC nella Guida per l'utente di Amazon VPC.

Indice

- Concetti di interfaccia di rete
- Schede di rete
- Numero massimo di indirizzi IP per interfaccia di rete
- Crea un'interfaccia di rete per la tua istanza EC2
- Allegati dell'interfaccia di rete per l'istanza EC2
- Gestire gli indirizzi IP per le interfacce di rete
- Modifica degli attributi dell'interfaccia di rete

- Interfacce di rete multiple per istanze Amazon EC2
- Requester-managed interfacce di rete
- Delega del prefisso per Interfacce di rete Amazon EC2
- Eliminazione di un'interfaccia di rete

Concetti di interfaccia di rete

Di seguito sono riportati alcuni concetti fondamentali da conoscere quando si inizia a utilizzare interfacce di rete.

Interfaccia di rete primaria

Ogni istanza dispone di un'interfaccia di rete predefinita, denominata interfaccia di rete primaria. Non è possibile scollegare un'interfaccia di rete primaria da un'istanza.

Interfacce di rete secondarie

Puoi creare e collegare interfacce di rete secondarie alla propria istanza. Il numero massimo di interfacce di rete varia a seconda del tipo di istanza. Per ulteriori informazioni, consulta Numero massimo di indirizzi IP per interfaccia di rete.

Indirizzi IPv4 pubblici per le interfacce di rete

Quando avvii un'istanza EC2 in una IPv4-only o più sottoreti, l'istanza riceve un indirizzo IP privato primario dall'intervallo di indirizzi IPv4 della sottorete. Si possono anche specificare ulteriori indirizzi IPv4 privati, i cosiddetti indirizzi IPv4 privati secondari. A differenza di quelli primari, gli indirizzi IP privati secondari possono essere riassegnati da un'istanza all'altra.

Indirizzi IPv4 pubblici per le interfacce di rete

Tutte le sottoreti hanno un attributo modificabile che determina se alle interfacce di rete create in tale sottorete e pertanto alle istanze avviate in quella sottorete viene assegnato un indirizzo IPv4 pubblico. Per ulteriori informazioni, consulta Impostazioni della sottorete nella Guida per l'utente di Amazon VPC. Quando avvii un'istanza, l'indirizzo IP viene assegnato all'interfaccia di rete primaria. Se specifichi un'interfaccia di rete esistente come interfaccia di rete primaria quando avvii un'istanza, l'indirizzo IPv4 pubblico viene determinato da questa interfaccia di rete.

Quando crei un'interfaccia di rete, essa eredita l'attributo di indirizzamento IPv4 pubblico dalla sottorete. Se modifichi l'attributo di indirizzamento IPv4 pubblico della sottorete in un secondo momento, l'interfaccia di rete conserva l'impostazione valida al momento della sua creazione.

Rilasciamo l'indirizzo IP pubblico quando l'istanza è arrestata, ibernata o terminata. Assegniamo un nuovo indirizzo IP pubblico all'avvio dell'istanza interrotta o ibernata, a meno che l'istanza non abbia un'interfaccia di rete secondaria o un indirizzo IPv4 privato secondario associato a un indirizzo IP Elastic.

Indirizzi IPv6 pubblici per le interfacce di rete

Puoi associare blocchi CIDR IPv6 al VPC e alla sottorete e assegnare indirizzi IPv6 in base all'intervallo della sottorete a un'interfaccia di rete. Ciascun indirizzo IPv6 può essere assegnato a un'interfaccia di rete.

Tutte le sottoreti hanno un attributo modificabile che determina se alle interfacce di rete create in tale sottorete e pertanto alle istanze avviate in quella sottorete viene automaticamente assegnato un indirizzo IPv6 in base all'intervallo della sottorete. Quando avvii un'istanza, l'indirizzo IPv6 viene assegnato all'interfaccia di rete primaria.

Indirizzi IP elastici per le interfacce di rete

Puoi associare un indirizzo IP elastico a uno o più indirizzi IPv4 privati per l'interfaccia di rete. Puoi associare un indirizzo IP elastico a ciascun indirizzo IPv4 privato. Se annulli l'associazione di un indirizzo IP elastico da un'interfaccia di rete, puoi rilasciarlo o associarlo a un'altra istanza.

Comportamento risoluzione

Puoi impostare il comportamento di interruzione per un'interfaccia di rete collegata a un'istanza. Puoi specificare se l'interfaccia di rete deve essere eliminata automaticamente quando cessi l'istanza a cui è collegata.

Source/destination verificando

Puoi abilitare o disabilitare source/destination i controlli, che assicurano che l'istanza sia l'origine o la destinazione del traffico che riceve. Source/destination i controlli sono abilitati per impostazione predefinita. È necessario disabilitare source/destination i controlli se l'istanza esegue servizi come la traduzione degli indirizzi di rete, il routing o i firewall.

Requester-managed interfacce di rete

Queste interfacce di rete sono create e gestite da Servizi AWS per consentire all'utente di utilizzare alcune risorse e servizi. Non puoi gestire queste interfacce di rete in autonomia. Per ulteriori informazioni, consulta Requester-managed interfacce di rete.

Delega prefisso

Un prefisso è un intervallo CIDR IPv4 o IPv6 privato riservato allocato per l'assegnazione automatica o manuale alle interfacce di rete associate a un'istanza. Utilizzando i prefissi delegati,

è possibile avviare i servizi più rapidamente assegnando un intervallo di indirizzi IP come un prefisso unico.

Interfacce di rete gestite

Un'interfaccia di rete gestita è gestita da un fornitore di servizi, come Amazon EKS Auto Mode. Non è possibile modificare direttamente le impostazioni di un'interfaccia di rete gestita. Le interfacce di rete gestite sono identificate da un valore true nel campo Gestito. Per ulteriori informazioni, consulta Istanze gestite di Amazon EC2.

Schede di rete

La maggior parte dei tipi di istanza supportano una scheda di rete. I tipo di istanze che supportano più schede di rete offrono prestazioni di rete superiori, tra cui capacità di larghezza di banda superiore a 100 Gb/s e prestazioni migliorate per la velocità dei pacchetti. Quando colleghi un'interfaccia di rete a un'istanza che supporta più schede di rete, puoi selezionare la scheda di rete per l'interfaccia di rete. L'interfaccia di rete primaria deve essere assegnata all'indice della scheda di rete 0.

Le interfacce EFA e EFA-only di rete sono considerate interfacce di rete. È possibile assegnare una sola interfaccia EFA o di rete per EFA-only scheda di rete. L'interfaccia di rete principale non può essere un'interfaccia EFA-only di rete.

I tipi di istanze seguenti supportano più schede di rete. Per informazioni sul numero di interfacce di rete supportate da un tipo di istanza, consulta Numero massimo di indirizzi IP per interfaccia di rete.

Tipo di istanza	Numero di schede di rete
c6in.32xlarge	2
c6in.metal	2
c8gb.48xlarge	2
c8gb.metal-48xl	2
c8gn.48xlarge	2
c8gn.metal-48xl	2
c8in.96xlarge	2

Tipo di istanza	Numero di schede di rete
c8in.metal-96xl	2
c8ib.96xlarge	2
c8ib.metal-96xl	2
dl1.24xlarge	4
g6e.24xlarge	2
g6e.48xlarge	4
g7.48xlarge	2
g7e.24xlarge	2
g7e.48xlarge	4
hpc6id.32xlarge	2
hpc7a.12xlarge	2
hpc7a.24xlarge	2
hpc7a.48xlarge	2
hpc7a.96xlarge	2
hpc8a.96xlarge	2
i7ie.48xlarge	2
i7ie.metal-48xl	2
i8ge.48xlarge	2
i8ge.metal-48xl	2
m6idn.32xlarge	2

Tipo di istanza	Numero di schede di rete
m6idn.metal	2
m6in.32xlarge	2
m6in.metal	2
m8gb.48xlarge	2
m8gb.metal-48xl	2
m8gn.48xlarge	2
m8gn.metal-48xl	2
m8in.96xlarge	2
m8in.metal-96xl	2
m8idn.96xlarge	2
m8idn.metal-96xl	2
m8ib.96xlarge	2
m8ib.metal-96xl	2
m8idb.96xlarge	2
m8idb.metal-96xl	2
p4d.24xlarge	4
p4de.24xlarge	4
p5.48xlarge	32
p5e.48xlarge	32
p5en.48xlarge	16

Tipo di istanza	Numero di schede di rete
p6-b200.48xlarge	8
p6-b300.48xlarge	17
p6e-gb200.36xlarge	17
r8gb.48xlarge	2
r8gb.metal-48xl	2
r8gn.48xlarge	2
r8gn.metal-48xl	2
r8in.96xlarge	2
r8in.metal-96xl	2
r8idn.96xlarge	2
r8idn.metal-96xl	2
r8ib.96xlarge	2
r8ib.metal-96xl	2
r8idb.96xlarge	2
r8idb.metal-96xl	2
r6idn.32xlarge	2
r6idn.metal	2
r6in.32xlarge	2
r6in.metal	2
trn1.32xlarge	8

Tipo di istanza	Numero di schede di rete
trn1n.32xlarge	16
trn2.48xlarge	16
trn2u.48xlarge	16
u7in-16tb.224xlarge	2
u7in-24tb.224xlarge	2
u7in-32tb.224xlarge	2
u7inh-32tb.480xlarge	2

Numero massimo di indirizzi IP per interfaccia di rete

Ogni tipo di istanza supporta un numero massimo di interfacce di rete, un numero massimo di indirizzi IPv4 privati per interfaccia di rete e un numero massimo di indirizzi IPv6 per interfaccia di rete. Il limite relativo agli indirizzi IPv6 è diverso da quello relativo agli indirizzi IPv4 privati per interfaccia di rete. Tieni presente che tutti i tipi di istanza supportano l'indirizzamento IPv6, ad eccezione dei seguenti: C1, M1, M2, M3 e T1.

Interfacce di rete disponibili

La Guida ai tipi di istanza EC2 di Amazon fornisce le informazioni sulle interfacce di rete disponibili per ciascun tipo di istanza. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Specifiche di rete: uso generico
- Specifiche di rete: ottimizzate per il calcolo
- Specifiche di rete: ottimizzate per la memoria
- Specifiche di rete: ottimizzate per l'archiviazione
- Specifiche di rete: calcolo accelerato
- Specifiche di rete: High-performance elaborazione
- Specifiche di rete: generazione precedente

Console

Per recuperare il numero massimo di interfacce di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instance Types (Tipi di istanza).
3. Aggiungi un filtro per specificare il tipo di istanza (Tipo di istanza =c5.12xlarge) o la famiglia di istanze (Famiglia di istanze=c5).
4. (Facoltativo) Scegli l'icona Preferenze, quindi attiva Numero massimo di interfacce di rete. Questa colonna indica il numero massimo di interfacce di rete per ogni tipo di istanza.
5. (Facoltativo) Seleziona il tipo di istanza. Nella scheda Rete, trova Numero massimo di interfacce di rete.

AWS CLI

Per recuperare il numero massimo di interfacce di rete

Puoi utilizzare il comando describe-instance-types per visualizzare informazioni su un tipo di istanza, ad esempio le interfacce di rete supportate e gli indirizzi IP per interfaccia. L'esempio seguente mostra queste informazioni per tutte le istanze C8i.

```
{ echo -e "InstanceType\tMaximumNetworkInterfaces\tIpv4AddressesPerInterface"; \
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c8i.*" \
    --query 'InstanceTypes[*].[InstanceType, NetworkInfo.MaximumNetworkInterfaces,
 NetworkInfo.Ipv4AddressesPerInterface]' \
    --output text | sort -k2 -n; } | column -t
```

Di seguito è riportato un output di esempio.

```
InstanceType    MaximumNetworkInterfaces  Ipv4AddressesPerInterface
c8i.large       3                         20
c8i.2xlarge     4                         30
c8i.xlarge      4                         30
c8i.4xlarge     8                         50
c8i.8xlarge     10                        50
c8i.12xlarge    12                        50
c8i.16xlarge    16                        64
c8i.24xlarge    16                        64
```

```
c8i.32xlarge    24                      64
c8i.48xlarge    24                      64
c8i.96xlarge    24                      64
c8i.metal-48xl  24                      64
c8i.metal-96xl  24                      64
```

PowerShell

Per recuperare il numero massimo di interfacce di rete

È possibile utilizzare il Get-EC2InstanceType PowerShell comando per visualizzare informazioni su un tipo di istanza, ad esempio le interfacce di rete supportate e gli indirizzi IP per interfaccia. L'esempio seguente visualizza queste informazioni per tutte le istanze C8i.

```
Get-EC2InstanceType -Filter @{Name="instance-type"; Values="c8i.*"} |
Select-Object `
    InstanceType,
    @{Name='MaximumNetworkInterfaces';
 Expression={$_.NetworkInfo.MaximumNetworkInterfaces}},
    @{Name='Ipv4AddressesPerInterface';
 Expression={$_.NetworkInfo.Ipv4AddressesPerInterface}} |
Sort-Object MaximumNetworkInterfaces |
Format-Table -AutoSize
```

Di seguito è riportato un output di esempio.

```
InstanceType   MaximumNetworkInterfaces Ipv4AddressesPerInterface
------------   ----------------------- -------------------------
c8i.large                            3                        20
c8i.xlarge                           4                        30
c8i.2xlarge                          4                        30
c8i.4xlarge                          8                        50
c8i.8xlarge                         10                        50
c8i.12xlarge                        12                        50
c8i.24xlarge                        16                        64
c8i.16xlarge                        16                        64
c8i.96xlarge                        24                        64
c8i.48xlarge                        24                        64
c8i.metal-96xl                      24                        64
c8i.32xlarge                        24                        64
c8i.metal-48xl                      24                        64
```

Crea un'interfaccia di rete per la tua istanza EC2

Puoi creare un'interfaccia di rete da utilizzare per le istanze EC2. Quando crei un'interfaccia di rete, specifichi la sottorete per cui viene creata. Una volta creata, non potrai spostare un'interfaccia di rete in un'altra sottorete. Dovrai collegare un'interfaccia di rete a un'istanza nella stessa zona di disponibilità. Puoi rimuovere un'interfaccia di rete secondaria da un'istanza e collegarla a un'altra istanza nella stessa zona di disponibilità. Non è possibile scollegare un'interfaccia di rete primaria da un'istanza. Per ulteriori informazioni, consulta the section called “Allegati dell'interfaccia di rete”.

Console

Per creare un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona Crea interfaccia di rete.
4. (Facoltativo) In Descrizione, immetti un nome descrittivo.
5. Per Subnet (Sottorete), selezionare una sottorete. Le opzioni disponibili nei passaggi successivi cambiano a seconda del tipo di sottorete selezionata (IPv4-only, IPv6-only, o dual-stack (IPv4 e IPv6)).
6. Per il tipo di interfaccia, scegli una delle seguenti opzioni:
   - ENA: un'interfaccia di rete ad alte prestazioni progettata per gestire velocità di trasmissione elevate e pacchetti al secondo per i protocolli riducendo al minimo l'utilizzo della CPU. TCP/IP Si tratta del valore di default. Per ulteriori informazioni su ENA, consulta Elastic Network Adapter.
   - EFA con ENA: un'interfaccia di rete che supporta dispositivi ENA ed EFA per il trasporto tradizionale insieme al trasporto basato su SRD. TCP/IP Se scegli EFA con ENA, l'istanza a cui lo colleghi deve supportare EFA. Per ulteriori informazioni su EFA, consulta Elastic Fabric Adapter.
   - EFA-only: Un'interfaccia di rete ad alte prestazioni progettata per gestire comunicazioni tra nodi ad alto throughput e bassa latenza per il trasporto basato su SRD bypassando lo stack del sistema operativo. Se scegli questa opzione, l'istanza a cui la stai collegando deve supportare EFA. ??? EFA-only le interfacce di rete non supportano gli indirizzi IP. Per ulteriori informazioni su EFA, consulta Elastic Fabric Adapter.
7. In Private IPv4 address (Indirizzo IPv4 privato), completa una delle seguenti operazioni:

- Scegli Auto-assign di consentire ad Amazon EC2 di selezionare un indirizzo IPv4 dalla sottorete.
- Scegli Personalizzato e immetti un indirizzo IPv4 selezionato dalla sottorete.

8. (Solo sottoreti con indirizzi IPv6) Per Indirizzo IPv6, completa una delle seguenti operazioni:
   - Scegli Nessuno se non desideri assegnare un indirizzo IPv6 all'interfaccia di rete.
   - Scegli Auto-assign di consentire ad Amazon EC2 di selezionare un indirizzo IPv6 dalla sottorete.
   - Scegli Personalizzato e immetti un indirizzo IPv6 selezionato dalla sottorete.
9. (Facoltativo) Se stai creando un'interfaccia di rete in un dual-stack o IPv6-only sottorete, hai la possibilità di assegnare l'IP IPv6 primario. Questo assegna un indirizzo unicast globale IPv6 (GUA) primario all'interfaccia di rete. L'assegnazione di un indirizzo IPv6 primario consente di evitare l'interruzione del traffico verso istanze o ENI. Scegli Abilita se l'istanza a cui verrà collegato questo ENI si basa sul fatto che il suo indirizzo IPv6 non cambia. AWS assegnerà automaticamente un indirizzo IPv6 associato all'ENI collegato all'istanza come indirizzo IPv6 primario. Dopo aver abilitato un indirizzo GUA IPv6 come IPv6 primario, non è possibile disabilitarlo. Quando si abilita un indirizzo GUA IPv6 come IPv6 primario, la prima GUA IPv6 verrà impostata come indirizzo IPv6 primario fino alla chiusura dell'istanza o alla disconnessione dell'interfaccia di rete. Se disponi di più indirizzi IPv6 associati a un ENI collegato all'istanza e abiliti un indirizzo IPv6 primario, il primo indirizzo GUA IPv6 associato all'ENI diventa l'indirizzo IPv6 primario.
10. (Facoltativo) Per creare un Elastic Fabric Adapter (EFA), scegli Elastic Fabric Adapter (EFA), Attiva.
11. (Facoltativo) In Impostazioni avanzate, facoltativamente puoi impostare la delega del prefisso IP. Per ulteriori informazioni, consulta Delega prefisso.
    - Auto-assign— AWS sceglie il prefisso tra i blocchi CIDR IPv4 o IPv6 per la sottorete e lo assegna all'interfaccia di rete.
    - Personalizzato: si specifica il prefisso dai blocchi CIDR IPv4 o IPv6 per la sottorete e si AWS verifica che il prefisso non sia già assegnato ad altre risorse prima di assegnarlo all'interfaccia di rete.
12. (Facoltativo) In Impostazioni avanzate, per Timeout di tracciamento della connessione inattiva, modifica i timeout di connessione inattiva predefiniti. Per ulteriori informazioni, consulta Timeout di tracciamento delle connessioni inattive.

- Timeout TCP stabilito: il timeout (in secondi) per le connessioni TCP inattive in uno stato stabilito.
  - Minimo: `60` secondi
  - Massimo: `432000` secondi
  - Predefinito: `350` secondi per i tipi di istanza Nitro v6 (P6e-GB200esclusi); secondi per tutti gli altri tipi di istanza (inclusi). `432000` P6e-GB200
  - Consigliato: meno di `432000` secondi.
- Timeout UDP: il timeout (in secondi) per i flussi UDP inattivi che hanno registrato traffico solo in un'unica direzione o una singola transazione richiesta-risposta.
  - Minimo: `30` secondi
  - Massimo: `60` secondi
  - Impostazione predefinita: `30` secondi
- Timeout del flusso UDP: il timeout (in secondi) per i flussi UDP inattivi classificati come flussi che hanno registrato più di una transazione richiesta-risposta.
  - Minimo: `60` secondi
  - Massimo: `180` secondi
  - Impostazione predefinita: `180` secondi

13. In Security groups (Gruppi di sicurezza), selezionare uno o più gruppi di sicurezza.
14. (Facoltativo) Per ogni tag, seleziona Aggiungi nuovo tag e specifica una chiave tag e un valore di tag facoltativo.
15. Seleziona Crea interfaccia di rete.

AWS CLI

Esempio 1: per creare un'interfaccia di rete con indirizzi IP scelti da Amazon EC2

Utilizza il comando create-network-interface. Questo esempio crea un'interfaccia di rete con un indirizzo IPv4 pubblico e un indirizzo IPv6 scelto da Amazon EC2.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my dual-stack network interface" \
    --ipv6-address-count 1 \
    --groups sg-1234567890abcdef0
```

Esempio 2: per creare un'interfaccia di rete con indirizzi IP specifici

Utilizza il comando create-network-interface.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my dual-stack network interface" \
    --private-ip-address 10.251.50.12 \
    --ipv6-addresses 2001:db8::1234:5678:1.2.3.4 \
    --groups sg-1234567890abcdef0
```

Esempio 3: per creare un'interfaccia di rete con un numero di indirizzi IP secondari

Utilizza il comando create-network-interface. In questo esempio, Amazon EC2 sceglie sia l'indirizzo IP primario che gli indirizzi IP secondari.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my network interface" \
    --secondary-private-ip-address-count 2 \
    --groups sg-1234567890abcdef0
```

Esempio 4: per creare un'interfaccia di rete con un indirizzo IP secondario specifico

Utilizza il comando create-network-interface. Questo esempio specifica un indirizzo IP primario e un indirizzo IP secondario.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my network interface" \
    --private-ip-addresses PrivateIpAddress=10.0.1.30,Primary=true \
                           PrivateIpAddress=10.0.1.31,Primary=false
    --groups sg-1234567890abcdef0
```

PowerShell

Esempio 1: per creare un'interfaccia di rete con indirizzi IP scelti da Amazon EC2

Utilizza il cmdlet New-EC2NetworkInterface. Questo esempio crea un'interfaccia di rete con un indirizzo IPv4 pubblico e un indirizzo IPv6 scelto da Amazon EC2.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my dual-stack network interface" `
    -Ipv6AddressCount 1 `
    -Group sg-1234567890abcdef0
```

Esempio 2: per creare un'interfaccia di rete con indirizzi IP specifici

Utilizza il cmdlet New-EC2NetworkInterface.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my dual-stack network interface" `
    -PrivateIpAddress 10.251.50.12 `
    -Ipv6Address $ipv6addr `
    -Group sg-1234567890abcdef0
```

Definisci gli indirizzi IPv6 come segue.

```
$ipv6addr = New-Object Amazon.EC2.Model.InstanceIpv6Address
$ipv6addr1.Ipv6Address = "2001:db8::1234:5678:1.2.3.4"
```

Esempio 3: per creare un'interfaccia di rete con un numero di indirizzi IP secondari

Utilizza il cmdlet New-EC2NetworkInterface. In questo esempio, Amazon EC2 sceglie sia l'indirizzo IP primario che gli indirizzi IP secondari.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my network interface" `
    -SecondaryPrivateIpAddressCount 2 `
    -Group sg-1234567890abcdef0
```

Esempio 4: per creare un'interfaccia di rete con un indirizzo IP secondario specifico

Utilizza il cmdlet New-EC2NetworkInterface. Questo esempio specifica un indirizzo IP primario e un indirizzo IP secondario.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
```

```
    -Description "my network interface" `
    -PrivateIpAddresses @($primary, $secondary) `
    -Group sg-1234567890abcdef0
```

Definisci gli indirizzi secondari come segue.

```
$primary = New-Object Amazon.EC2.Model.PrivateIpAddressSpecification
$primary.PrivateIpAddress = "10.0.1.30"
$primary.Primary = $true
$secondary = New-Object Amazon.EC2.Model.PrivateIpAddressSpecification
$secondary.PrivateIpAddress = "10.0.1.31"
$secondary.Primary = $false
```

Allegati dell'interfaccia di rete per l'istanza EC2

Puoi creare interfacce di rete da utilizzare per le tue istanze EC2 come interfacce di rete primarie o secondarie. Devi collegare un'interfaccia di rete a un'istanza EC2 se è nella stessa zona di disponibilità dell'interfaccia di rete. Il tipo di istanza determina quante interfacce di rete è possibile collegare all'istanza. Per ulteriori informazioni, consulta the section called “Indirizzi IP per interfaccia di rete”.

Considerazioni

- Puoi collegare un'interfaccia di rete a un'istanza quando è in esecuzione (collegamento a caldo), quando è arrestata (collegamento standard) o quando l'istanza viene avviata (collegamento a freddo).
- Puoi scollegare le interfacce di rete secondarie quando l'istanza è in esecuzione o arrestata. Non puoi tuttavia distaccare l'interfaccia di rete primaria.
- Puoi scollegare un'interfaccia di rete secondaria da un'istanza e collegarla a un'altra istanza.
- Quando avvii un'istanza utilizzando la CLI, l'API o un SDK, è possibile specificare l'interfaccia di rete primaria e interfacce di rete aggiuntive. Tieni presente che non puoi abilitare l’assegnazione automatica di indirizzi IPv4 pubblici se aggiungi un’interfaccia di rete secondaria durante l’avvio.
- L'avvio di un'istanza Amazon Linux o Windows Server con più interfacce di rete configura automaticamente le interfacce, gli indirizzi IPv4 privati e le tabelle di routing sul sistema operativo dell'istanza.
- Un collegamento di tipo warm o hot di un'interfaccia di rete aggiuntiva potrebbe richiedere l'implementazione manuale di una seconda interfaccia, la configurazione dell'indirizzo IPv4

privato e la modifica della tabella di routing. Le istanze che eseguono Amazon Linux o Windows Server riconoscono automaticamente il collegamento di tipo warm o a caldo ed eseguono automaticamente la configurazione.

- Non è possibile collegare un'altra interfaccia di rete a un'istanza (ad esempio una configurazione di un gruppo di NIC) per aumentare o raddoppiare la larghezza di banda della rete dalla o all'istanza dual-homed.
- Se colleghi più interfacce di rete della stessa sottorete a un'istanza, potresti riscontrare errori a livello di rete, ad esempio il routing asimmetrico. Se possibile, aggiungi invece un indirizzo IPv4 privato secondario sull'interfaccia di rete primaria.
- Per le istanze EC2 in una IPv6-only sottorete, se si collega un'interfaccia di rete secondaria, il nome host DNS privato dell'interfaccia di rete secondaria si risolve nell'indirizzo IPv6 primario per l'interfaccia di rete primaria.
- [Istanze di Windows]: se aggiungi più interfacce di rete a un'istanza, devi configurarle in modo che utilizzino il routing statico.

Collega un'interfaccia di rete

Puoi collegare un'interfaccia di rete a qualsiasi istanza nella stessa zona di disponibilità dell'interfaccia di rete, utilizzando la pagina Istanze o Interfacce di rete della console Amazon EC2. In alternativa, puoi specificare interfacce di rete esistenti all'avvio delle istanze.

Se l'indirizzo IPv4 pubblico sull'istanza viene rilasciato, l'istanza non ne riceverà uno nuovo se è presente più di un'interfaccia di rete collegata all'istanza. Per ulteriori informazioni sul funzionamento degli indirizzi IPv4 pubblici, consulta Indirizzi IPv4 pubblici.

Console

Per collegare un'interfaccia di rete utilizzando la pagina Istanze

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona la casella di controllo relativa all'istanza.
4. Scegliere Actions (Operazioni), Networking (Reti), Attach network interface (Collega interfaccia di rete).
5. Selezione di un VPC. L'interfaccia di rete può risiedere nello stesso VPC dell'istanza o in un altro VPC di tua proprietà, purché l'interfaccia di rete si trovi nella stessa zona di disponibilità

dell'istanza. Ciò consente di creare istanze multi-homed su VPC con configurazioni di rete e sicurezza differenti.

6. Selezionare un'interfaccia di rete. Se l'istanza supporta più schede di rete, è possibile scegliere una scheda di rete.
7. Scegliere Attach (Collega).

Per collegare un'interfaccia di rete a utilizzando la pagina Interfacce di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete.
4. Seleziona Operazioni, Collega volume.
5. Scegli un'istanza. Se l'istanza supporta più schede di rete, è possibile scegliere una scheda di rete.
6. Scegliere Attach (Collega).

AWS CLI

Per collegare un'interfaccia di rete

Utilizza il seguente comando attach-network-interface.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-1234567890abcdef0 \
    --instance-id i-1234567890abcdef0 \
    --device-index 1
```

PowerShell

Per collegare un'interfaccia di rete

Utilizza il cmdlet Add-EC2NetworkInterface.

```
Add-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -InstanceId i-1234567890abcdef0 `
```

```
    -DeviceIndex 1
```

Scollega un'interfaccia di rete

Puoi scollegare un'interfaccia di rete secondaria collegata a un'istanza EC2 in qualsiasi momento utilizzando la pagina Instances (Istanze) o Network Interfaces (Interfacce di rete) della console Amazon EC2.

Se si tenta di scollegare un'interfaccia di rete collegata a una risorsa da un altro servizio, ad esempio un sistema di bilanciamento del carico Elastic Load Balancing, una funzione Lambda WorkSpace, un gateway NAT o un gateway NAT, viene visualizzato un messaggio di errore indicante che non si dispone dell'autorizzazione per accedere alla risorsa. Per individuare quale servizio ha creato la risorsa collegata a un'interfaccia di rete, controlla la descrizione dell'interfaccia di rete. Se si elimina la risorsa, viene eliminata anche la sua interfaccia di rete.

Console

Per scollegare un'interfaccia di rete utilizzando la pagina Istanze

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona la casella di controllo relativa all'istanza. Controlla la sezione Interfacce di rete della scheda Rete per verificare che l'interfaccia dell'istanza di rete sia collegata a un'istanza come interfaccia di rete secondaria.
4. Scegliere Actions (Operazioni), Networking (Reti), Detach network interface (Scollega interfaccia di rete).
5. Selezionare l'interfaccia di rete e scegliere Detach (Scollega).

Per scollegare un'interfaccia di rete utilizzando la pagina Interfacce di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete. Controlla la sezione Dettagli istanza della scheda Dettagli per verificare che l'interfaccia dell'istanza di rete sia collegata a un'istanza come interfaccia di rete secondaria.
4. Seleziona Operazioni, Elimina.

5. Quando viene richiesta la conferma, seleziona Detach (Scollega).
6. Se non è possibile scollegare l'interfaccia di rete dall'istanza, seleziona Forza scollegamento, Attiva, quindi riprova. Si consiglia di forzare lo scollegamento solo come ultima risorsa. La forzatura di uno scollegamento può impedire di collegare un'interfaccia di rete diversa sullo stesso indice fino a quando non si riavvia l'istanza. Può anche impedire ai metadati dell'istanza di mostrare che l'interfaccia di rete è stata scollegata fino a quando non si riavvia l'istanza.

AWS CLI

Per scollegare un'interfaccia di rete

Utilizza il comando describe-network-interface.

```
aws ec2 detach-network-interface --attachment-id eni-attach-016c93267131892c9
```

PowerShell

Per scollegare un'interfaccia di rete

Utilizza il cmdlet Dismount-EC2NetworkInterface.

```
Dismount-EC2NetworkInterface -AttachmentId eni-attach-016c93267131892c9
```

Gestire gli indirizzi IP per le interfacce di rete

È possibile gestire i seguenti indirizzi IP per le interfacce di rete:

- Indirizzi IP elastici (uno per indirizzo IPv4 privato)
- Indirizzi IPv4
- Indirizzi IPv6

Console

Per gestire gli indirizzi IP di un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo relativa all'interfaccia di rete.
4. Per gestire gli indirizzi IPv4 e IPv6, procedi come segue:
    a. Seleziona Operazioni, Gestisci indirizzi IP.
    b. Espandere l'interfaccia di rete.
    c. Per Indirizzi IPv4, modifica gli indirizzi IP secondo necessità. Per assegnare un indirizzo IPv4 aggiuntivo, scegli Assegna nuovo indirizzo IP, quindi specifica un indirizzo IPv4 dall'intervallo di sottorete o lascia che ne scelga uno per te. AWS
    d. (Dual stack o solo IPv6) Per gli indirizzi IPv6, modifica gli indirizzi IP secondo necessità. Per assegnare un indirizzo IPv6 aggiuntivo, scegli Assegna nuovo IP, quindi specifica un indirizzo IPv6 dall'intervallo di sottoreti o lascia che AWS ne scelga uno per te.
    e. Per assegnare o annullare l'assegnazione di un indirizzo IPv4 pubblico a un'interfaccia di rete, scegli IP pubblico. Auto-assign Puoi abilitarlo o disabilitarlo per qualsiasi interfaccia di rete, ma influisce solo sull'interfaccia di rete primaria.
    f. (Dual stack o IPv6-only) Per Assegna IP IPv6 primario, scegli Abilita per assegnare un indirizzo IPv6 primario. Il primo GUA associato all'interfaccia di rete è scelto come indirizzo IPv6 primario. Dopo aver assegnato un indirizzo IPv6 primario, non puoi modificarlo. Questo indirizzo è l'indirizzo IPv6 primario fino alla terminazione dell'istanza o allo scollegamento dell'interfaccia di rete.
    g. Selezionare Salva.
5. Per associare un indirizzo IP elastico, effettuare le seguenti operazioni:
    a. Quindi seleziona Actions (Operazioni), Associate address (Associa indirizzo).
    b. In Indirizzo, seleziona l'indirizzo IP elastico.
    c. Per Indirizzo IPv4 privato, seleziona l'indirizzo IPv4 privato da associare all'indirizzo IP elastico.
    d. (Facoltativo) Seleziona Consenti di riassociare l'indirizzo IP elastico se l'interfaccia di rete è attualmente associata a un'altra istanza o interfaccia di rete.
    e. Seleziona Associate (Associa).
6. Per disassociare un indirizzo IP elastico, effettuare le seguenti operazioni:
    a. Selezionare Actions (Operazioni), scegliere Disassociate address (Disassocia indirizzo).
    b. In Indirizzo IP pubblico, seleziona l'indirizzo IP elastico.

c. Selezionare Disassociate (Annulla associazione).

AWS CLI

Per gestire gli indirizzi IPv4

Utilizza il seguente comando assign-private-ip-addresses per assegnare un indirizzo IPv4.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --private-ip-addresses 10.0.0.82
```

Utilizza il seguente comando unassign-private-ip-addresses per rimuovere l'assegnazione di un indirizzo IPv4.

```
aws ec2 unassign-private-ip-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --private-ip-addresses 10.0.0.82
```

Per gestire gli indirizzi IPv6

Utilizza il seguente comando assign-ipv6-addresses per assegnare un indirizzo IPv6.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Utilizza il seguente comando unassign-ipv6-addresses per rimuovere l'assegnazione di un indirizzo IPv6.

```
aws ec2 unassign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Per gestire l'indirizzo IP elastico per l'indirizzo IPv4 privato primario

Utilizza il seguente comando associate-address per associare un indirizzo IP elastico all'indirizzo IPv4 privato primario.

```
aws ec2 associate-address \
    --allocation-id eipalloc-0b263919b6EXAMPLE \
    --network-interface-id eni-1234567890abcdef0
```

Utilizza il seguente comando disassociate-address per dissociare un indirizzo IP elastico dall'indirizzo IPv4 privato primario.

```
aws ec2 disassociate-address --association-id eipassoc-2bebb745a1EXAMPLE
```

PowerShell

Per gestire gli indirizzi IPv4

Utilizza il Register-EC2PrivateIpAddress cmdlet per assegnare un indirizzo IPv4.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -PrivateIpAddress 10.0.0.82
```

Utilizzare il Unregister-EC2PrivateIpAddress cmdlet per annullare l'assegnazione di un indirizzo IPv4.

```
Unregister-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -PrivateIpAddress 10.0.0.82
```

Per gestire gli indirizzi IPv6

Utilizzare il Register-EC2Ipv6AddressList cmdlet per assegnare un indirizzo IPv6.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Utilizzare il Unregister-EC2Ipv6AddressList cmdlet per annullare l'assegnazione di un indirizzo IPv6.

```
Unregister-EC2Ipv6AddressList `
```

```
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Per gestire l'indirizzo IP elastico per l'indirizzo IPv4 privato primario

Utilizza il Register-EC2Address cmdlet per associare un indirizzo IP elastico all'indirizzo IPv4 privato primario.

```
Register-EC2Address `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -AllocationId eipalloc-0b263919b6EXAMPLE
```

Utilizza il Unregister-EC2Address cmdlet per dissociare un indirizzo IP elastico dall'indirizzo IPv4 privato primario.

```
Unregister-EC2Address -AssociationId eipassoc-2bebb745a1EXAMPLE
```

Modifica degli attributi dell'interfaccia di rete

È possibile modificare i seguenti attributi dell'interfaccia di rete:

- Descrizione
- Gruppi di sicurezza
- Elimina al termine
- Source/destination controllare
- Timeout di tracciamento delle connessioni inattive

Considerazioni

Non puoi scollegare un'interfaccia di rete gestita dal richiedente.

Console

Per modificare gli attributi dell'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).

3. Seleziona la casella di controllo relativa all'interfaccia di rete.
4. Per modificare la descrizione, procedi come segue:
   a. Scegli Operazioni, Modifica descrizione.
   b. In Description (Descrizione), inserire una descrizione.
   c. Selezionare Salva.
5. Per modificare i gruppi di sicurezza, procedi come segue:
   a. Seleziona Operazioni, Gestisci gruppi di sicurezza.
   b. Per Gruppi di sicurezza associati, aggiungi e rimuovi i gruppi di sicurezza secondo necessità. Il gruppo di protezione e l'interfaccia di rete devono essere creati per lo stesso VPC.
   c. Selezionare Salva.
6. Per modificare il comportamento di terminazione, procedi come segue:
   a. Seleziona Operazioni, Modifica comportamento di risoluzione.
   b. Seleziona o deseleziona Elimina alla terminazione, Abilita.
   c. Selezionare Salva.
7. Per modificare il source/destination controllo, procedi come segue:
   a. Scegli Azioni, source/dest Verifica modifica.
   b. Seleziona o deseleziona il Source/destination segno di spunta, Abilita.
   c. Selezionare Salva.
8. Per modificare i timeout di tracciamento delle connessioni inattive, procedi come seuge:
   a. Scegli Azioni, Modifica il timeout di tracciamento della connessione inattiva.
   b. Modifica i valori di timeout secondo necessità. Per ulteriori informazioni, consulta Timeout di tracciamento delle connessioni inattive.
      - Timeout TCP stabilito: il timeout (in secondi) per le connessioni TCP inattive in uno stato stabilito.
        - Minimo: `60` secondi
        - Massimo: `432000` secondi
        - Predefinito: `350` secondi per i tipi di istanze Nitro v6 (esclusi P6e-GB200); `432000` secondi per tutti gli altri tipi di istanze (inclusi). P6e-GB200

- Consigliato: meno di `432000` secondi.
- Timeout UDP: il timeout (in secondi) per i flussi UDP inattivi che hanno registrato traffico solo in un'unica direzione o una singola transazione richiesta-risposta.
  - Minimo: `30` secondi
  - Massimo: `60` secondi
  - Impostazione predefinita: `30` secondi
- Timeout del flusso UDP: il timeout (in secondi) per i flussi UDP inattivi classificati come flussi che hanno registrato più di una transazione richiesta-risposta.
  - Minimo: `60` secondi
  - Massimo: `180` secondi
  - Impostazione predefinita: `180` secondi

c. Selezionare Salva.

AWS CLI

Example Esempio: per modificare la descrizione

Utilizza il seguente comando modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --description "my updated description"
```

Example Esempio: per modificare i gruppi di sicurezza

Utilizza il seguente comando modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --groups sg-1234567890abcdef0
```

Example Esempio: per modificare il comportamento di terminazione

Utilizza il seguente comando modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
```

```
    --attachment AttachmentId=eni-attach-43348162abEXAMPLE,DeleteOnTermination=false
```

Example Esempio: per abilitare il controllo source/destination

Utilizza il seguente comando modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --source-dest-check
```

Example Esempio: per modificare il timeout di tracciamento della connessione inattiva

Utilizza il seguente comando modify-network-interface-attribute. Per ulteriori informazioni, consulta Timeout di tracciamento delle connessioni inattive.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --connection-tracking-specification
 TcpEstablishedTimeout=172800,UdpStreamTimeout=90,UdpTimeout=60
```

PowerShell

Example Esempio: per modificare la descrizione

Utilizza il cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Description "my updated description"
```

Example Esempio: per modificare i gruppi di sicurezza

Utilizza il cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Group sg-1234567890abcdef0
```

Example Esempio: per modificare il comportamento di terminazione

Utilizza il cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Attachment_AttachmentId eni-attach-43348162abEXAMPLE `
    -Attachment_DeleteOnTermination $false
```

Example Esempio: per abilitare source/destination il controllo

Utilizza il cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -SourceDestCheck $true
```

Example Esempio: per modificare i timeout di tracciamento della connessione inattiva

Utilizza il cmdlet Edit-EC2NetworkInterfaceAttribute. Per ulteriori informazioni, consulta Timeout di tracciamento delle connessioni inattive.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -ConnectionTrackingSpecification_TcpEstablishedTimeout 172800 `
    -ConnectionTrackingSpecification_UdpStreamTimeout 90 `
    -ConnectionTrackingSpecification_UdpTimeout 60
```

Interfacce di rete multiple per istanze Amazon EC2

Il collegamento di più interfacce di rete a un'istanza risulta utile quando ti serve ciò che segue:

- Una gestione di rete.
- Apparecchiature di rete e di sicurezza.
- Dual-homed istanze con carichi di lavoro in diverse sottoreti o VPC. ???
- Una soluzione economica a elevata disponibilità.

Gestione di rete

La seguente panoramica descrive una gestione di rete creata utilizzando più interfacce di rete.

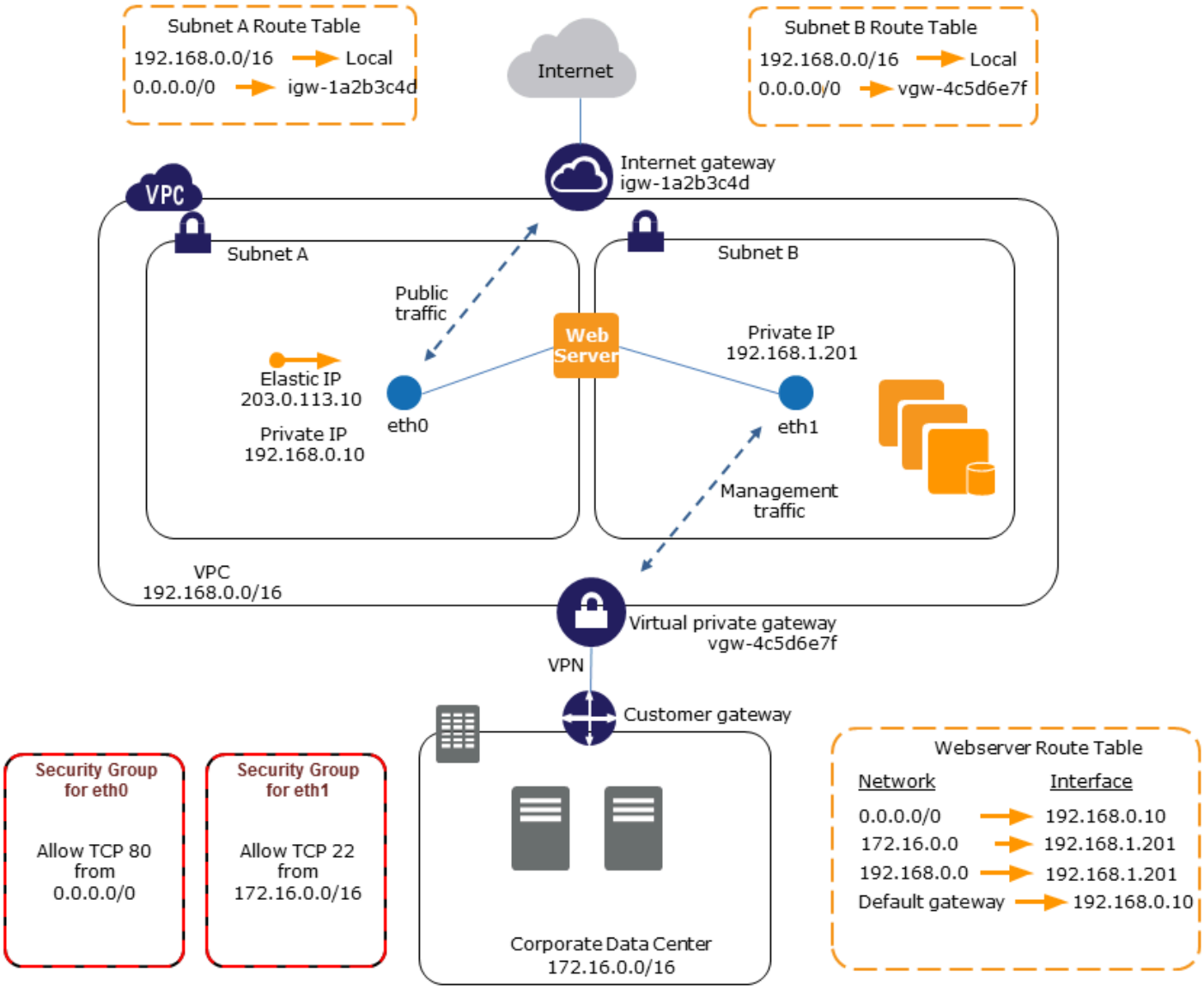
Criteri

- L'interfaccia di rete primaria sull'istanza (per esempio, eth0) gestisce il traffico pubblico.
- L'interfaccia di rete secondaria sull'istanza (per esempio, eth1) gestisce il traffico di gestione del backend. È connessa a una sottorete separata con controlli di accesso più restrittivi e si trova nella stessa zona di disponibilità dell'interfaccia di rete principale.

Settings

- L'interfaccia di rete principale, che può essere o meno dietro un sistema di bilanciamento del carico, ha un gruppo di sicurezza associato che consente l'accesso al server da Internet. Ad esempio, consenti le porte TCP 80 e 443 da 0.0.0. 0/0 o dal load balancer.
- L'interfaccia di rete secondaria ha un gruppo di sicurezza associato che consente solo l'accesso SSH, avviato da una delle seguenti posizioni:
  - Un intervallo consentito di indirizzi IP, all'interno del VPC privato virtuale o da Internet.
  - Una sottorete privata all'interno della stessa zona di disponibilità dell'interfaccia di rete principale.
  - Un gateway privato virtuale.

> **Note**
>
> Per garantire le funzionalità di failover, considera di utilizzare un indirizzo IPv4 privato secondario per il traffico in entrata su un'interfaccia di rete. In caso di errore di un'istanza, è possibile spostare l'indirizzo IPv4 privato and/or secondario dell'interfaccia in un'istanza standby.



Apparecchiature di rete e sicurezza

Alcune appliance di rete e sicurezza, ad esempio i load balancer, i server Network Address Translation (NAT) e i server proxy preferiscono una configurazione basata su più interfacce di rete. È possibile creare e collegare interfacce di rete secondarie alle istanze che eseguono questi tipi di applicazioni e configurare le interfacce aggiuntive con indirizzi IP pubblici e privati, gruppi di sicurezza e controlli propri. source/destination

Dual-homed istanze con carichi di lavoro in sottoreti diverse

Puoi inserire un'interfaccia di rete su ciascun server Web che si connette a una rete di livello intermedio in cui si trova un server applicazioni. Anche il server applicazioni può essere di tipo dual-homed in una rete backend (sottorete) in cui si trova il server di database. Anziché instradare i pacchetti di rete tramite istanze dual-homed, ogni istanza dual-homed riceve ed elabora le richieste sul front-end, stabilisce una connessione con il back-end, quindi invia le richieste ai server sulla rete back-end.

Dual-homed istanze con carichi di lavoro in VPC diversi nello stesso account

Puoi avviare un'istanza EC2 in un VPC e collegare un ENI secondario da un altro VPC, purché l'interfaccia di rete i trovi nella stessa zona di disponibilità dell'istanza. Ciò consente di creare istanze multi-homed su VPC con configurazioni di rete e sicurezza differenti. Non puoi creare istanze multi-homed su VPC in account diversi. AWS

Puoi utilizzare le istanze dual-homed su più VPC nei seguenti casi d'uso:

- Supera le sovrapposizioni CIDR tra due VPC che non possono essere collegati tra loro: puoi sfruttare un CIDR secondario in un VPC e consentire a un'istanza di comunicare tra due intervalli IP non sovrapposti.
- Connetti più VPC all'interno di un unico account: abilita la comunicazione tra singole risorse che normalmente sarebbero separate dai confini del VPC.

Low-budget, soluzione ad alta disponibilità

Se una delle istanze che servono una particolare funzione si guasta, la relativa interfaccia di rete può essere collegata a un'istanza sostitutiva o hot standby preconfigurata per lo stesso ruolo per ripristinare rapidamente il servizio. Ad esempio, puoi creare un'interfaccia di rete come interfaccia di rete primaria o secondaria per un servizio fondamentale, ad esempio un'istanza di database o un'istanza NAT. Se l'istanza non riesce, tu (o più probabilmente il codice eseguito per tuo conto) puoi collegare l'interfaccia di rete a un'istanza hot standby. Dal momento che l'interfaccia conserva i propri indirizzi IP privati, gli indirizzi IP elastici e l'indirizzo MAC, il traffico di rete comincia a essere indirizzato all'istanza in standby non appena colleghi l'interfaccia di rete all'istanza di sostituzione. Gli utenti rileveranno una breve interruzione della connettività tra il momento in cui l'esecuzione dell'istanza non riesce e il momento in cui l'interfaccia di rete viene collegata all'istanza in standby. Non è tuttavia richiesta alcuna modifica alla tabella di routing VPC o al server DNS.

Requester-managed interfacce di rete

Un'interfaccia di rete gestita dal richiedente è un'interfaccia di rete che un Servizio AWS crea nel VPC per tuo conto. L'interfaccia di rete è associata a una risorsa per un altro servizio, ad esempio un'istanza database di Amazon RDS, un gateway NAT o un endpoint VPC di interfaccia da AWS PrivateLink.

Considerazioni

- Puoi visualizzare le interfacce di rete gestite dal richiedente nel tuo account e aggiungere o rimuovere tag. Tuttavia, non puoi eseguire le seguenti azioni su un'interfaccia di rete gestita dal richiedente:
  - Modifica degli attributi dell'interfaccia di rete
  - Collegare o scollegare l'interfaccia di rete
  - Associare o dissociare gli indirizzi IP elastici
  - Assegna o annulla l'assegnazione di indirizzi IP privati
  - Specificate l'interfaccia di rete quando avviate un'istanza

  Puoi comunque reimpostare gli attributi dell'interfaccia di rete, anche se non puoi modificarli.
- Quando si elimina la risorsa associata a un'interfaccia di rete gestita dal richiedente, l'interfaccia di rete Servizio AWS viene scollegata e la elimina. Se il servizio ha scollegato un'interfaccia di rete ma non l'ha eliminata, puoi eliminare l'interfaccia di rete scollegata.

Console

Per visualizzare le interfacce di rete gestite dal richiedente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegli Network & Security (Rete e sicurezza), quindi Network Interfaces (Interfacce di rete).
3. Seleziona l'ID dell'interfaccia di rete per aprirne la pagina dei dettagli.
4. Di seguito sono riportati i campi chiave che puoi usare per determinare lo scopo dell'interfaccia di rete:
   - Description (Descrizione): una descrizione fornita dal servizio AWS che ha creato l'interfaccia. Ad esempio, "VPC Endpoint Interface vpce 089f2123488812123".

- Requester-managed: indica se l'interfaccia di rete è gestita da. AWS
- ID richiedente: l'alias o l'ID dell' AWS account del committente o del servizio che ha creato l'interfaccia di rete. Se hai creato l'interfaccia di rete, questo è il tuo Account AWS ID. In caso contrario, è stata creata da un'altra entità principale o da un altro servizio.

AWS CLI

Per visualizzare le interfacce di rete gestite dal richiedente

Usa il comando describe-network-interfaces come indicato di seguito.

```
aws ec2 describe-network-interfaces \
    --filters "Name=requester-managed,Values=true" \
    --query "NetworkInterfaces[*].[Description, InterfaceType]" \
    --output table
```

Di seguito è riportato un output di esempio che mostra i campi chiave che puoi usare per determinare lo scopo dell'interfaccia di rete: `Description` e `InterfaceType`.

```
-------------------------------------------------------------------------------
|                          DescribeNetworkInterfaces                          |
+-----------------------------------------------------+-------------------------+
|  VPC Endpoint Interface: vpce-0f00567fa8477a1e6     |  interface              |
|  VPC Endpoint Interface vpce-0d8ddce4be80e4474      |  interface              |
|  VPC Endpoint Interface vpce-078221a1e27d1ea5b      |  vpc_endpoint           |
|  Resource Gateway Interface rgw-0bba03f3d56060135   |  interface              |
|  VPC Endpoint Interface: vpce-0cc199f605eaeace7     |  interface              |
|  VPC Endpoint Interface vpce-019b90d6f16d4f958      |  interface              |
+-----------------------------------------------------+-------------------------+
```

PowerShell

Per visualizzare le interfacce di rete gestite dal richiedente

Utilizza il cmdlet Get-EC2NetworkInterface come riportato di seguito.

```
Get-EC2NetworkInterface -Filter @{Name="requester-managed"; Values="true"} | Select
 Description, InterfaceType
```

Di seguito è riportato un output di esempio che mostra i campi chiave che puoi usare per determinare lo scopo di un'interfaccia di rete: `Description` e `InterfaceType`.

```
Description                                        InterfaceType
-----------                                        -------------
VPC Endpoint Interface: vpce-0f00567fa8477a1e6   interface
VPC Endpoint Interface vpce-0d8ddce4be80e4474    interface
VPC Endpoint Interface vpce-078221a1e27d1ea5b    vpc_endpoint
Resource Gateway Interface rgw-0bba03f3d56060135 interface
VPC Endpoint Interface: vpce-0cc199f605eaeace7   interface
VPC Endpoint Interface vpce-019b90d6f16d4f958    interface
```

Delega del prefisso per Interfacce di rete Amazon EC2

È possibile assegnare un intervallo CIDR IPv4 o IPv6 privato, automaticamente o manualmente, alle interfacce di rete. Assegnando i prefissi, è possibile dimensionare e semplificare la gestione delle applicazioni, incluse le applicazioni container e di rete che richiedono più indirizzi IP su un'istanza. Per ulteriori informazioni sugli indirizzi IPv4 e IPv6, consulta Indirizzamento IP per le istanze Amazon EC2.

Sono disponibili le seguenti opzioni di incarico:

- Assegnazione automatica: AWS sceglie il prefisso e lo assegna all'interfaccia di rete. Se la sottorete per l'interfaccia di rete dispone di una prenotazione CIDR della sottorete di tipo `prefix`, selezioniamo i prefissi da tale prenotazione. In caso contrario, li selezioniamo dall'intervallo CIDR della sottorete.
- Assegnazione manuale: si specifica il prefisso e si AWS verifica che non sia già assegnato ad altre risorse prima di assegnarlo all'interfaccia di rete.

L'assegnazione dei prefissi presenta i seguenti vantaggi:

- Aumento degli indirizzi IP su un'interfaccia di rete: quando si utilizza un prefisso, si assegna un blocco di indirizzi IP anziché singoli indirizzi IP. Questo aumenta il numero di indirizzi IP per un'interfaccia di rete.
- Gestione VPC semplificata per i container: nelle applicazioni container, ogni container richiede un indirizzo IP univoco. L'assegnazione dei prefissi alla tua istanza semplifica la gestione dei tuoi VPC, poiché puoi avviare e terminare i container senza dover chiamare le API Amazon EC2 per i singoli incarichi IP.

Indice

- Nozioni di base
- Considerazioni
- Gestisci i prefissi per le interfacce di rete
  - Assegnare i prefissi durante la creazione dell'interfaccia di rete
  - Assegnare prefissi a un'interfaccia di rete esistente
  - Rimuovere i prefissi dalle interfacce di rete

Nozioni di base

- È possibile assegnare un prefisso a interfacce di rete nuove o esistenti.
- Per utilizzare i prefissi, è necessario assegnare un prefisso all'interfaccia di rete, allegare l'interfaccia di rete all'istanza e configurare il sistema operativo.
- Quando si sceglie l'opzione per specificare un prefisso, il prefisso deve soddisfare i seguenti requisiti:
  - Il prefisso IPv4 che è possibile specificare è `/28`.
  - Il prefisso IPv6 che è possibile specificare è `/80`.
  - Il prefisso si trova nella sottorete CIDR dell'interfaccia di rete e non si sovrappone ad altri prefissi o indirizzi IP assegnati alle risorse esistenti nella sottorete.
- È possibile assegnare un prefisso all'interfaccia di rete primaria o secondaria.
- È possibile assegnare un indirizzo IP elastico a un'interfaccia di rete a cui è stato assegnato un prefisso.
- Puoi inoltre assegnare un indirizzo IP elastico alla parte di indirizzo IP del prefisso assegnato.
- Un nome host DNS privato (interno) di un'istanza viene risolto all'indirizzo IPv4 privato.
- Assegniamo ogni indirizzo IPv4 privato per un'interfaccia di rete, inclusi quelli dei prefissi, utilizzando il seguente formato:
  - Regione `us-east-1`

    ```
    ip-private-ipv4-address.ec2.internal
    ```

  - Tutte le altre Regioni

    ```
    ip-private-ipv4-address.region.compute.internal
    ```

Considerazioni

Quando si utilizzano i prefissi, prendere in considerazione quanto segue:

- Le interfacce di rete con prefissi sono supportate con le istanze. Nitro-based
- I prefissi per le interfacce di rete devono utilizzare indirizzi IPv6 o indirizzi IPv4 privati.
- Il numero massimo di indirizzi IP che è possibile assegnare a un'interfaccia di rete dipende dal tipo di istanza. Ogni prefisso assegnato a un'interfaccia di rete conta come un unico indirizzo IP. Ad esempio, un'istanza `c5.large` ha un limite di `10` indirizzi IPv4 per interfaccia di rete. Ogni interfaccia di rete per questa istanza ha un indirizzo IPv4 primario. Se un'interfaccia di rete non ha indirizzi IPv4 secondari, è possibile assegnare fino a 9 prefissi all'interfaccia di rete. Per ogni indirizzo IPv4 aggiuntivo assegnato a un'interfaccia di rete, a questa è possibile assegnare un prefisso in meno. Per ulteriori informazioni, consulta Numero massimo di indirizzi IP per interfaccia di rete.
- I prefissi sono inclusi nei controlli. source/destination
- Devi configurare il sistema operativo affinché funzioni con le interfacce di rete con prefissi. Tenere presente quanto segue:
  - Alcune AMI Amazon Linux contengono script aggiuntivi installati da AWS, noti come. `ec2-net-utils` Questi script automatizzano facoltativamente la configurazione delle interfacce di rete. Sono disponibili per l'uso solo per Amazon Linux.
  - Per i container, puoi utilizzare un'interfaccia di rete container (CNI) per il plug-in Kubernetes, oppure `dockerd` se gestisci i container con Docker.

Gestisci i prefissi per le interfacce di rete

Quando assegni prefissi a un'interfaccia di rete, puoi scegliere di consentirci di assegnarli automaticamente o specificare prefissi personalizzati. Se ci consenti di assegnare automaticamente i prefissi e la sottorete per l'interfaccia di rete dispone di una prenotazione CIDR della sottorete di tipo `prefix`, selezioniamo i prefissi da tale prenotazione. In caso contrario, li selezioniamo dall'intervallo CIDR della sottorete.

Processi

- Assegnare i prefissi durante la creazione dell'interfaccia di rete
- Assegnare prefissi a un'interfaccia di rete esistente
- Rimuovere i prefissi dalle interfacce di rete

Assegnare i prefissi durante la creazione dell'interfaccia di rete

Puoi assegnare prefissi automatici o personalizzati quando crei un'interfaccia di rete.

Console

Per assegnare prefissi automatici durante la creazione dell'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona Crea interfaccia di rete.
4. inserisci una descrizione per l'interfaccia di rete, selezionare la sottorete in cui creare l'interfaccia di rete e configurare gli indirizzi IPv4 e IPv6 privati.
5. Espandere Advanced settings (Impostazioni avanzate).
6. Per la delega del prefisso IPv4, effettua una delle seguenti operazioni:
   - Per assegnare automaticamente un prefisso IPv4, scegli. Auto-assign Per Numero di prefissi IPv4, inserisci il numero di prefissi da assegnare.
   - Per assegnare un prefisso IPv4 specifico, scegli Personalizzato. Scegli Aggiungi nuovo prefisso e inserisci il prefisso.
7. Per la delega del prefisso IPv6, effettua una delle seguenti operazioni:
   - Per assegnare automaticamente un prefisso IPv6, scegli. Auto-assign Per Numero di prefissi IPv6, inserisci il numero di prefissi da assegnare.
   - Per assegnare un prefisso IPv6 specifico, scegli Personalizzato. Scegli Aggiungi nuovo prefisso e inserisci il prefisso.

   > **Note**
   >
   > L'opzione IPv6 prefix delegation (Delega del prefisso IPv6) viene visualizzata solo se la sottorete selezionata è abilitata per IPv6.

8. Selezionare i gruppi di sicurezza da associare all'interfaccia di rete e assegnare i tag di risorse se necessario.
9. Seleziona Crea un'interfaccia di rete.

AWS CLI

Per assegnare prefissi IPv4 automatici durante la creazione dell'interfaccia di rete

Utilizzate il comando create-network-interface e impostate il numero di prefissi IPv4 `--ipv4-prefix-count` da assegnare. AWS Nel seguente esempio, assegna un prefisso IPv4. AWS

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 automatic example" \
    --ipv4-prefix-count 1
```

Per assegnare prefissi IPv4 specifici durante la creazione dell'interfaccia di rete

Usa il comando create-network-interface e imposta `--ipv4-prefixes` sui prefissi. AWS seleziona gli indirizzi IPv4 da questo intervallo. Nell'esempio seguente, il prefisso CIDR è 10.0.0.208/28.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 manual example" \
    --ipv4-prefixes Ipv4Prefix=10.0.0.208/28
```

Per assegnare prefissi IPv6 automatici durante la creazione dell'interfaccia di rete

Utilizzate il comando create-network-interface e impostatelo sul numero di prefissi IPv6 `--ipv6-prefix-count` da assegnare. AWS Nel seguente esempio, assegna un prefisso IPv6. AWS

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 automatic example" \
    --ipv6-prefix-count 1
```

Per assegnare prefissi IPv6 specifici durante la creazione dell'interfaccia di rete

Usa il comando create-network-interface e imposta `--ipv6-prefixes` sui prefissi. AWS seleziona gli indirizzi IPv6 da questo intervallo. Nell'esempio seguente, il prefisso CIDR è 2600:1f13:fc2:a700:1768::/80.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 manual example" \
```

```
    --ipv6-prefixes Ipv6Prefix=2600:1f13:fc2:a700:1768::/80
```

PowerShell

Per assegnare prefissi IPv4 automatici durante la creazione dell'interfaccia di rete

Utilizzare il New-EC2NetworkInterface cmdlet e impostarlo sul numero di prefissi `Ipv4PrefixCount` IPv4 da assegnare. AWS Nel seguente esempio, assegna un prefisso IPv4. AWS

```
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv4 automatic example' `
    -Ipv4PrefixCount 1
```

Per assegnare prefissi IPv4 specifici durante la creazione dell'interfaccia di rete

Utilizza il New-EC2NetworkInterface cmdlet e imposta i prefissi. `Ipv4Prefix` AWS seleziona gli indirizzi IPv4 da questo intervallo. Nell'esempio seguente, il prefisso CIDR è 10.0.0.208/28.

```
Import-Module AWS.Tools.EC2
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv4 manual example' `
    -Ipv4Prefix (New-Object `
        -TypeName Amazon.EC2.Model.Ipv4PrefixSpecificationRequest `
        -Property @{Ipv4Prefix = '10.0.0.208/28'})
```

Per assegnare prefissi IPv6 automatici durante la creazione dell'interfaccia di rete

Utilizza il New-EC2NetworkInterface cmdlet e imposta il numero di `Ipv6PrefixCount` prefissi IPv6 da assegnare. AWS Nel seguente esempio, assegna un prefisso IPv6. AWS

```
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv6 automatic example' `
    -Ipv6PrefixCount 1
```

Per assegnare prefissi IPv6 specifici durante la creazione dell'interfaccia di rete

Utilizza il New-EC2NetworkInterface cmdlet e imposta i prefissi. `Ipv6Prefixes` AWS seleziona gli indirizzi IPv6 da questo intervallo. Nell'esempio seguente, il prefisso CIDR è 2600:1f13:fc2:a700:1768::/80.

```
Import-Module AWS.Tools.EC2
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv6 manual example' `
    -Ipv6Prefix (New-Object `
        -TypeName Amazon.EC2.Model.Ipv6PrefixSpecificationRequest `
        -Property @{Ipv6Prefix = '2600:1f13:fc2:a700:1768::/80'})
```

Assegnare prefissi a un'interfaccia di rete esistente

Puoi assegnare dei prefissi automatici o personalizzati a un'interfaccia di rete esistente.

Console

Per assegnare prefissi automatici a un'interfaccia di rete esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Network Interfaces (Interfacce di rete).
3. Selezionare l'interfaccia di rete a cui assegnare i prefissi e scegliere Actions (Operazioni), Manage prefixes (Gestisci prefissi).
4. Per la delega del prefisso IPv4, effettua una delle seguenti operazioni:
   - Per assegnare automaticamente un prefisso IPv4, scegli. Auto-assign Per Numero di prefissi IPv4, inserisci il numero di prefissi da assegnare.
   - Per assegnare un prefisso IPv4 specifico, scegli Personalizzato. Scegli Aggiungi nuovo prefisso e inserisci il prefisso.
5. Per la delega del prefisso IPv6, effettua una delle seguenti operazioni:
   - Per assegnare automaticamente un prefisso IPv6, scegli. Auto-assign Per Numero di prefissi IPv6, inserisci il numero di prefissi da assegnare.
   - Per assegnare un prefisso IPv6 specifico, scegli Personalizzato. Scegli Aggiungi nuovo prefisso e inserisci il prefisso.

> **Note**
>
> L'opzione IPv6 prefix delegation (Delega del prefisso IPv6) viene visualizzata solo se la sottorete selezionata è abilitata per IPv6.

6. Scegli Save (Salva).

AWS CLI

Usa il comando assign-ipv6-addresses per assegnare prefissi IPv6 e il comando assign-private-ip-addresses per assegnare prefissi IPv4 alle interfacce di rete esistenti.

Per assegnare prefissi IPv4 automatici a un'interfaccia di rete esistente

Utilizzate il comando assign-private-ip-addresses e impostatelo sul numero di prefissi IPv4 `--ipv4-prefix-count` da assegnare. AWS Nel seguente esempio, assegna un prefisso IPv4. AWS

```
aws ec2 assign-private-ip-addresses \
    --network-interface-id eni-081fbb4095EXAMPLE \
    --ipv4-prefix-count 1
```

Per assegnare prefissi IPv4 specifici a un'interfaccia di rete esistente

Utilizzare il comando assign-private-ip-addresses e impostare `--ipv4-prefixes` sul prefisso. AWS seleziona gli indirizzi IPv4 da questo intervallo. Nell'esempio seguente, il prefisso CIDR è 10.0.0.208/28.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-id eni-081fbb4095EXAMPLE \
    --ipv4-prefixes 10.0.0.208/28
```

Per assegnare prefissi IPv6 automatici a un'interfaccia di rete esistente

Utilizzate il comando assign-ipv6-addresses e impostatelo sul numero di prefissi IPv6 `--ipv6-prefix-count` da assegnare. AWS Nel seguente esempio, assegna un prefisso IPv6. AWS

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-00d577338cEXAMPLE \
```

```
    --ipv6-prefix-count 1
```

Per assegnare prefissi IPv6 specifici a un'interfaccia di rete esistente

Utilizzate il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/assign-ipv6-addresses.html assign-ipv6-addresses e impostatelo sul prefisso. `--ipv6-prefixes` AWS seleziona gli indirizzi IPv6 da questo intervallo. Nell'esempio seguente, il prefisso CIDR è 2600:1f13:fc2:a700:18bb::/80.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-00d577338cEXAMPLE \
    --ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

PowerShell

Per assegnare prefissi IPv4 automatici a un'interfaccia di rete esistente

Utilizza il Register-EC2PrivateIpAddress cmdlet e imposta il numero di `Ipv4PrefixCount` prefissi IPv4 da assegnare. AWS Nel seguente esempio, assegna un prefisso IPv4. AWS

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv4PrefixCount 1
```

Per assegnare prefissi IPv4 specifici a un'interfaccia di rete esistente

Usa il Register-EC2PrivateIpAddress cmdlet e imposta il prefisso. `Ipv4Prefix` AWS seleziona gli indirizzi IPv4 da questo intervallo. Nell'esempio seguente, il prefisso CIDR è 10.0.0.208/28.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv4Prefix '10.0.0.208/28'
```

Per assegnare prefissi IPv6 automatici a un'interfaccia di rete esistente

Utilizza il Register-EC2Ipv6AddressList cmdlet e imposta il numero di `Ipv6PrefixCount` prefissi IPv4 da assegnare. AWS Nel seguente esempio, assegna un prefisso IPv6. AWS

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv6PrefixCount 1
```

Per assegnare prefissi IPv6 specifici a un'interfaccia di rete esistente

Usa il Register-EC2Ipv6AddressList cmdlet e imposta il prefisso. `Ipv6Prefix` AWS seleziona gli indirizzi IPv6 da questo intervallo. Nell'esempio seguente, il prefisso CIDR è 2600:1f13:fc2:a700:18bb::/80.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv6Prefix '2600:1f13:fc2:a700:18bb::/80'
```

Rimuovere i prefissi dalle interfacce di rete

Puoi rimuovere i prefissi da un'interfaccia di rete esistente.

Console

Per rimuovere i prefissi da un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Selezionare l'interfaccia di rete.
4. Scegli Azioni, Gestisci prefissi.
5. Per la delega del prefisso IPv4, per rimuovere prefissi specifici, scegli Annulla assegnazione accanto ai prefissi da rimuovere. Per rimuovere tutti i prefissi, scegli Non assegnare.
6. Per la delega del prefisso IPv6, per rimuovere prefissi specifici, scegli Annulla assegnazione accanto ai prefissi da rimuovere. Per rimuovere tutti i prefissi, scegli Non assegnare.

   > **Note**
   >
   > L'opzione IPv6 prefix delegation (Delega del prefisso IPv6) viene visualizzata solo se la sottorete selezionata è abilitata per IPv6.

7. Scegli Save (Salva).

AWS CLI

Puoi utilizzare il comando unassign-ipv6-addresses per rimuovere i prefissi IPv6 e il comando unassign-private-ip-addresses per rimuovere i prefissi IPv4 dalle interfacce di rete esistenti.

Per rimuovere i prefissi IPv4 da un'interfaccia di rete

Usa il comando unassign-private-ip-addresses e imposta `--ipv4-prefix` sul prefisso CIDR da rimuovere.

```
aws ec2 unassign-private-ip-addresses \
    --network-interface-id eni-081fbb4095EXAMPLE \
    --ipv4-prefixes 10.0.0.176/28
```

Per rimuovere i prefissi IPv6 da un'interfaccia di rete

Usa il comando unassign-ipv6-addresses e imposta `--ipv6-prefix` sul prefisso CIDR da rimuovere.

```
aws ec2 unassign-ipv6-addresses \
    --network-interface-id eni-00d577338cEXAMPLE \
    --ipv6-prefix 2600:1f13:fc2:a700:18bb::/80
```

PowerShell

Per rimuovere i prefissi IPv4 da un'interfaccia di rete

Utilizzare il Unregister-EC2PrivateIpAddress cmdlet e impostarlo sul prefisso CIDR `Ipv4Prefix` per rimuoverlo.

```
Unregister-EC2PrivateIpAddress `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv4Prefix '10.0.0.208/28'
```

Per rimuovere i prefissi IPv6 da un'interfaccia di rete

Usa il Unregister-EC2Ipv6AddressList cmdlet e imposta il prefisso CIDR `Ipv6Prefix` per rimuoverlo.

```
Unregister-EC2Ipv6AddressList `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv6Prefix '2600:1f13:fc2:a700:18bb::/80'
```

Eliminazione di un'interfaccia di rete

L'eliminazione di un'interfaccia di rete rilascia tutti gli attributi associati all'interfaccia e gli indirizzi IP privati o gli indirizzi IP elastici utilizzati da un'altra istanza.

Non puoi eliminare un'interfaccia di rete in uso. Innanzitutto, è necessario Scollegare l'interfaccia di rete.

Console

Come eliminare un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Network Interfaces (Interfacce di rete).
3. Seleziona la casella di controllo dell'interfaccia di rete, quindi seleziona Operazioni, Elimina.
4. Quando viene richiesta la conferma, seleziona Elimina.

AWS CLI

Per eliminare un'interfaccia di rete

Utilizza il comando describe-network-interfaces.

```
aws ec2 delete-network-interface --network-interface-id eni-1234567890abcdef0
```

PowerShell

Per eliminare un'interfaccia di rete

Utilizza il cmdlet Remove-EC2NetworkInterface.

```
Remove-EC2NetworkInterface -NetworkInterfaceId eni-1234567890abcdef0
```

Larghezza di banda di rete dell'istanza Amazon EC2

Le specifiche della larghezza di banda dell'istanza si applicano sia al traffico in entrata che in uscita dell'istanza. Ad esempio, se un'istanza specifica fino a 10 Gbps di larghezza di banda, significa che

ha fino a 10 Gbps di larghezza di banda per il traffico in entrata e, al contempo, fino a 10 Gbps per il traffico in uscita. La larghezza di banda della rete disponibile per un'istanza EC2 dipende da diversi fattori, come descritto di seguito:

Multi-flow traffico

Quando il traffico passa attraverso un gateway Internet o un gateway locale, la larghezza di banda disponibile per il traffico a più flussi dipende dal tipo di istanza.

Tipi di istanza	Larghezza di banda disponibile
Tipi di istanza con meno di 32 vCPU	Limitato a 5 Gbps
Tipi di istanza con più di 32 vCPU	Limitato al 50% della larghezza di banda disponibile per il tipo di istanza
Istanze C8in, C8ine, M8in, M8ine, M8idn, R8in, R8idn	Limitato alla larghezza di banda di base per il tipo di istanza

Single-flow traffico

Quando le istanze non si trovano nello stesso gruppo di posizionamento del cluster, la larghezza di banda per il traffico a flusso singolo è limitata a 5 Gbps. Per ridurre la latenza e aumentare la larghezza di banda a flusso singolo, prova una delle seguenti opzioni:

- Utilizza un gruppo di collocazione cluster per ottenere una larghezza di banda fino a 10 Gbps per le istanze all'interno dello stesso gruppo di collocazione.
- Imposta più percorsi tra due endpoint qualsiasi per ottenere una maggiore larghezza di banda con Multipath TCP (MPTCP).
- Configura ENA Express per le istanze idonee all'interno della stessa zona di disponibilità per raggiungere fino a 25 Gbps tra tali istanze.

> **Note**
>
> Un flusso singolo è considerato un flusso TCP o UDP unico a 5 tuple. Per altri protocolli che seguono l'intestazione IP, come `GRE` o `IPsec`, per definire un flusso vengono utilizzati il 3-tuple dell'IP di origine, l'IP di destinazione e il protocollo successivo.

Larghezza di banda disponibile per l'istanza

La larghezza di banda di rete disponibile per un'istanza dipende dal numero di vCPU di cui dispone. Ad esempio, un'istanza `m5.8xlarge` ha 32 vCPUs e una larghezza di banda di rete a 10 Gb/s e un'istanza `m5.16xlarge` ha una larghezza di banda di 64 vCPUs e larghezza di banda di rete di 20 Gb/s. Le istanze potrebbero tuttavia non raggiungere questa larghezza di banda, ad esempio se superano i limiti di rete a livello di istanza, come il numero di pacchetti al secondo o di connessioni tracciate. La quantità di larghezza di banda disponibile che il traffico può utilizzare dipende dal numero di vCPU e dalla destinazione. Ad esempio, un'`m5.16xlarge`istanza dispone di 64 vCPU, quindi il traffico verso un'altra istanza nella regione può utilizzare l'intera larghezza di banda disponibile (20 Gbps). Tuttavia, il traffico che passa attraverso un gateway Internet o un gateway locale può utilizzare solo il 50% della larghezza di banda disponibile (10 Gbps).

In genere, istanze con 16 vCPUs o meno (dimensioni `4xlarge` e inferiori) sono documentate come aventi "fino a" una larghezza di banda specificata; ad esempio, "fino a 10 Gb/s". Queste istanze hanno una larghezza di banda di base. Per soddisfare una domanda aggiuntiva, possono utilizzare un meccanismo di I/O credito di rete per superare la larghezza di banda di base. Le istanze possono utilizzare la larghezza di banda burst per un periodo di tempo limitato, in genere da 5 a 60 minuti, a seconda delle dimensioni dell'istanza.

Un'istanza riceve il numero massimo di I/O crediti di rete al momento del lancio. Se l'istanza esaurisce i I/O crediti di rete, torna alla larghezza di banda di base. Un'istanza in esecuzione guadagna I/O crediti di rete ogni volta che utilizza una larghezza di banda di rete inferiore rispetto alla larghezza di banda di base. Un'istanza interrotta non guadagna crediti di rete. I/O L'ottimizzazione dell'istanza è basata sul massimo sforzo, anche quando l'istanza ha crediti disponibili, poiché la larghezza di banda burst è una risorsa condivisa.

Esistono bucket I/O di credito di rete separati per il traffico in entrata e in uscita.

Prestazioni di rete di base e potenziate

La Guida ai tipi di istanza Amazon EC2 descrive le prestazioni di rete per ogni tipo di istanza, oltre alla larghezza di banda della rete di base disponibile per le istanze che possono utilizzare la larghezza di banda burst. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Specifiche di rete: uso generico
- Specifiche di rete: ottimizzate per il calcolo
- Specifiche di rete: ottimizzate per la memoria

- Specifiche di rete: ottimizzate per l'archiviazione
- Specifiche di rete: calcolo accelerato
- Specifiche di rete: elaborazione High-performance
- Specifiche di rete: generazione precedente

In alternativa, è possibile utilizzare uno strumento a riga di comando per ottenere queste informazioni. La console Amazon EC2 non visualizza la larghezza di banda della rete di base di un tipo di istanza.

AWS CLI

Puoi utilizzare il comando describe-instance-types per visualizzare informazioni su un tipo di istanza. Nell'esempio seguente vengono visualizzate le informazioni sulle prestazioni di rete per tutte le istanze C5.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c5.*" \
    --query "InstanceTypes[].[InstanceType, NetworkInfo.NetworkPerformance,
 NetworkInfo.NetworkCards[0].BaselineBandwidthInGbps] | sort_by(@,&[2])" \
    --output table
```

Di seguito è riportato un output di esempio. Se nell'output manca la lunghezza di banda di base, è necessario effettuare l'aggiornamento alla versione più recente della AWS CLI.

```
-----------------------------------------------
|           DescribeInstanceTypes             |
+--------------+--------------------+---------+
|  c5.large    |  Up to 10 Gigabit  |  0.75   |
|  c5.xlarge   |  Up to 10 Gigabit  |  1.25   |
|  c5.2xlarge  |  Up to 10 Gigabit  |  2.5    |
|  c5.4xlarge  |  Up to 10 Gigabit  |  5.0    |
|  c5.9xlarge  |  12 Gigabit        |  12.0   |
|  c5.12xlarge |  12 Gigabit        |  12.0   |
|  c5.18xlarge |  25 Gigabit        |  25.0   |
|  c5.24xlarge |  25 Gigabit        |  25.0   |
|  c5.metal    |  25 Gigabit        |  25.0   |
+--------------+--------------------+---------+
```

PowerShell

È possibile utilizzare il Get-EC2InstanceType PowerShell comando per visualizzare informazioni su un tipo di istanza. Nell'esempio seguente vengono visualizzate le informazioni sulle prestazioni di rete per tutte le istanze C5.

```
Get-EC2InstanceType -Filter @{Name = "instance-type"; Values = "c5.*" } | `
    Select-Object `
    InstanceType,
    @{Name = 'NetworkPerformance'; Expression =
 {($_.Networkinfo.NetworkCards.NetworkPerformance)}},
    @{Name = 'BaselineBandwidthInGbps'; Expression =
 {($_.Networkinfo.NetworkCards.BaselineBandwidthInGbps)}} | `
Format-Table -AutoSize
```

Di seguito è riportato un output di esempio.

```
InstanceType NetworkPerformance BaselineBandwidthInGbps
------------ ------------------ ----------------------
c5.4xlarge   Up to 10 Gigabit                     5.00
c5.xlarge    Up to 10 Gigabit                     1.25
c5.12xlarge  12 Gigabit                          12.00
c5.9xlarge   12 Gigabit                          12.00
c5.24xlarge  25 Gigabit                          25.00
c5.metal     25 Gigabit                          25.00
c5.2xlarge   Up to 10 Gigabit                     2.50
c5.large     Up to 10 Gigabit                     0.75
c5.18xlarge  25 Gigabit                          25.00
```

Configurazione della ponderazione della larghezza di banda dell'istanza EC2

Alcuni tipi di istanze supportano una ponderazione della larghezza di banda configurabile, che consente di selezionare una ponderazione della larghezza di banda di base che favorisca l'elaborazione di rete o le operazioni EBS. Le impostazioni predefinite per la larghezza di banda di base sono determinate dal tipo di istanza. Puoi configurare la ponderazione della larghezza di banda durante l'avvio o modificare le impostazioni dell'istanza con le seguenti preferenze di ponderazione:

- predefinito: questa opzione utilizza la configurazione della larghezza di banda standard per il tipo di istanza.

- vpc-1: questa opzione aumenta la larghezza di banda di base disponibile per il networking e riduce la larghezza di banda di base per le operazioni EBS.
- ebs-1: questa opzione aumenta la larghezza di banda di base disponibile per le operazioni EBS e riduce la larghezza di banda di base per il networking.

Considerazioni sulla ponderazione della larghezza di banda

Di seguito sono riportate alcune considerazioni che potrebbero influire sulla strategia di ponderazione della larghezza di banda.

- L'impostazione delle preferenze di ponderazione della larghezza di banda influisce soltanto sulle specifiche della larghezza di banda. Le specifiche dei pacchetti di rete al secondo (PPS) e input/output delle operazioni EBS al secondo (IOPS) non cambiano.
- La specifica della larghezza di banda combinata tra rete ed EBS non cambia. Quando si seleziona una configurazione di ponderazione della larghezza di banda, la larghezza di banda di base disponibile per l'opzione selezionata aumenta e la larghezza di banda di base per l'opzione rimanente è ridotta della stessa quantità assoluta. Per tutte le istanze tranne quelle Flex, la larghezza di banda burst disponibile rimane la stessa per l'opzione selezionata ed è ridotta per l'opzione rimanente. Per le istanze Flex fino a 4 volte più grandi, la larghezza di banda burst rimane invariata. Per le istanze Flex di dimensioni pari o superiori a 8 volte, la larghezza di banda burst aumenta della stessa quantità della larghezza di banda di base.
- È importante capire in che modo le modifiche nell'allocazione della larghezza di banda possono influire sulle prestazioni di EBS. I/O Per le istanze EC2 con configurazione `vpc-1` (maggiore larghezza di banda della rete), potresti riscontrare una riduzione di IOPS per i volumi EBS se raggiungi il limite di larghezza di banda EBS prima di aver raggiunto il limite di IOPS. Ciò è più evidente con dimensioni maggiori. I/O

  Ad esempio, su un tipo di istanza che normalmente supporta 240.000 IOPS con una I/O dimensione di 16 KiB, se si seleziona la `vpc-1` ponderazione, ciò potrebbe ridurre gli IOPS ottenibili a causa del limite di larghezza di banda di base di EBS modificato.

  Quando pianifichi il carico di lavoro, considera le tue dimensioni e i tuoi modelli. I/O Le I/O dimensioni più piccole hanno meno probabilità di essere influenzate dalle limitazioni della larghezza di banda, mentre le I/O dimensioni maggiori o i carichi di lavoro sequenziali potrebbero subire un impatto maggiore dalle modifiche alla larghezza di banda. Testa sempre il tuo carico di lavoro specifico per garantire prestazioni ottimali con la configurazione scelta.

- La specifica di larghezza di banda multi-flusso per il traffico che passa attraverso un gateway Internet o un gateway locale è adattata al 50% della larghezza di banda di base dell'opzione configurata o a 5 Gbps, ove applicabile. Per ulteriori informazioni, consulta Larghezza di banda di rete dell'istanza Amazon EC2.

  L'esempio seguente si basa su un tipo di istanza con una larghezza di banda di base predefinita di 40 Gbps e una larghezza di banda di confine predefinita di 20 Gbps. Se scegli la ponderazione della larghezza di banda `vpc-1` per questa istanza, la larghezza di banda di base ponderata passa a 50 Gbps e la larghezza di banda di confine diventa 25 Gbps.
- Questa funzionalità è disponibile in tutte le regioni commerciali, in linea con la disponibilità e il supporto delle istanze EC2.
- Tale funzionalità non comporta costi aggiuntivi all'istanza EC2.

Tipi di istanze supportati per la ponderazione della larghezza di banda

I tipi di istanze nelle seguenti famiglie di istanze supportano la ponderazione configurabile della larghezza di banda.

- Uso generale: M8a, M8g, M8gd, M8i, M8id, M9g, M9gd M8i-flex
- Ottimizzato per il calcolo: C8a, C8g, C8gd, C8i, C8id, C9g, C9gd C8i-flex
- Memoria ottimizzata: R8a, R8g, R8gd, R8i, R8id, R9g, R9gd, X8g, X8aedz, X8i R8i-flex

Verifica delle impostazioni correnti della larghezza di banda

Per visualizzare le impostazioni correnti della larghezza di banda per la tua istanza, seleziona una delle schede per visualizzare le istruzioni.

Console

Per ottenere l'impostazione della larghezza di banda per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza che desideri verificare dall'elenco e vai alla scheda Rete. L'impostazione corrente è mostrata nel campo Larghezza di banda configurata. Amazon EC2 utilizza le impostazioni predefinite per il tipo di istanza se la larghezza di banda non è impostata su un valore specifico.

AWS CLI

Per ottenere l'impostazione della larghezza di banda per un'istanza

Utilizza il comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].NetworkPerformanceOptions.BandwidthWeighting
 \
    --output text
```

Di seguito è riportato un output di esempio.

```
default
```

Questo esempio elenca tutte le istanze che hanno la preferenza di ponderazione della larghezza di banda impostata su `vpc-1`, per una maggiore larghezza di banda della rete.

```
aws ec2 describe-instances \
    --filters "Name=network-performance-options.bandwidth-weighting,Values=vpc-1" \
    --query Reservations[].Instances[].InstanceId \
    --output text
```

PowerShell

Per ottenere l'impostazione della larghezza di banda per un'istanza

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -
InstanceId i-1234567890abcdef0).Instances.NetworkPerformanceOptions.BandwidthWeighting.Value
```

Di seguito è riportato un output di esempio.

```
default
```

Questo esempio elenca tutte le istanze che hanno la preferenza di ponderazione della larghezza di banda impostata su `vpc-1`, per una maggiore larghezza di banda della rete.

```
(Get-EC2Instance `
    -Filter @{Name="network-performance-options.bandwidth-
weighting";Values="vpc-1"}).Instances.InstanceId
```

Configurazione della ponderazione della larghezza di banda per la tua istanza

È possibile configurare la ponderazione della larghezza di banda all'avvio o modificando le istanze esistenti dalla console API/SDKs EC2 o dalla CLI.

Configurazione della ponderazione della larghezza di banda all'avvio di un'istanza

Per configurare le impostazioni della larghezza di banda all'avvio di un'istanza, seleziona una delle schede per le istruzioni.

È inoltre possibile specificare la ponderazione della larghezza di banda in un modello di avvio. Per creare un modello di avvio, consulta Creare un modello di avvio Amazon EC2. Il parametro da impostare si trova nella stessa posizione in cui è utilizzato per l'avvio di un'istanza direttamente dalla console. Espandi la sezione Dettagli avanzati e imposta la Configurazione della larghezza di banda dell'istanza.

Per avviare un'istanza con il tuo modello di lancio, consulta Avvio di istanze EC2 usando un modello di avvio.

Console

Per avviare un'istanza con ponderazione della larghezza di banda configurabile

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Scegliere Launch Instances (Avvia istanze). Ciò apre la finestra di dialogo Avvia un'istanza. Vi sono svariati modi aggiuntivi per accedere alla finestra di dialogo di avvio, a seconda delle preferenze. Ad esempio, puoi avviare un'istanza direttamente da un'AMI o dalla dashboard Amazon EC2 stessa.
4. L'Amazon Machine Image (AMI) da cui si effettua l'avvio deve essere basata sull'architettura `Arm`. Molte immagini Quick Start supportano entrambe le architetture `x86` e `Arm`. Dopo aver scelto il sistema operativo per l'istanza, seleziona l'opzione `Arm` dall'elenco Architettura.
5. Il tipo di istanza deve essere Tipi di istanze supportati per questa funzionalità.

6. Quando espandi la sezione Dettagli avanzati, puoi scorrere verso il basso per trovare le impostazioni di configurazione della larghezza di banda dell'istanza. Seleziona l'opzione di configurazione della larghezza di banda per la tua istanza.
7. Configura tutte le altre impostazioni per l'istanza come faresti normalmente e scegli Avvia istanza.

AWS CLI

Per avviare un'istanza con ponderazione della larghezza di banda configurabile

Utilizza il comando run-instances con l'opzione seguente per avviare istanze configurate per una maggiore ponderazione della larghezza di banda della rete.

```
--network-performance-options BandwidthWeighting=vpc-1
```

Utilizza il comando run-instances con l'opzione seguente per avviare istanze configurate per una maggiore ponderazione della larghezza di banda EBS.

```
--network-performance-options BandwidthWeighting=ebs-1
```

PowerShell

Per avviare un'istanza con ponderazione della larghezza di banda configurabile

Utilizza il New-EC2Instance cmdlet con il seguente parametro per avviare istanze configurate per una maggiore ponderazione della larghezza di banda di rete.

```
-NetworkPerformanceOptions_BandwidthWeighting vpc-1
```

Utilizza il New-EC2Instance cmdlet con il seguente parametro per avviare istanze configurate per una maggiore ponderazione della larghezza di banda EBS.

```
-NetworkPerformanceOptions_BandwidthWeighting ebs-1
```

Aggiornamento della ponderazione della larghezza di banda per un'istanza esistente

Per aggiornare la ponderazione della larghezza di banda per un'istanza esistente, l'istanza deve trovarsi nello stato `Stopped`.

Console

Per aggiornare la ponderazione della larghezza di banda

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza che desideri aggiornare dall'elenco.
4. Prima di modificare la configurazione della larghezza di banda, l'istanza deve trovarsi in uno stato `Stopped`. Se l'istanza è in esecuzione, seleziona Arresta istanza dal menu Stato dell'istanza.
5. Scegli Gestisci la larghezza di banda dal menu Azioni > Rete. Si apre la finestra di dialogo Gestisci larghezza di banda.

> **Note**
>
> Se il tipo di istanza non supporta la configurazione per la ponderazione della larghezza di banda, tale voce di menu è disabilitata.

6. Seleziona l'opzione per aggiornare l'istanza e scegli Cambia per salvare le impostazioni.

AWS CLI

Per aggiornare la ponderazione della larghezza di banda

Utilizza il comando modify-instance-network-performance-options per configurare una ponderazione più elevata della larghezza di banda della rete per l'istanza specificata.

```
aws ec2 modify-instance-network-performance-options \
    --instance-id i-1234567890abcdef0 \
    --bandwidth-weighting=vpc-1
```

L'esempio seguente configura una ponderazione più elevata della larghezza di banda EBS per l'istanza specificata.

```
aws ec2 modify-instance-network-performance-options \
    --instance-id i-1234567890abcdef0 \
    --bandwidth-weighting=ebs-1
```

PowerShell

Per aggiornare la ponderazione della larghezza di banda

Utilizza il Edit-EC2InstanceNetworkPerformanceOption cmdlet per configurare una maggiore ponderazione della larghezza di banda di rete per l'istanza specificata.

```
Edit-EC2InstanceNetworkPerformanceOption `
    -InstanceId i-1234567890abcdef0 `
    -BandwidthWeighting vpc-1
```

L'esempio seguente configura una ponderazione più elevata della larghezza di banda EBS per l'istanza specificata.

```
Edit-EC2InstanceNetworkPerformanceOption `
    -InstanceId i-1234567890abcdef0 `
    -BandwidthWeighting ebs-1
```

Prestazioni di rete

La tabella seguente mostra le prestazioni di rete, in Gbps, che possono essere ottenute con le configurazioni `default`, `vpc-1` e `ebs-1`.

Tipo di istanza	**`default`** (Base/burst)	**`vpc-1`** (Base/burst)	**`ebs-1`** (Base/burst)
c8a.medium	0,52/12,5	0,65/12,5	0,438/10,0
c8a. grande	0,937/12,5	1,172/12,5	0,774/10,0
c8a.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
c8a.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
c8a.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
c8a.8xlarge	15.0	18,75	12,5

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
c8a.12x grande	22,5	28,125	18,75
c8a.16x grande	30,0	37,5	25.0
c8a.24xlarge	40,0	50.0	32,5
c8a.48x grande	75.0	93,75	60,0
c8a.metallo-24xl	40,0	50.0	32,5
c8a.metallo-48xl	75.0	93,75	60,0
c8g.medium	0,52/12,5	0,65/12,5	0,441/10,0
c8g.large	0,937/12,5	1,171/12,5	0,779/10,0
c8g.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
c8g.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
c8g.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
c8g.8xlarge	15,0	18,75	12,5
c8g.12xlarge	22,5	28,125	18,75
c8g.16xlarge	30,0	37,5	25.0
c8g.24xlarge	40,0	50.0	32,5
c8g.48xlarge	50.0	62,5	40,0
c8g.metal-24xl	40,0	50.0	32,5
c8g.metal-48xl	50.0	62,5	40,0
c8gd.medium	0,52/12,5	0,65/12,5	0,441/10,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
c8gd.large	0,937/12,5	1,171/12,5	0,779/10,0
c8gd.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
c8gd.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
c8gd.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
c8gd.8xlarge	15,0	18,75	12,5
c8gd.12xlarge	22,5	28,125	18,75
c8gd.16xlarge	30,0	37,5	25.0
c8gd.24xlarge	40,0	50.0	32,5
c8gd.48xlarge	50.0	62,5	40,0
c8gd.metal-24xl	40,0	50.0	32,5
c8gd.metal-48xl	50.0	62,5	40,0
c8i.large	0,937/12,5	1,172/12,5	0,774/10,0
c8i.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
c8i.2x grande	3,75/15,0	4,688/15,0	3,125/12,5
c8i.4xgrande	7,5/15,0	9,375/15,0	6,25/12,5
c8i.8xgrande	15.0	18,75	12,5
c8i.12x grande	22,5	28,125	18,75
c8i.16x grande	30,0	37,5	25.0
c8i.24x grande	40,0	50.0	32,5

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
c8i.32x grande	50.0	62,5	40,0
c8i.48x grande	75.0	93,75	60,0
c8i.96xlarge	100.0	125,0	80,0
c8i.metallo-48xl	75.0	93,75	60,0
c8i.metal-96xl	100.0	125,0	80,0
c8id. grande	0,937/12,5	1,172/12,5	0,774/10,0
c8id.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
c8id.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
c8id.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
c8id.8xlarge	15.0	18,75	12,5
c8 id.12x grande	22,5	28,125	18,75
c8 id.16x grande	30,0	37,5	25.0
c8id.24x grande	40,0	50.0	32,5
c8id.32x grande	50.0	62,5	40,0
c8id.48x grande	75.0	93,75	60,0
c8id.96x grande	100.0	125.0	80,0
c8id.metallo-48xl	75.0	93,75	60,0
c8id.metallo-96xl	100.0	125,0	80,0
c8i-flex.large	0,468/12,5	0,585/12,5	0,389/10,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
c8i-flex.xlarge	0,937/12,5	1,172/12,5	0,779/10,0
c8i-flex.2xlarge	1,875/15,0	2,344/15,0	1,562/12,5
c8i-flex.4xlarge	3,75/15,0	4,688/15,0	3,125/12,5
c8i-flex.8xlarge	7,5/15,0	9,375/18,75	6,25/12,5
c8i-flex.12xlarge	11,25/22,5	14,063/28,125	9,375/18,75
c8i-flex.16xlarge	15,0/30,0	18,75/37,5	12,5/25,0
c9g. medio	0,55/15,0	0,688/15,0	0,455/12,0
cm 9 g. Grande	1,0/15,0	1,25/15,0	0,81/12,0
c9g.x grande	2,1/15,0	2.625/15.0	1,725/12,0
c 9g. 2x grande	4,25/17,0	5.313/17.0	3,5/14,0
cm 9g. 4x grande	8,5/17,0	10.625/17.0	7,0/14,0
cm 9 g. 8 x grande	17,0	21,25	14,0
cm 9g. 12x grande	25.0	31,25	20,5
cm 9 g. 16 x grande	34,0	42,5	28,0
cm 9 g. 24 x grande	50.0	62,5	41,0
cm 9g. 48x grande	100.0	125.0	82,0
c9g. Metallo-48xl	100.0	125,0	82,0
c9gd. medio	0,55/15,0	0,688/15,0	0,455/12,0
c9gd. grande	1,0/15,0	1,25/15,0	0,81/12,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
c9gd.xlarge	2,1/15,0	2.625/15.0	1,725/12,0
c9g. 2x grande	4,25/17,0	5.313/17.0	3,5/14,0
c9g. 4x grande	8,5/17,0	10.625/17.0	7,0/14,0
c9g. 8x grande	17.0	21,25	14,0
cm 9 g. 12 x grande	25.0	31,25	20,5
cm 9 g. 16 x grande	34,0	42,5	28,0
cm 9 g. 24 x grande	50.0	62,5	41,0
cm 9 g. 48 x grande	100.0	125.0	82,0
c9gd.metallo-48xl	100.0	125,0	82,0
m8a.medium	0,52/12,5	0,65/12,5	0,438/10,0
m8a.large	0,937/12,5	1,172/12,5	0,774/10,0
m8a.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
m8a.2x grande	3,75/15,0	4,688/15,0	3,125/12,5
m8a.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
m8a.8xlarge	15,0	18,75	12,5
m8a.12x grande	22,5	28,125	18,75
m8a.16x grande	30,0	37,5	25.0
m8a.24x grande	40,0	50.0	32,5
m8a.48x grande	75.0	93,75	60,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
m8a.metal-24xl	40,0	50.0	32,5
m8a.metallo-48xl	75.0	93,75	60,0
m8g.medium	0,52/12,5	0,65/12,5	0,441/10,0
m8g.large	0,937/12,5	1,171/12,5	0,779/10,0
m8g.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
m8g.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
m8g.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
m8g.8xlarge	15,0	18,75	12,5
m8g.12xlarge	22,5	28,125	18,75
m8g.16xlarge	30,0	37,5	25.0
m8g.24xlarge	40,0	50.0	32,5
m8g.48xlarge	50.0	62,5	40,0
m8g.metal-24xl	40,0	50.0	32,5
m8g.metal-48xl	50.0	62,5	40,0
m8gd.medium	0,52/12,5	0,65/12,5	0,441/10,0
m8gd.large	0,937/12,5	1,171/12,5	0,779/10,0
m8gd.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
m8gd.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
m8gd.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
m8gd.8xlarge	15,0	18,75	12,5
m8gd.12xlarge	22,5	28,125	18,75
m8gd.16xlarge	30,0	37,5	25.0
m8gd.24xlarge	40,0	50.0	32,5
m8gd.48xlarge	50.0	62,5	40,0
m8gd.metal-24xl	40,0	50.0	32,5
m8gd.metal-48xl	50.0	62,5	40,0
m8i.large	0,937/12,5	1,172/12,5	0,774/10,0
m8i.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
m8i.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
m8i.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
m8i.8xlarge	15,0	18,75	12,5
m8i.12xlarge	22,5	28,125	18,75
m8i.16xlarge	30,0	37,5	25.0
m8i.24xlarge	40,0	50.0	32,5
m8i.32xlarge	50.0	62,5	40,0
m8i.48xlarge	75.0	93,75	60,0
m8i.96xlarge	100.0	125,0	80,0
m8i.metal-48xl	75.0	93,75	60,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
m8i.metal-96xl	100.0	125,0	80,0
m8id. grande	0,937/12,5	1,172/12,5	0,774/10,0
m8id.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
m8id.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
m8id.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
m8id.8xlarge	15.0	18,75	12,5
m8 id.12x grande	22,5	28,125	18,75
m8 id.16x grande	30,0	37,5	25.0
m8id.24x grande	40,0	50.0	32,5
m8 id.32x grande	50.0	62,5	40,0
m8 id.48x grande	75.0	93,75	60,0
m8 id.96x grande	100.0	125.0	80,0
m8id.metallo-48xl	75.0	93,75	60,0
m8id.metallo-96xl	100.0	125,0	80,0
m8i-flex.large	0,468/12,5	0,585/12,5	0,389/10,0
m8i-flex.xlarge	0,937/12,5	1,172/12,5	0,779/10,0
m8i-flex.2xlarge	1,875/15,0	2,344/15,0	1,562/12,5
m8i-flex.4xlarge	3,75/15,0	4,688/15,0	3,125/12,5
m8i-flex.8xlarge	7,5/15,0	9,375/18,75	6,25/12,5

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
m8i-flex.12xlarge	11,25/22,5	14,063/28,125	9,375/18,75
m8i-flex.16xlarge	15,0/30,0	18,75/37,5	12,5/25,0
9 g. Medio	0,55/15,0	0,688/15,0	0,455/12,0
9 mg di grandi dimensioni	1,0/15,0	1,25/15,0	0,81/12,0
m 9 g.x grande	2,1/15,0	2.625/15.0	1,725/12,0
9g. 2x grande	4,25/17,0	5.313/17.0	3,5/14,0
9g. 4x grande	8,5/17,0	10.625/17.0	7,0/14,0
9g. 8x grande	17,0	21,25	14,0
9g. 12x grande	25.0	31,25	20,5
m 9 g. 16 x grande	34,0	42,5	28,0
9g. 24x grande	50.0	62,5	41,0
9g. 48x grande	100.0	125,0	82,0
9g. Metallo-48xl	100.0	125,0	82,0
9 mg. Medio	0,55/15,0	0,688/15,0	0,455/12,0
9 mg. grande	1,0/15,0	1,25/15,0	0,81/12,0
m9gd.xlarge	2,1/15,0	2.625/15.0	1,725/12,0
m 9 g. 2 x grandi	4,25/17,0	5.313/17.0	3,5/14,0
m 9 g. 4x grande	8,5/17,0	10.625/17.0	7,0/14,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
m 9g. 8x grande	17.0	21,25	14,0
m 9 g. 12 x grande	25.0	31,25	20,5
m 9 g. 16 x grande	34,0	42,5	28,0
m 9 g. 24 x grande	50.0	62,5	41,0
m 9 g. 48 x grande	100.0	125.0	82,0
m9gd.metallo-48xl	100.0	125,0	82,0
r8a.medium	0,52/12,5	0,65/12,5	0,438/10,0
r8a.large	0,937/12,5	1,172/12,5	0,774/10,0
r8a.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
r8a.2x grande	3,75/15,0	4,688/15,0	3,125/12,5
r8a.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
r8a.8xlarge	15.0	18,75	12,5
r8a.12x grande	22,5	28,125	18,75
r8a.16x grande	30,0	37,5	25.0
r8a.24xlarge	40,0	50.0	32,5
r8a.48x grande	75.0	93,75	60,0
r8a.metal-24xl	40,0	50.0	32,5
r8a.metallo-48xl	75.0	93,75	60,0
r8g.medium	0,52/12,5	0,65/12,5	0,441/10,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
r8g.large	0,937/12,5	1,171/12,5	0,779/10,0
r8g.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
r8g.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
r8g.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
r8g.8xlarge	15,0	18,75	12,5
r8g.12xlarge	22,5	28,125	18,75
r8g.16xlarge	30,0	37,5	25.0
r8g.24xlarge	40,0	50.0	32,5
r8g.48xlarge	50.0	62,5	40,0
r8g.metal-24xl	40,0	50.0	32,5
r8g.metal-48xl	50.0	62,5	40,0
r8gd.medium	0,52/12,5	0,65/12,5	0,441/10,0
r8gd.large	0,937/12,5	1,171/12,5	0,779/10,0
r8gd.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
r8gd.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
r8gd.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
r8gd.8xlarge	15,0	18,75	12,5
r8gd.12xlarge	22,5	28,125	18,75
r8gd.16xlarge	30,0	37,5	25.0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
r8gd.24xlarge	40,0	50.0	32,5
r8gd.48xlarge	50.0	62,5	40,0
r8gd.metal-24xl	40,0	50.0	32,5
r8gd.metal-48xl	50.0	62,5	40,0
r8i.large	0,937/12,5	1,172/12,5	0,774/10,0
r8i.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
r8i.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
r8i.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
r8i.8xlarge	15,0	18,75	12,5
r8i.12xlarge	22,5	28,125	18,75
r8i.16xlarge	30,0	37,5	25.0
r8i.24xlarge	40,0	50.0	32,5
r8i.32xlarge	50.0	62,5	40,0
r8i.48xlarge	75.0	93,75	60,0
r8i.96xlarge	100.0	125,0	80,0
r8i.metal-48xl	75.0	93,75	60,0
r8i.metal-96xl	100.0	125,0	80,0
r8id. grande	0,937/12,5	1,172/12,5	0,774/10,0
r8id.xlarge	1,875/12,5	2,344/12,5	1,562/10,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
r8id.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
r8id.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
r8id.8xlarge	15.0	18,75	12,5
r8id.12x grande	22,5	28,125	18,75
r8id.16x grande	30,0	37,5	25.0
r8id.24xlarge	40,0	50.0	32,5
r8id.32x grande	50.0	62,5	40,0
r8id.48x grande	75.0	93,75	60,0
r8id.96xlarge	100.0	125.0	80,0
r8id.metallo-48xl	75.0	93,75	60,0
r8id.metallo-96xl	100.0	125,0	80,0
r8i-flex.large	0,468/12,5	0,585/12,5	0,389/10,0
r8i-flex.xlarge	0,937/12,5	1,172/12,5	0,779/10,0
r8i-flex.2xlarge	1,875/15,0	2,344/15,0	1,562/12,5
r8i-flex.4xlarge	3,75/15,0	4,688/15,0	3,125/12,5
r8i-flex.8xlarge	7,5/15,0	9,375/18,75	6,25/12,5
r8i-flex.12xlarge	11,25/22,5	14,063/28,125	9,375/18,75
r8i-flex.16xlarge	15,0/30,0	18,75/37,5	12,5/25,0
r9g. Medio	0,55/15,0	0,688/15,0	0,455/12,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
r9 g. Grande	1,0/15,0	1,25/15,0	0,81/12,0
r9g.x grande	2,1/15,0	2.625/15.0	1,725/12,0
r 9 g. 2 x grande	4,25/17,0	5.313/17.0	3,5/14,0
r 9 g. 4 x grande	8,5/17,0	10.625/17.0	7,0/14,0
r 9 g. 8 x grande	17,0	21,25	14,0
r 9 g. 12 x grande	25.0	31,25	20,5
r 9 g. 16 x grande	34,0	42,5	28,0
r 9 g. 24 x grande	50.0	62,5	41,0
r 9g. 48x grande	100.0	125.0	82,0
r9g. metallo-48xl	100.0	125,0	82,0
r9gd. medio	0,55/15,0	0,688/15,0	0,455/12,0
r9gd. grande	1,0/15,0	1,25/15,0	0,81/12,0
r9gd.xlarge	2,1/15,0	2.625/15.0	1,725/12,0
r9gd.2x grande	4,25/17,0	5.313/17.0	3,5/14,0
r9g. 4x grande	8,5/17,0	10.625/17.0	7,0/14,0
r9gd.8x grande	17,0	21,25	14,0
r9gd.12x grande	25.0	31,25	20,5
r9gd.16x grande	34,0	42,5	28,0
r9gd.24x grande	50.0	62,5	41,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
r9gd.48x grande	100.0	125.0	82,0
r9gd.metallo-48xl	100.0	125,0	82,0
x8g.medium	0,52/12,5	0,65/12,5	0,441/10,0
x8g.large	0,937/12,5	1,171/12,5	0,779/10,0
x8g.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
x8g.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
x8g.4xlarge	7,5/15,0	9,375/15,0	6,25/12,5
x8g.8xlarge	15,0	18,75	12,5
x8g.12xlarge	22,5	28,125	18,75
x8g.16xlarge	30,0	37,5	25.0
x8g.24xlarge	40,0	50.0	32,5
x8g.48xlarge	50.0	62,5	40,0
x8g.metal-24xl	40,0	50.0	32,5
x8g.metal-48xl	50.0	62,5	40,0
x8aedz. grande	1.562/18,75	1.953/18,75	1,249/15,0
x8aedz.xlarge	3,125/18,75	3.907/18,75	2,5/15,0
x8aedz.3x grande	9,375/18,75	11.719/18.75	7,5/15,0
x8aedz.6x grande	18,75	23,438	15,0
x8aedz.12x grande	37,5	46,875	30,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
x8aedz.24x grande	75.0	93,75	60,0
x8aedz.metallo-12xl	37,5	46,875	30,0
x8aedz.metallo-24xl	75.0	93,75	60,0
x8i. Grande	0,937/12,5	1,172/12,5	0,774/10,0
x8i.xlarge	1,875/12,5	2,344/12,5	1,562/10,0
x8i.2xlarge	3,75/15,0	4,688/15,0	3,125/12,5
x8i.4x grande	7,5/15,0	9,375/15,0	6,25/12,5
x8i.8x grande	15.0	18,75	12,5
x8i.12x grande	22,5	28,125	18,75
x8i.16x grande	30,0	37,5	25.0
x8i.24x grande	40,0	50.0	32,5
x8i.32x grande	50.0	62,5	40,0
x8i.48x grande	75.0	93,75	60,0
x8i.64x grande	80,0	100.0	62,5
x8i.96x grande	100.0	125.0	80,0
x8i.metallo-48xl	75.0	93,75	60,0
x8i.metallo-96xl	100.0	125,0	80,0

Prestazioni Amazon EBS

La tabella seguente mostra le prestazioni di Amazon EBS, in Gbps, che possono essere ottenute con le configurazioni `default`, `vpc-1` `eebs-1`.

Tipo di istanza	**`default`** (Base/burst)	**`vpc-1`** (Base/burst)	**`ebs-1`** (Base/burst)
c8a. medio	0,325/10,0	0,195/6,25	0,407/10,0
c8a. grande	0,65/10,0	0,415/6,25	0,813/10,0
c8a.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
c8a.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0
c8a.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
c8a.8xlarge	10.0	6,25	12,5
c8a.12x grande	15.0	9,375	18,75
c8a.16x grande	20.0	12,5	25.0
c8a.24xlarge	30,0	20.0	37,5
c8a.48x grande	60,0	41,25	75.0
c8a.metallo-24xl	30,0	20.0	37,5
c8a.metallo-48xl	60,0	41,25	75.0
c8g.medium	0,315/10,0	0,185/6,25	0,394/10,0
c8g.large	0,63/10,0	0,396/6,25	0,788/10,0
c8g.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
c8g.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
c8g.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
c8g.8xlarge	10.0	6,25	12,5
c8g.12xlarge	15,0	9,375	18,75
c8g.16xlarge	20.0	12,5	25.0
c8g.24xlarge	30,0	20.0	37,5
c8g.48xlarge	40,0	27,5	50.0
c8g.metal-24xl	30,0	20.0	37,5
c8g.metal-48xl	40,0	27,5	50.0
c8gd.medium	0,315/10,0	0,185/6,25	0,394/10,0
c8gd.large	0,63/10,0	0,396/6,25	0,788/10,0
c8gd.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
c8gd.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0
c8gd.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
c8gd.8xlarge	10.0	6,25	12,5
c8gd.12xlarge	15,0	9,375	18,75
c8gd.16xlarge	20.0	12,5	25.0
c8gd.24xlarge	30,0	20.0	37,5
c8gd.48xlarge	40,0	27,5	50.0
c8gd.metal-24xl	30,0	20.0	37,5

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
c8gd.metal-48xl	40,0	27,5	50.0
c8i.large	0,65/10,0	0,415/6,25	0,813/10,0
c8i.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
c8i.2x grande	2,5/10,0	1,562/6,25	3,125/10,0
c8i.4xgrande	5,0/10,0	3,125/6,25	6,25/10,0
c8i.8xgrande	10.0	6,25	12,5
c8i.12x grande	15.0	9,375	18,75
c8i.16x grande	20.0	12,5	25.0
c8i.24x grande	30,0	20.0	37,5
c8i.32x grande	40,0	27,5	50.0
c8i.48x grande	60,0	41,25	75.0
c8i.96xlarge	80,0	55,0	100.0
c8i.metallo-48xl	60,0	41,25	75.0
c8i.metal-96xl	80,0	55,0	100.0
c8id. grande	0,65/10,0	0,415/6,25	0,813/10,0
c8id.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
c8id.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0
c8id.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
c8id.8xlarge	10.0	6,25	12,5

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
c8id.12x grande	15.0	9,375	18,75
c8 id.16x grande	20.0	12,5	25.0
c8id.24x grande	30,0	20.0	37,5
c8id.32x grande	40,0	27,5	50.0
c8 id.48x grande	60,0	41,25	75.0
c8id.96x grande	80,0	55,0	100.0
c8id.metallo-48xl	60,0	41,25	75.0
c8id.metallo-96xl	80,0	55,0	100.0
c8i-flex.large	0,315/10,0	0,198/6,25	0,394/10,0
c8i-flex.xlarge	0,63/10,0	0,395/6,25	0,788/10,0
c8i-flex.2xlarge	1,25/10,0	0,781/6,25	1,563/10,0
c8i-flex.4xlarge	2,5/10,0	1,562/6,25	3,125/10,0
c8i-flex.8xlarge	5,0/10,0	3,125/6,25	6,25/12,5
c8i-flex.12xlarge	7,5/15,0	4,687/9,375	9,375/18,75
c8i-flex.16xlarge	10,0/20,0	6,25/12,5	12,5/25,0
c9g. medio	0,38/12,0	0,242/7,75	0,475/12,0
cm 9 g. Grande	0,76/12,0	0,51/7,75	0,95/12,0
c9g.x grande	1,5/12,0	0,975/7,75	1,875/12,0
c 9g. 2x grande	3,0/12,0	1,937/7,75	3,75/12,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
cm 9 g. 4 x grande	6,0/12,0	3,875/7,75	7,5/12,0
cm 9g. 8x grande	12.0	7.75	15.0
cm 9 g. 12 x grande	18,0	11.75	22,5
cm 9 g. 16 x grande	24,0	15,5	30,0
cm 9 g. 24 x grande	36,0	23,5	45.0
cm 9g. 48x grande	72,0	47,0	90,0
c9g. Metallo-48xl	72,0	47,0	90,0
9gd. medio	0,38/12,0	0,242/7,75	0,475/12,0
c9gd. grande	0,76/12,0	0,51/7,75	0,95/12,0
c9gd.xlarge	1,5/12,0	0,975/7,75	1,875/12,0
c9g. 2x grande	3,0/12,0	1,937/7,75	3,75/12,0
c9g. 4x grande	6,0/12,0	3,875/7,75	7,5/12,0
c9g. 8x grande	12.0	7.75	15.0
cm 9 g. 12 x grande	18.0	11.75	22,5
cm 9 g. 16 x grande	24,0	15,5	30,0
cm 9 g. 24 x grande	36,0	23,5	45.0
cm 9 g. 48 x grande	72,0	47,0	90,0
c9gd.metallo-48xl	72,0	47,0	90,0
m8a.medium	0,325/10,0	0,195/6,25	0,407/10,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
m8a.large	0,65/10,0	0,415/6,25	0,813/10,0
m8a.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
m8a.2x grande	2,5/10,0	1,562/6,25	3,125/10,0
m8a.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
m8a.8xlarge	10.0	6,25	12,5
m8a.12x grande	15,0	9,375	18,75
m8a.16x grande	20.0	12,5	25.0
m8a.24x grande	30,0	20.0	37,5
m8a.48x grande	60,0	41,25	75.0
m8a.metal-24xl	30,0	20.0	37,5
m8a.metallo-48xl	60,0	41,25	75.0
m8g.medium	0,315/10,0	0,185/6,25	0,394/10,0
m8g.large	0,63/10,0	0,396/6,25	0,788/10,0
m8g.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
m8g.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0
m8g.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
m8g.8xlarge	10.0	6,25	12,5
m8g.12xlarge	15,0	9,375	18,75
m8g.16xlarge	20.0	12,5	25.0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
m8g.24xlarge	30,0	20.0	37,5
m8g.48xlarge	40,0	27,5	50.0
m8g.metal-24xl	30,0	20.0	37,5
m8g.metal-48xl	40,0	27,5	50.0
m8gd.medium	0,315/10,0	0,185/6,25	0,394/10,0
m8gd.large	0,63/10,0	0,396/6,25	0,788/10,0
m8gd.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
m8gd.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0
m8gd.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
m8gd.8xlarge	10.0	6,25	12,5
m8gd.12xlarge	15,0	9,375	18,75
m8gd.16xlarge	20.0	12,5	25.0
m8gd.24xlarge	30,0	20.0	37,5
m8gd.48xlarge	40,0	27,5	50.0
m8gd.metal-24xl	30,0	20.0	37,5
m8gd.metal-48xl	40,0	27,5	50.0
m8i.large	0,65/10,0	0,415/6,25	0,813/10,0
m8i.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
m8i.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
m8i.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
m8i.8xlarge	10.0	6,25	12,5
m8i.12xlarge	15,0	9,375	18,75
m8i.16xlarge	20.0	12,5	25.0
m8i.24xlarge	30,0	20.0	37,5
m8i.32xlarge	40,0	27,5	50.0
m8i.48xlarge	60,0	41,25	75.0
m8i.96xlarge	80,0	55,0	100.0
m8i.metal-48xl	60,0	41,25	75.0
m8i.metal-96xl	80,0	55,0	100.0
m8id. grande	0,65/10,0	0,415/6,25	0,813/10,0
m8id.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
m8id.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0
m8id.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
m8id.8xlarge	10.0	6,25	12,5
m8 id.12x grande	15.0	9,375	18,75
m8 id.16x grande	20.0	12,5	25.0
m8id.24x grande	30,0	20.0	37,5
m8id.32x grande	40,0	27,5	50.0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
m8 id.48x grande	60,0	41,25	75.0
m8 id.96x grande	80,0	55,0	100.0
m8id.metallo-48xl	60,0	41,25	75.0
m8id.metallo-96xl	80,0	55,0	100.0
m8i-flex.large	0,315/10,0	0,198/6,25	0,394/10,0
m8i-flex.xlarge	0,63/10,0	0,395/6,25	0,788/10,0
m8i-flex.2xlarge	1,25/10,0	0,781/6,25	1,563/10,0
m8i-flex.4xlarge	2,5/10,0	1,562/6,25	3,125/10,0
m8i-flex.8xlarge	5,0/10,0	3,125/6,25	6,25/12,5
m8i-flex.12xlarge	7,5/15,0	4,687/9,375	9,375/18,75
m8i-flex.16xlarge	10,0/20,0	6,25/12,5	12,5/25,0
9 g. Medio	0,38/12,0	0,242/7,75	0,475/12,0
9 g. Grande	0,76/12,0	0,51/7,75	0,95/12,0
9g. x grande	1,5/12,0	0,975/7,75	1,875/12,0
9g. 2x grande	3,0/12,0	1,937/7,75	3,75/12,0
9g. 4x grande	6,0/12,0	3,875/7,75	7,5/12,0
9g. 8x grande	12,0	7.75	15.0
9g. 12x grande	18,0	11.75	22,5
9 m. 16 x grande	24,0	15,5	30,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
9 g. 24 x grande	36,0	23,5	45.0
9g. 48x grande	72,0	47,0	90,0
9g. Metallo-48xl	72,0	47,0	90,0
9 mg. Medio	0,38/12,0	0,242/7,75	0,475/12,0
9 mg. grande	0,76/12,0	0,51/7,75	0,95/12,0
m9gd.xlarge	1,5/12,0	0,975/7,75	1,875/12,0
9 m g. 2 x grande	3,0/12,0	1,937/7,75	3,75/12,0
m 9 g. 4x grande	6,0/12,0	3,875/7,75	7,5/12,0
m 9 g. 8 x grande	12.0	7.75	15.0
m 9 g. 12 x grande	18.0	11.75	22,5
m 9 g. 16 x grande	24,0	15,5	30,0
m 9 g. 24 x grande	36,0	23,5	45.0
m 9 g. 48 x grande	72,0	47,0	90,0
m9gd.metallo-48xl	72,0	47,0	90,0
r8a.medium	0,325/10,0	0,195/6,25	0,407/10,0
r8a.large	0,65/10,0	0,415/6,25	0,813/10,0
r8a.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
r8a.2x grande	2,5/10,0	1,562/6,25	3,125/10,0
r8a.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
r8a.8xlarge	10.0	6,25	12,5
r8a.12x grande	15,0	9,375	18,75
r8a.16x grande	20.0	12,5	25.0
r8a.24xlarge	30,0	20.0	37,5
r8a.48x grande	60,0	41,25	75.0
r8a.metal-24xl	30,0	20.0	37,5
r8a.metallo-48xl	60,0	41,25	75.0
r8g.medium	0,315/10,0	0,185/6,25	0,394/10,0
r8g.large	0,63/10,0	0,396/6,25	0,788/10,0
r8g.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
r8g.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0
r8g.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
r8g.8xlarge	10.0	6,25	12,5
r8g.12xlarge	15,0	9,375	18,75
r8g.16xlarge	20.0	12,5	25.0
r8g.24xlarge	30,0	20.0	37,5
r8g.48xlarge	40,0	27,5	50.0
r8g.metal-24xl	30,0	20.0	37,5
r8g.metal-48xl	40,0	27,5	50.0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
r8gd.medium	0,315/10,0	0,185/6,25	0,394/10,0
r8gd.large	0,63/10,0	0,396/6,25	0,788/10,0
r8gd.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
r8gd.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0
r8gd.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
r8gd.8xlarge	10.0	6,25	12,5
r8gd.12xlarge	15,0	9,375	18,75
r8gd.16xlarge	20.0	12,5	25.0
r8gd.24xlarge	30,0	20.0	37,5
r8gd.48xlarge	40,0	27,5	50.0
r8gd.metal-24xl	30,0	20.0	37,5
r8gd.metal-48xl	40,0	27,5	50.0
r8i.large	0,65/10,0	0,415/6,25	0,813/10,0
r8i.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
r8i.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0
r8i.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
r8i.8xlarge	10.0	6,25	12,5
r8i.12xlarge	15,0	9,375	18,75
r8i.16xlarge	20.0	12,5	25.0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
r8i.24xlarge	30,0	20.0	37,5
r8i.32xlarge	40,0	27,5	50.0
r8i.48xlarge	60,0	41,25	75.0
r8i.96xlarge	80,0	55,0	100.0
r8i.metal-48xl	60,0	41,25	75.0
r8i.metal-96xl	80,0	55,0	100.0
r8id.grande	0,65/10,0	0,415/6,25	0,813/10,0
r8id.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
r8id.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0
r8id.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
r8id.8xlarge	10.0	6,25	12,5
r8id.12x grande	15.0	9,375	18,75
r8id.16x grande	20.0	12,5	25.0
r8id.24xlarge	30,0	20.0	37,5
r8id.32xlarge	40,0	27,5	50.0
r8id.48x grande	60,0	41,25	75.0
r8id.96x grande	80,0	55,0	100.0
r8id.metallo-48xl	60,0	41,25	75.0
r8id.metallo-96xl	80,0	55,0	100.0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
r8i-flex.large	0,315/10,0	0,198/6,25	0,394/10,0
r8i-flex.xlarge	0,63/10,0	0,395/6,25	0,788/10,0
r8i-flex.2xlarge	1,25/10,0	0,781/6,25	1,563/10,0
r8i-flex.4xlarge	2,5/10,0	1,562/6,25	3,125/10,0
r8i-flex.8xlarge	5,0/10,0	3,125/6,25	6,25/12,5
r8i-flex.12xlarge	7,5/15,0	4,687/9,375	9,375/18,75
r8i-flex.16xlarge	10,0/20,0	6,25/12,5	12,5/25,0
r9g. Medio	0,38/12,0	0,242/7,75	0,475/12,0
r9 g. Grande	0,76/12,0	0,51/7,75	0,95/12,0
r9g.x grande	1,5/12,0	0,975/7,75	1,875/12,0
r 9 g. 2 x grande	3,0/12,0	1,937/7,75	3,75/12,0
r 9 g. 4 x grande	6,0/12,0	3,875/7,75	7,5/12,0
r 9 g. 8 x grande	12,0	7.75	15.0
r 9 g. 12 x grande	18,0	11.75	22,5
r 9 g. 16 x grande	24,0	15,5	30,0
r 9 g. 24 x grande	36,0	23,5	45.0
r 9g. 48x grande	72,0	47,0	90,0
R9g. Metallo-48xl	72,0	47,0	90,0
r9gd. medio	0,38/12,0	0,242/7,75	0,475/12,0

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
r9gd. grande	0,76/12,0	0,51/7,75	0,95/12,0
r9gd.xlarge	1,5/12,0	0,975/7,75	1,875/12,0
r9gd.2x grande	3,0/12,0	1,937/7,75	3,75/12,0
r9g. 4x grande	6,0/12,0	3,875/7,75	7,5/12,0
r9g. 8x grande	12.0	7.75	15.0
r9gd.12x grande	18.0	11.75	22,5
r9g. 16x grande	24,0	15,5	30,0
r9gd.24x grande	36,0	23,5	45.0
r9gd.48x grande	72,0	47,0	90,0
r9gd.metallo-48xl	72,0	47,0	90,0
x8g.medium	0,315/10,0	0,185/6,25	0,394/10,0
x8g.large	0,63/10,0	0,396/6,25	0,788/10,0
x8g.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
x8g.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0
x8g.4xlarge	5,0/10,0	3,125/6,25	6,25/10,0
x8g.8xlarge	10.0	6,25	12,5
x8g.12xlarge	15,0	9,375	18,75
x8g.16xlarge	20.0	12,5	25.0
x8g.24xlarge	30,0	20.0	37,5

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
x8g.48xlarge	40,0	27,5	50.0
x8g.metal-24xl	30,0	20.0	37,5
x8g.metal-48xl	40,0	27,5	50.0
x8aedz. grande	1,25/15,0	0,859/10,312	1,563/15,0
x8aedz.xlarge	2,5/15,0	1.718/10.312	3,125/15,0
x8aedz.3x grande	7,5/15,0	5.156/10.312	9,375/15,0
x8aedz.6x grande	15,0	10,312	18,75
x8aedz.12x grande	30,0	20,625	37,5
x8aedz.24x grande	60,0	41,25	75.0
x8aedz.metallo-12xl	30,0	20,625	37,5
x8aedz.metallo-24xl	60,0	41,25	75.0
x8i. Grande	0,65/10,0	0,415/6,25	0,813/10,0
x8i.xlarge	1,25/10,0	0,781/6,25	1,563/10,0
x8i.2xlarge	2,5/10,0	1,562/6,25	3,125/10,0
x8i.4x grande	5,0/10,0	3,125/6,25	6,25/10,0
x8i.8x grande	10.0	6,25	12,5
x8i.12x grande	15.0	9,375	18,75
x8i.16x grande	20.0	12,5	25.0
x8i.24x grande	30,0	20.0	37,5

Tipo di istanza	**default** (Base/burst)	**vpc-1** (Base/burst)	**ebs-1** (Base/burst)
x8i.32x grande	40,0	27,5	50.0
x8i.48x grande	60,0	41,25	75.0
x8i.64x grande	70,0	50.0	87,5
x8i.96x grande	80,0	55,0	100.0
x8i.metallo-48xl	60,0	41,25	75.0
x8i.metallo-96xl	80,0	55,0	100.0

Monitorare la larghezza di banda delle istanze

È possibile utilizzare CloudWatch le metriche per monitorare la larghezza di banda della rete dell'istanza e i pacchetti inviati e ricevuti. Puoi utilizzare i parametri delle prestazioni di rete fornite dal driver ENA (Elastic Network Adapter) per monitorare quando il traffico supera le quote di rete definite da Amazon EC2 a livello di istanza.

Puoi configurare se Amazon EC2 invia i dati metrici per l'istanza CloudWatch utilizzando periodi di un minuto o periodi di cinque minuti. È possibile che le metriche delle prestazioni di rete mostrino che è stata superata una soglia e che i pacchetti sono stati eliminati, mentre le metriche dell'istanza no. CloudWatch Ciò può verificarsi quando l'istanza ha un breve picco nella domanda di risorse di rete (noto come microburst), ma le CloudWatch metriche non sono sufficientemente granulari da riflettere questi picchi di microsecondi.

Ulteriori informazioni

- Parametri dell'istanza
- Monitoraggio delle prestazioni di rete

Rete migliorata per le istanze Amazon EC2

La rete avanzata utilizza la I/O virtualizzazione a root singolo (SR-IOV) per fornire funzionalità di rete ad alte prestazioni sui tipi di istanze supportati. SR-IOV è un metodo di virtualizzazione dei dispositivi che offre I/O prestazioni più elevate e un minore utilizzo della CPU rispetto alle tradizionali interfacce di rete virtualizzate. Le reti avanzate forniscono infatti una larghezza di banda più alta, prestazioni PPS (pacchetti al secondo) superiori e latenze tra istanze significativamente più basse. L'utilizzo di questo servizio avanzato non comporta costi supplementari.

Per ulteriori informazioni sulla velocità di rete supportata per ogni tipo di istanza, consulta Tipi di istanze Amazon EC2.

È possibile abilitare la rete avanzata utilizzando uno dei seguenti meccanismi:

Elastic Network Adapter (ENA)

Elastic Network Adapter (ENA) supporta velocità di rete fino a 100 Gbps per i tipi di istanza supportati.

Tutte le Nitro-based istanze utilizzano ENA per una rete avanzata. Inoltre, le seguenti Xen-based istanze utilizzano ENA: H1, I3, G3, P3`m4.16xlarge`, P3dn e R4.

Per ulteriori informazioni, consulta Abilitazione delle reti avanzate con ENA su istanze EC2.

Interfaccia VF (Virtual Function) Intel 82599

L'interfaccia VF (Virtual Function) Intel 82599 supporta velocità di rete fino a 10 Gbps per i tipi di istanza supportati.

I seguenti tipi di istanza utilizzano l'interfaccia Intel 82599 VF per una rete avanzata: C3, C4, D2, I2, M4 (tranne m4.16xlarge) e R3.

Per ulteriori informazioni, consulta Reti avanzate con l'interfaccia VF Intel 82599 sulle istanze.

Indice

- Abilitazione delle reti avanzate con ENA su istanze EC2
- Migliora le prestazioni di rete tra le istanze EC2 con ENA Express
- Reti avanzate con l'interfaccia VF Intel 82599 sulle istanze
- Monitoraggio delle prestazioni di rete per le impostazioni ENA dell'istanza EC2

- Miglioramento della latenza di rete per le istanze EC2 basate su Linux
- Considerazioni sul sistema Nitro per l'ottimizzazione delle prestazioni
- Ottimizza le prestazioni di rete sulle istanze Windows EC2

Abilitazione delle reti avanzate con ENA su istanze EC2

Amazon EC2 fornisce funzionalità di rete avanzate tramite Elastic Network Adapter (ENA). Per utilizzare la rete avanzata, devi utilizzare un'AMI che includa il driver ENA richiesto o installarlo manualmente. Quindi puoi abilitare il supporto ENA sull'istanza.

Per rivedere le note di rilascio o le istruzioni di installazione di un driver ENA, consulta la scheda corrispondente alla piattaforma del sistema operativo dell'istanza.

Linux

È possibile consultare la seguente documentazione su GitHub:

- Consulta le note sulla versione del driver del kernel ENA Linux su GitHub.
- Per una panoramica del driver del kernel Linux ENA che include le istruzioni di installazione, consulta il driver del kernel Linux per la famiglia Elastic Network Adapter (ENA) su. GitHub

Windows

Puoi consultare la seguente documentazione nella sezione Gestisci driver dei dispositivi di questa guida:

- Traccia rilasci della versione del driver ENA Windows.
- Installa il driver ENA su istanze EC2 Windows.

Ad Nitro-based esempio, le funzionalità di rete avanzate variano in base alla versione di Nitro implementata dal tipo di istanza.

Per esaminare le specifiche di rete per la tua istanza, scegli il link della famiglia di istanze per il tipo di istanza. Se non sei sicuro della famiglia di istanze applicabile, consulta Convenzioni di denominazione nella guida ai Tipi di istanza di Amazon EC2.

- Specifiche di rete per istanze a calcolo accelerato
- Specifiche di rete per istanze ottimizzate per il calcolo

- Specifiche di rete per istanze per uso generico
- Specifiche di rete per istanze di calcolo ad alte prestazioni
- Specifiche di rete per istanze ottimizzate per la memoria
- Specifiche di rete per istanze ottimizzate per l'archiviazione

Indice

- Prerequisiti per reti avanzate con ENA
- Verifica dell'abilitazione delle reti avanzate
- Abilitazione delle reti avanzate su un'istanza
- Code ENA
- Risolvere i problemi relativi al driver ENA kernel su Linux
- Risoluzione dei problemi del driver dell'Adattatore elastico di rete per Windows

Prerequisiti per reti avanzate con ENA

Per preparare la configurazione delle funzionalità delle reti avanzate tramite ENA, configura l'istanza nel seguente modo:

- Avvia un'istanza. Nitro-based
- Verificare che l'istanza disponga di connettività Internet.
- Se sull'istanza sono presenti dati importanti che devono essere conservati, è consigliabile eseguire una copia di backup di tali dati ora mediante la creazione di un'AMI dall'istanza. L'aggiornamento dei kernel ENA e l'abilitazione dell'attributo `enaSupport` potrebbero rendere non compatibili le istanze o irraggiungibili i sistemi operativi. Se disponi di un backup recente, i tuoi dati saranno mantenuti.
- Istanze Linux – Avvia l'istanza utilizzando una versione supportata del kernel Linux e una distribuzione supportata, in modo che la rete avanzata ENA sia abilitata automaticamente per la tua istanza. Per ulteriori informazioni, consulta le note di rilascio del driver ENA Linux Kernel.
- Istanze Windows: se l'istanza esegue Windows Server 2008 R2 SP1, assicurati che disponga dell'aggiornamento del supporto per la firma del SHA-2 codice.
- Utilizzalo AWS CloudShell da Console di gestione AWS, oppure installa e configura il AWS CLI o il AWS Tools for Windows PowerShell su qualsiasi computer tu scelga, preferibilmente sul desktop o sul laptop locale. Per ulteriori informazioni, consulta Accesso a Amazon EC2 o la Guida per l'utente di AWS CloudShell. Le reti avanzate non possono essere gestite dalla console Amazon EC2.

Verifica dell'abilitazione delle reti avanzate

Puoi verificare se la rete avanzata è abilitata nelle tue istanze o nelle tue AMI.

Attributo dell'istanza

Controlla il valore dell'attributo dell'istanza `enaSupport`.

AWS CLI

Utilizza il comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[].Instances[].EnaSupport"
```

Se le reti avanzate sono abilitate, viene visualizzato il seguente output.

```
[
    true
]
```

PowerShell

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.EnaSupport
```

Se le reti avanzate sono abilitate, viene visualizzato il seguente output.

```
True
```

Attributo dell'immagine

Controlla il valore dell'attributo dell'immagine `enaSupport`.

AWS CLI

Utilizza il comando describe-images.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query "Images[].EnaSupport"
```

Se le reti avanzate sono abilitate, viene visualizzato il seguente output.

```
[
    true
]
```

PowerShell

Utilizza il cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).EnaSupport
```

Se le reti avanzate sono abilitate, viene visualizzato il seguente output.

```
True
```

Driver dell'interfaccia di rete Linux

Utilizza il comando seguente per verificare se il driver del kernel `ena` viene utilizzato su un'interfaccia specifica, sostituendo il nome dell'interfaccia che desideri controllare. Se usi una singola interfaccia (impostazione predefinita), essa sarà `eth0`. Se la tua distribuzione Linux supporta nomi di rete prevedibili, questo potrebbe essere un nome simile a `ens5`. Per ulteriori informazioni, espandi la sezione relativa a RHEL, SUSE e CentOS in Abilitazione delle reti avanzate su un'istanza.

Nell'esempio seguente, il driver del kernel `ena` non viene caricato, perché il driver nell'elenco è `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
```

```
supports-priv-flags: no
```

In questo caso, il driver del kernel `ena` è caricato con la versione minima consigliata. Questa istanza dispone della funzionalità per reti avanzate adeguatamente configurata.

```
[ec2-user ~]$ ethtool -i eth0
driver: ena
version: 1.5.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Abilitazione delle reti avanzate su un'istanza

La procedura utilizzata dipende dal sistema operativo dell'istanza.

Amazon Linux

Le AMI per Amazon Linux includono il driver del kernel necessario per migliorare il networking con ENA installato e hanno il supporto ENA abilitato. Pertanto, se si avvia un'istanza con una versione HVM di Amazon Linux su un tipo di istanza supportato, l'istanza dispone già dell'abilitazione delle reti avanzate. Per ulteriori informazioni, consulta Verifica dell'abilitazione delle reti avanzate.

Ubuntu

Le più recenti AMI HVM di Ubuntu includono il driver del kernel necessario per migliorare il networking con ENA installato e hanno il supporto ENA abilitato. Pertanto, se si avvia un'istanza con la più recente versione Ubuntu HVM AMI; su un tipo di istanza supportato, l'istanza dispone già dell'abilitazione delle reti avanzate. Per ulteriori informazioni, consulta Verifica dell'abilitazione delle reti avanzate.

Se l'istanza è stata avviata utilizzando un'AMI di una versione precedente per la quale la funzionalità di reti avanzate non è abilitata, puoi installare il pacchetto kernel `linux-aws` per avere i driver di rete ottimizzati più recenti e aggiornare l'attributo richiesto.

Per installare il pacchetto del **`kernel`** linux-aws (Ubuntu 16.04 o successivo)

Ubuntu 16.04 e 18.04 vengono forniti con il kernel personalizzato Ubuntu (pacchetto kernel `linux-aws`). Per usare un kernel diverso, contatta Supporto.

Per installare il pacchetto kernel linux-aws (Ubuntu Trusty 14.04)

1. Connettiti alla tua istanza.
2. Aggiorna la cache dei pacchetti e i pacchetti.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Se durante il processo di aggiornamento viene richiesto di installare `grub`, utilizza `/dev/xvda` per installare `grub`, quindi scegli di conservare la versione corrente di `/boot/grub/menu.lst`.

3. [EBS-backed istanza] Dal tuo computer locale, interrompi l'istanza utilizzando la console Amazon EC2 o uno dei seguenti comandi: () o (). stop-instancesAWS CLIStop-EC2InstanceAWS Tools for Windows PowerShell

   [Istanza supportata da instance store] Non è possibile arrestare l'istanza per modificare l'attributo. Segui invece questa procedura: Per abilitare le reti avanzate su Ubuntu (istanze supportate da instance store).
4. Dal computer locale, abilita l'attributo relativo alle reti avanzate utilizzando uno dei seguenti comandi:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --ena-support
     ```

   - Edit-EC2InstanceAttribute(Strumenti per Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $true
     ```
5. (Facoltativo) Crea un'AMI dall'istanza, come descritto in Crea un' EBS-backed AMI Amazon. L'AMI eredita l'attributo `enaSupport` relativo alle reti avanzate dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con le reti avanzate abilitate per impostazione di default.

6. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI) o Start-EC2Instance (AWS Tools for Windows PowerShell).

Per abilitare le reti avanzate su Ubuntu (istanze supportate da instance store)

Segui la procedura precedente fino al punto in cui si arresta l'istanza. Crea una nuova AMI come descritto in Crea un' S3-backed AMI Amazon, assicurandoti di abilitare l'attributo relativo alle reti avanzate durante la registrazione dell'AMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

RHEL, SUSE, CentOS

Le più recenti AMI per Red Hat Enterprise Linux, SUSE Linux Enterprise Server e CentOS includono il driver del kernel necessario per migliorare la rete con ENA e hanno il supporto ENA abilitato. Pertanto, se si lancia un'istanza con la più recente versione di AMI su un tipo di istanza supportato, l'istanza dispone già dell'abilitazione delle reti avanzate. Per ulteriori informazioni, consulta Verifica dell'abilitazione delle reti avanzate.

La procedura seguente descrive le fasi generali per abilitare le reti avanzate ENA su una distribuzione Linux diversa da AMI Amazon Linux o Ubuntu. Per ulteriori informazioni, ad esempio sintassi dettagliata dei comandi, posizione dei file o supporto di pacchetti e strumenti, consulta la documentazione per la distribuzione Linux in uso.

Per abilitare le reti avanzate su Linux

1. Connettiti alla tua istanza.
2. Clona il codice sorgente per il driver del `ena` kernel sulla tua istanza da GitHub at. https://github.com/amzn/amzn-drivers (SUSE Linux Enterprise Server 12 SP2 e versioni successive includono ENA 2.02 per impostazione predefinita, pertanto non è necessario scaricare e compilare il driver ENA. Per SUSE Linux Enterprise Server 12 SP2 e versioni successive, è

necessario presentare una richiesta per aggiungere la versione del driver che si desidera al kernel di serie).

```
git clone https://github.com/amzn/amzn-drivers
```

3. Compila e installa il driver del kernel `ena` sull'istanza. Questi passaggi dipendono dalla distribuzione Linux. Per ulteriori informazioni sulla compilazione del driver del kernel su Red Hat Enterprise Linux, consulta Come installare il driver ENS più recente per un supporto di rete avanzato su un'istanza Amazon EC2 che esegue RHEL?
4. Esegui il comando sudo depmod per aggiornare le dipendenze del driver del kernel.
5. Aggiorna `initramfs` sull'istanza in modo che il nuovo driver del kernel venga caricato in fase di avvio. Ad esempio, se la distribuzione supporta dracut, è possibile utilizzare il seguente comando:

```
dracut -f -v
```

6. Determina se il sistema utilizza nomi di interfaccia di rete prevedibili per impostazione di default. I sistemi che utilizzano systemd o udev versione 197 o successive possono rinominare i dispositivi Ethernet e pertanto non garantiscono che la singola interfaccia di rete venga rinominata in `eth0`. Questo comportamento potrebbe causare problemi durante la connessione all'istanza. Per ulteriori informazioni e per informazioni sulle altre opzioni di configurazione disponibili, consulta l'argomento relativo ai nomi di interfaccia di rete prevedibili sul sito Web freedesktop.org.

   a. Puoi controllare le udev versioni di systemd or sui RPM-based sistemi con il seguente comando.

   ```
   rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
   systemd-208-11.el7_0.2.x86_64
   ```

   In questo esempio di Red Hat Enterprise Linux 7, la systemd versione è 208, quindi i nomi prevedibili delle interfacce di rete devono essere disabilitati.

   b. Disabilitare i nomi di interfaccia di rete prevedibili aggiungendo l'opzione `net.ifnames=0` alla riga `GRUB_CMDLINE_LINUX` in `/etc/default/grub`.

   ```
   sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /etc/default/
   grub
   ```

   c. Ricompila il file di configurazione di grub.

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [EBS-backed istanza] Dal computer locale, interrompi l'istanza utilizzando la console Amazon EC2 o uno dei seguenti comandi: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell).

   [Istanza supportata da instance store] Non è possibile arrestare l'istanza per modificare l'attributo. Segui invece questa procedura: Per abilitare le reti avanzate su Linux (istanze supportate da archivio istanze).

8. Dal computer locale, abilita l'attributo `enaSupport` relativo alle reti avanzate utilizzando uno dei seguenti comandi:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --ena-support
     ```

   - Edit-EC2InstanceAttribute(Strumenti per Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $true
     ```

9. (Facoltativo) Crea un'AMI dall'istanza, come descritto in Crea un' EBS-backed AMI Amazon. L'AMI eredita l'attributo `enaSupport` relativo alle reti avanzate dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con le reti avanzate abilitate per impostazione di default.

   Se il sistema operativo dell'istanza contiene un file `/etc/udev/rules.d/70-persistent-net.rules`, è necessario eliminarlo prima di creare l'AMI. Questo file contiene l'indirizzo MAC per la scheda Ethernet dell'istanza originale. Se un'altra istanza viene avviata con questo file, il sistema operativo non sarà in grado di trovare il dispositivo ed `eth0` potrebbe non funzionare causando problemi di avvio. Questo file viene rigenerato al successivo ciclo di avvio e qualsiasi istanza avviata dall'AMI crea la propria versione del file.

10. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI) o Start-EC2Instance (AWS Tools for Windows PowerShell).

11. (Facoltativo) Connettiti all'istanza e verifica che il driver del kernel sia installato.

    Se è impossibile connettersi all'istanza dopo aver abilitato le reti avanzate, consulta Risolvere i problemi relativi al driver ENA kernel su Linux.

Per abilitare le reti avanzate su Linux (istanze supportate da archivio istanze)

Segui la procedura precedente fino al punto in cui si arresta l'istanza. Crea una nuova AMI come descritto in Crea un' S3-backed AMI Amazon, assicurandoti di abilitare l'attributo relativo alle reti avanzate durante la registrazione dell'AMI.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport ...
```

Ubuntu con DKMS

Questo metodo è solo per scopi di test e feedback. Non è pensato per l'utilizzo con distribuzioni di produzione. Per distribuzioni di produzione, consulta Ubuntu.

> **Important**
>
> L'uso di DKMS annulla il contratto di assistenza per l'abbonamento. Non deve essere utilizzato per le distribuzioni di produzione.

Per abilitare una rete avanzata con ENA su Ubuntu (EBS-backed istanze)

1. Seguire le fasi 1 e 2 in Ubuntu.
2. Installare i pacchetti `build-essential` per compilare il driver del kernel e il pacchetto `dkms` in modo che il driver del kernel `ena` venga ricompilato a ogni aggiornamento del kernel.

   ```
   ubuntu:~$ sudo apt-get install -y build-essential dkms
   ```

3. Clona il codice sorgente del driver del `ena` kernel sulla tua istanza da at. GitHub https://github.com/amzn/amzn-drivers

   ```
   ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
   ```

4. Spostare il pacchetto `amzn-drivers` nella directory `/usr/src/` in modo che DKMS riesca a individuarlo e compilarlo per ogni aggiornamento del kernel. Aggiungere il numero di versione (il numero di versione corrente è disponibile nelle note di rilascio) del codice sorgente al nome della directory. Nell'esempio seguente viene visualizzata la seguente versione `1.0.0`.

```
ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
```

5. Creare il file di configurazione DKMS con i seguenti valori, sostituendo la versione in uso di `ena`.

   Creare il file.

```
ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
```

   Modificare il file e aggiungere i valori seguenti.

```
ubuntu:~$ sudo vim /usr/src/amzn-drivers-1.0.0/dkms.conf
PACKAGE_NAME="ena"
PACKAGE_VERSION="1.0.0"
CLEAN="make -C kernel/linux/ena clean"
MAKE="make -C kernel/linux/ena/ BUILD_KERNEL=${kernelver}"
BUILT_MODULE_NAME[0]="ena"
BUILT_MODULE_LOCATION="kernel/linux/ena"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ena"
AUTOINSTALL="yes"
```

6. Aggiungere, compilare e installare il driver del kernel `ena` sull'istanza utilizzando DKMS.

   Aggiungere il driver del kernel a DKMS.

```
ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
```

   Compilare il driver del kernel usando il comando dkms.

```
ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
```

   Installare il driver del kernel usando dkms.

```
ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
```

7. Ricompilare `initramfs` in modo che il driver del kernel corretto venga caricato in fase di avvio.

```
ubuntu:~$ sudo update-initramfs -u -k all
```

8. Verificare che il driver del kernel `ena` sia installato utilizzando il comando modinfo ena disponibile in Verifica dell'abilitazione delle reti avanzate.

```
ubuntu:~$ modinfo ena
filename:    /lib/modules/3.13.0-74-generic/updates/dkms/ena.ko
version:  1.0.0
license:  GPL
description: Elastic Network Adapter (ENA)
author:   Amazon.com, Inc. or its affiliates
srcversion:  9693C876C54CA64AE48F0CA
alias:    pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
vermagic:    3.13.0-74-generic SMP mod_unload modversions
parm:     debug:Debug level (0=none,...,16=all) (int)
parm:     push_mode:Descriptor / header push mode (0=automatic,1=disable,3=enable)
    0 - Automatically choose according to device capability (default)
    1 - Don't push anything to device memory
    3 - Push descriptors and header buffer to device memory (int)
parm:     enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1) (int)
parm:     enable_missing_tx_detection:Enable missing Tx completions. (default=1)
 (int)
parm:     numa_node_override_array:Numa node override map
(array of int)
parm:     numa_node_override:Enable/Disable numa node override (0=disable)
(int)
```

9. Continuare con la fase 3 in Ubuntu.

Abilitazione delle reti avanzate su Windows

Se hai avviato l'istanza per la quale la funzionalità di reti avanzate non è già abilitata, devi scaricare e installare il driver per la scheda di rete richiesto sull'istanza e quindi impostare l'attributo `enaSupport` dell'istanza in modo da attivare le reti avanzate.

Per abilitare le reti avanzate

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. [Solo Windows Server 2016 e 2019] Esegui il seguente PowerShell script EC2Launch per configurare l'istanza dopo l'installazione del driver.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

3. Dall'istanza, installare il driver nel seguente modo:

   a. Scarica il driver più recente per l'istanza.

   b. Estrai l'archivio .zip.

   c. Installa il driver eseguendo lo script. `install.ps1` PowerShell

   > **Note**
   >
   > Se si verifica un errore della policy di esecuzione, impostare la policy su `Unrestricted` (per impostazione predefinita è impostata su `Restricted` o `RemoteSigned`). In una riga di comando`Set-ExecutionPolicy -ExecutionPolicy Unrestricted`, esegui e quindi esegui nuovamente `install.ps1` PowerShell lo script.

4. Dal computer locale, arresta l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: stop-instances (AWS CLI) oppure Stop-EC2Instance (AWS Tools for Windows PowerShell).
5. Abilita il supporto ENA sull'istanza nel seguente modo:

   a. Dal computer locale, controlla l'attributo relativo al supporto ENA per l'istanza EC2 sull'istanza eseguendo uno dei seguenti comandi. Se l'attributo non è abilitato, l'output riporterà "[]" o sarà vuoto. `EnaSupport` è configurato su `false` per impostazione predefinita.

   - describe-instances (AWS CLI)

     ```
     aws ec2 describe-instances --instance-ids i-1234567890abcdef0 --query
      "Reservations[].Instances[].EnaSupport"
     ```

   - Get-EC2Instance(Strumenti per Windows PowerShell)

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.EnaSupport
```

b. Per abilitare il supporto ENA, esegui uno dei comandi riportati di seguito:

- modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --ena-support
```

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $true
```

Se si verificano problemi durante il riavvio dell'istanza, è possibile disabilitare il supporto ENA utilizzando uno dei seguenti comandi:

- modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --no-ena-support
```

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $false
```

c. Verifica che l'attributo sia stato impostato su `true` utilizzando describe-instances o Get-EC2Instance come descritto in precedenza. Ora l'output restituito sarà simile al seguente:

```
[
 true
]
```

6. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI) o Start-EC2Instance (AWS Tools for Windows PowerShell).
7. Nell'istanza, verifica che il driver ENA sia installato e abilitato nel seguente modo:

a. Apri il menu contestuale (clic con il pulsante destro del mouse) per l'icona di rete e scegli Apri Centro connessioni di rete e condivisione.

b. Seleziona la scheda Ethernet (ad esempio, Ethernet 2).

c. Seleziona Details (Dettagli). In Network Connection Details (Dettagli connessione di rete), verifica che nel campo Description (Descrizione) sia visualizzato Amazon Elastic Network Adapter.

8. (Facoltativo) Crea un'AMI dall'istanza. L'AMI eredita l'attributo `enaSupport` dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con ENA abilitato per impostazione di default.

Code ENA

Le code Elastic Network Adapter (ENA) gestiscono l'elaborazione dei pacchetti per le interfacce di rete Amazon EC2. Ogni tipo di istanza ha un determinato numero di code ENA condivise tra le sue Elastic Network Interfaces (ENI). Per impostazione predefinita, ogni ENI riceve un numero fisso di code in base al tipo e alla dimensione dell'istanza.

Con l'allocazione delle code ENA configurabile, puoi scegliere quante code riceve ogni ENI. Il totale per ENI e per istanza è ancora limitato. Questo ti aiuta ad abbinare l'elaborazione dei pacchetti al tuo carico di lavoro. Ad esempio, puoi assegnare più code a un ENI con traffico intenso e meno a uno con traffico leggero.

Argomenti

- Specifiche della coda ENA per i tipi di istanze EC2
- Configura l'allocazione delle code ENA

Specifiche della coda ENA per i tipi di istanze EC2

Le tabelle seguenti elencano i tipi di istanza che supportano l'allocazione configurabile delle code ENA, insieme ai relativi valori di coda predefiniti e massimi.

> **Note**
>
> Per i valori delle code ENA per tutti i tipi di istanze, inclusi i tipi che non supportano l'allocazione di code ENA configurabile, consulta le tabelle delle specifiche di rete nella guida ai tipi di istanze di Amazon EC2. https://docs.aws.amazon.com/ec2/latest/instancetypes/ec2-instance-type-specifications.html

General purpose

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
m6i.large	2	2	6
m6i.xlarge	4	4	16
m6i.2xlarge	8	8	32
m6i.4xlarge	8	16	64
m6i.8xlarge	8	32	64
m6i.12xlarge	8	32	64
m6i.16xlarge	8	32	120
m6i.24xlarge	8	32	120
m6i.32xlarge	8	32	120
m6id.large	2	2	6
m6id.xlarge	4	4	16
m6id.2xlarge	8	8	32
m6id.4xlarge	8	16	64
m6id.8xlarge	8	32	64
m6id.12xlarge	8	32	64
m6id.16xlarge	8	32	120
m6id.24xlarge	8	32	120

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
m6id.32xlarge	8	32	120
m6idn.large	2	2	6
m6idn.xlarge	4	4	16
m6idn.2xlarge	8	8	32
m6idn.4xlarge	8	16	64
m6idn.8xlarge	16	32	128
m6idn.12xlarge	16	32	128
m6idn.16xlarge	16	32	240
m6idn.24xlarge	32	32	480
m6idn.32xlarge	32	32	512 *
m6in.large	2	2	6
m6in.xlarge	4	4	16
m6in.2xlarge	8	8	32
m6in.4xlarge	8	16	64
m6in.8xlarge	16	32	128
m6in.12xlarge	16	32	128
m6in.16xlarge	16	32	240
m6in.24xlarge	32	32	480

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
m6in.32xlarge	32	32	512 *
m8a.medium	1	1	3
m8a.large	2	2	6
m8a.xlarge	4	4	16
m8a.2xlarge	8	8	32
m8a.4xlarge	8	16	64
m8a.8xlarge	8	32	128
m8a.12xlarge	16	64	192
m8a.16xlarge	16	64	256
m8a.24xlarge	16	128	384
m8a.48xlarge	32	128	768
m8a.metal-24xl	16	128	384
m8a.metal-48xl	32	128	768
m8azn.medium	1	1	3
m8azn.large	2	2	8
m8azn.xlarge	4	4	16
m8azn.3xlarge	4	16	48
m8azn.6xlarge	8	32	96

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
m8azn.12xlarge	8	64	192
m8azn.24xlarge	16	128	384
m8azn.metal-12xl	8	64	192
m8azn.metal-24xl	16	128	384
m8gb.medium	1	1	2
m8gb.large	2	2	6
m8gb.xlarge	4	4	16
m8gb.2xlarge	8	8	32
m8gb.4xlarge	8	16	64
m8gb.8xlarge	8	32	128
m8gb.12xlarge	16	64	192
m8gb.16xlarge	16	64	256
m8gb.24xlarge	16	128	384
m8gb.48xlarge	32	128	768 *
m8gb.metal-24xl	32	128	768
m8gb.metal-48xl	32	128	768 *
m8gn.medium	1	1	2
m8gn.large	2	2	6

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
m8gn.xlarge	4	4	16
m8gn.2xlarge	8	8	32
m8gn.4xlarge	8	16	64
m8gn.8xlarge	8	32	128
m8gn.12xlarge	16	64	192
m8gn.16xlarge	16	64	256
m8gn.24xlarge	16	128	384
m8gn.48xlarge	32	128	768 *
m8gn.metal-24xl	32	128	768
m8gn.metal-48xl	32	128	768 *
m8i.large	2	2	6
m8i.xlarge	4	4	16
m8i.2xlarge	8	8	32
m8i.4xlarge	8	16	64
m8i.8xlarge	8	32	128
m8i.12xlarge	16	64	192
m8i.16xlarge	16	64	256
m8i.24xlarge	16	128	384

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
m8i.32xlarge	16	128	512
m8i.48xlarge	32	128	768
m8i.96xlarge	32	128	1536
m8i.metal-48xl	32	128	768
m8i.metal-96xl	32	128	1536
m8id.large	2	2	6
m8id.xlarge	4	4	16
m8id.2xlarge	8	8	32
m8id.4xlarge	8	16	64
m8id.8xlarge	8	32	128
m8id.12xlarge	16	64	192
m8id.16xlarge	16	64	256
m8id.24xlarge	16	128	384
m8id.32xlarge	16	128	512
m8id.48xlarge	32	128	768
m8id.96xlarge	32	128	1536
m8id.metal-48xl	32	128	768
m8id.metal-96xl	32	128	1536

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
m8i-flex.large	1	1	3
m8i-flex.xlarge	2	2	8
m8i-flex.2xlarge	4	4	16
m8i-flex.4xlarge	4	8	32
m8i-flex.8xlarge	4	16	64
m8i-flex.12xlarge	8	32	96
m8i-flex.16xlarge	8	32	128
m8in.large	2	2	8
m8in.xlarge	4	4	16
m8in.2xlarge	8	8	32
m8in.4xlarge	8	16	64
m8in.8xlarge	16	32	128
m8in.12xlarge	16	64	192
m8in.16xlarge	16	64	256
m8in.24xlarge	16	128	256
m8in.32xlarge	32	128	512
m8in.48xlarge	32	128	768
m8in.96xlarge	32	128	1536 *

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
m8in.metal-48xl	32	128	768
m8in.metal-96xl	32	128	1536 *
m8idn.large	2	2	8
m8idn.xlarge	4	4	16
m8idn.2xlarge	8	8	32
m8idn.4xlarge	8	16	64
m8idn.8xlarge	16	32	128
m8idn.12xlarge	16	64	192
m8idn.16xlarge	16	64	256
m8idn.24xlarge	16	128	256
m8idn.32xlarge	32	128	512
m8idn.48xlarge	32	128	768
m8idn.96xlarge	32	128	1536 *
m8idn.metal-48xl	32	128	768
m8idn.metal-96xl	32	128	1536 *
m8ine.large	2	2	8
m8ine.xlarge	4	4	16
m8ine.2xlarge	8	8	32

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
m8ine.4xlarge	16	16	128
m8ine.8xlarge	32	32	256
m8ine.12xlarge	32	64	384
m8ib.large	2	2	8
m8ib.xlarge	4	4	16
m8ib.2xlarge	8	8	32
m8ib.4xlarge	8	16	64
m8ib.8xlarge	16	32	128
m8ib.12xlarge	16	64	192
m8ib.16xlarge	16	64	256
m8ib.24xlarge	16	128	256
m8ib.32xlarge	32	128	512
m8ib.48xlarge	32	128	768
m8ib.96xlarge	32	128	1536 *
m8ib.metal-48xl	32	128	768
m8ib.metal-96xl	32	128	1536 *
m8idb.large	2	2	8
m8idb.xlarge	4	4	16

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
m8idb.2xlarge	8	8	32
m8idb.4xlarge	8	16	64
m8idb.8xlarge	16	32	128
m8idb.12xlarge	16	64	192
m8idb.16xlarge	16	64	256
m8idb.24xlarge	16	128	256
m8idb.32xlarge	32	128	512
m8idb.48xlarge	32	128	768
m8idb.96xlarge	32	128	1536 *
m8idb.metal-48xl	32	128	768
m8idb.metal-96xl	32	128	1536 *
m9g.medium	1	1	2
m9g.large	2	2	6
m9g.xlarge	4	4	16
m9g.2xlarge	8	8	32
m9g.4xlarge	8	16	64
m9g.8xlarge	8	32	128
m9g.12xlarge	16	64	192

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
m9g.16xlarge	16	64	256
m9g.24xlarge	16	128	384
m9g.48xlarge	32	128	768
m9g.metal-48xl	32	128	768
m9gd.medium	1	1	2
m9gd.large	2	2	6
m9gd.xlarge	4	4	16
m9gd.2xlarge	8	8	32
m9gd.4xlarge	8	16	64
m9gd.8xlarge	8	32	128
m9gd.12xlarge	16	64	192
m9gd.16xlarge	16	64	256
m9gd.24xlarge	16	128	384
m9gd.48xlarge	32	128	768
m9gd.metal-48xl	32	128	768

Compute optimized

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
c6i.large	2	2	6
c6i.xlarge	4	4	16
c6i.2xlarge	8	8	32
c6i.4xlarge	8	16	64
c6i.8xlarge	8	32	64
c6i.12xlarge	8	32	64
c6i.16xlarge	8	32	120
c6i.24xlarge	8	32	120
c6i.32xlarge	8	32	120
c6id.large	2	2	6
c6id.xlarge	4	4	16
c6id.2xlarge	8	8	32
c6id.4xlarge	8	16	64
c6id.8xlarge	8	32	64
c6id.12xlarge	8	32	64
c6id.16xlarge	8	32	120
c6id.24xlarge	8	32	120

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
c6id.32xlarge	8	32	120
c6in.large	2	2	6
c6in.xlarge	4	4	16
c6in.2xlarge	8	8	32
c6in.4xlarge	8	16	64
c6in.8xlarge	16	32	128
c6in.12xlarge	16	32	128
c6in.16xlarge	16	32	240
c6in.24xlarge	32	32	480
c6in.32xlarge	32	32	512 *
c8a.medium	1	1	3
c8a.large	2	2	6
c8a.xlarge	4	4	16
c8a.2xlarge	8	8	32
c8a.4xlarge	8	16	64
c8a.8xlarge	8	32	128
c8a.12xlarge	16	64	192
c8a.16xlarge	16	64	256

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
c8a.24xlarge	16	128	384
c8a.48xlarge	32	128	768
c8a.metal-24xl	16	128	384
c8a.metal-48xl	32	128	768
c8gb.medium	1	1	2
c8gb.large	2	2	6
c8gb.xlarge	4	4	16
c8gb.2xlarge	8	8	32
c8gb.4xlarge	8	16	64
c8gb.8xlarge	8	32	128
c8gb.12xlarge	16	64	192
c8gb.16xlarge	16	64	256
c8gb.24xlarge	16	128	384
c8gb.48xlarge	32	128	768 *
c8gb.metal-24xl	32	128	768
c8gb.metal-48xl	32	128	768 *
c8gn.medium	1	1	2
c8gn.large	2	2	6

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
c8gn.xlarge	4	4	16
c8gn.2xlarge	8	8	32
c8gn.4xlarge	8	16	64
c8gn.8xlarge	8	32	128
c8gn.12xlarge	16	64	192
c8gn.16xlarge	16	64	256
c8gn.24xlarge	16	128	384
c8gn.48xlarge	32	128	768 *
c8gn.metal-24xl	32	128	768
c8gn.metal-48xl	32	128	768 *
c8i.large	2	2	6
c8i.xlarge	4	4	16
c8i.2xlarge	8	8	32
c8i.4xlarge	8	16	64
c8i.8xlarge	8	32	128
c8i.12xlarge	16	64	192
c8i.16xlarge	16	64	256
c8i.24xlarge	16	128	384

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
c8i.32xlarge	16	128	512
c8i.48xlarge	32	128	768
c8i.96xlarge	32	128	1536
c8i.metal-48xl	32	128	768
c8i.metal-96xl	32	128	1536
c8id.large	2	2	6
c8id.xlarge	4	4	16
c8id.2xlarge	8	8	32
c8id.4xlarge	8	16	64
c8id.8xlarge	8	32	128
c8id.12xlarge	16	64	192
c8id.16xlarge	16	64	256
c8id.24xlarge	16	128	384
c8id.32xlarge	16	128	512
c8id.48xlarge	32	128	768
c8id.96xlarge	32	128	1536
c8id.metal-48xl	32	128	768
c8id.metal-96xl	32	128	1536

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
c8i-flex.large	1	1	3
c8i-flex.xlarge	2	2	8
c8i-flex.2xlarge	4	4	16
c8i-flex.4xlarge	4	8	32
c8i-flex.8xlarge	4	16	64
c8i-flex.12xlarge	8	32	96
c8i-flex.16xlarge	8	32	128
c8in.large	2	2	8
c8in.xlarge	4	4	16
c8in.2xlarge	8	8	32
c8in.4xlarge	8	16	64
c8in.8xlarge	16	32	128
c8in.12xlarge	16	64	192
c8in.16xlarge	16	64	256
c8in.24xlarge	16	128	256
c8in.32xlarge	32	128	512
c8in.48xlarge	32	128	768
c8in.96xlarge	32	128	1536 *

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
c8in.metal-48xl	32	128	768
c8in.metal-96xl	32	128	1536 *
c8ine.large	2	2	8
c8ine.xlarge	4	4	16
c8ine.2xlarge	8	8	32
c8ine.4xlarge	16	16	128
c8ine.8xlarge	32	32	256
c8ine.12xlarge	32	64	384
c8ib.large	2	2	8
c8ib.xlarge	4	4	16
c8ib.2xlarge	8	8	32
c8ib.4xlarge	8	16	64
c8ib.8xlarge	16	32	128
c8ib.12xlarge	16	64	192
c8ib.16xlarge	16	64	256
c8ib.24xlarge	16	128	256
c8ib.32xlarge	32	128	512
c8ib.48xlarge	32	128	768

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
c8ib.96xlarge	32	128	1536 *
c8ib.metal-48xl	32	128	768
c8ib.metal-96xl	32	128	1536 *
c9g.medium	1	1	2
c9g.large	2	2	6
c9g.xlarge	4	4	16
c9g.2xlarge	8	8	32
c9g.4xlarge	8	16	64
c9g.8xlarge	8	32	128
c9g.12xlarge	16	64	192
c9g.16xlarge	16	64	256
c9g.24xlarge	16	128	384
c9g.48xlarge	32	128	768
c9g.metal-48xl	32	128	768
c9gd.medium	1	1	2
c9gd.large	2	2	6
c9gd.xlarge	4	4	16
c9gd.2xlarge	8	8	32

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
c9gd.4xlarge	8	16	64
c9gd.8xlarge	8	32	128
c9gd.12xlarge	16	64	192
c9gd.16xlarge	16	64	256
c9gd.24xlarge	16	128	384
c9gd.48xlarge	32	128	768
c9gd.metal-48xl	32	128	768

Memory optimized

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
r6i.large	2	2	6
r6i.xlarge	4	4	16
r6i.2xlarge	8	8	32
r6i.4xlarge	8	16	64
r6i.8xlarge	8	32	64
r6i.12xlarge	8	32	64
r6i.16xlarge	8	32	120

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
r6i.24xlarge	8	32	120
r6i.32xlarge	8	32	120
r6id.large	2	2	6
r6id.xlarge	4	4	16
r6id.2xlarge	8	8	32
r6id.4xlarge	8	16	64
r6id.8xlarge	8	32	64
r6id.12xlarge	8	32	64
r6id.16xlarge	8	32	120
r6id.24xlarge	8	32	120
r6id.32xlarge	8	32	120
r6idn.large	2	2	6
r6idn.xlarge	4	4	16
r6idn.2xlarge	8	8	32
r6idn.4xlarge	8	16	64
r6idn.8xlarge	16	32	128
r6idn.12xlarge	16	32	128
r6idn.16xlarge	16	32	240

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
r6idn.24xlarge	32	32	480
r6idn.32xlarge	32	32	512 *
r6in.large	2	2	6
r6in.xlarge	4	4	16
r6in.2xlarge	8	8	32
r6in.4xlarge	8	16	64
r6in.8xlarge	16	32	128
r6in.12xlarge	16	32	128
r6in.16xlarge	16	32	240
r6in.24xlarge	32	32	480
r6in.32xlarge	32	32	512 *
r8a.medium	1	1	3
r8a.large	2	2	6
r8a.xlarge	4	4	16
r8a.2xlarge	8	8	32
r8a.4xlarge	8	16	64
r8a.8xlarge	8	32	128
r8a.12xlarge	16	64	192

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
r8a.16xlarge	16	64	256
r8a.24xlarge	16	128	384
r8a.48xlarge	32	128	768
r8a.metal-24xl	16	128	384
r8a.metal-48xl	32	128	768
r8gb.medium	1	1	2
r8gb.large	2	2	6
r8gb.xlarge	4	4	16
r8gb.2xlarge	8	8	32
r8gb.4xlarge	8	16	64
r8gb.8xlarge	8	32	128
r8gb.12xlarge	16	64	192
r8gb.16xlarge	16	64	256
r8gb.24xlarge	16	128	384
r8gb.48xlarge	32	128	768 *
r8gb.metal-24xl	32	128	768
r8gb.metal-48xl	32	128	768 *
r8gn.medium	1	1	2

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
r8gn.large	2	2	6
r8gn.xlarge	4	4	16
r8gn.2xlarge	8	8	32
r8gn.4xlarge	8	16	64
r8gn.8xlarge	8	32	128
r8gn.12xlarge	16	64	192
r8gn.16xlarge	16	64	256
r8gn.24xlarge	16	128	384
r8gn.48xlarge	32	128	768 *
r8gn.metal-24xl	32	128	768
r8gn.metal-48xl	32	128	768 *
r8i.large	2	2	6
r8i.xlarge	4	4	16
r8i.2xlarge	8	8	32
r8i.4xlarge	8	16	64
r8i.8xlarge	8	32	128
r8i.12xlarge	16	64	192
r8i.16xlarge	16	64	256

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
r8i.24xlarge	16	128	384
r8i.32xlarge	16	128	512
r8i.48xlarge	32	128	768
r8i.96xlarge	32	128	1536
r8i.metal-48xl	32	128	768
r8i.metal-96xl	32	128	1536
r8id.large	2	2	6
r8id.xlarge	4	4	16
r8id.2xlarge	8	8	32
r8id.4xlarge	8	16	64
r8id.8xlarge	8	32	128
r8id.12xlarge	16	64	192
r8id.16xlarge	16	64	256
r8id.24xlarge	16	128	384
r8id.32xlarge	16	128	512
r8id.48xlarge	32	128	768
r8id.96xlarge	32	128	1536
r8id.metal-48xl	32	128	768

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
r8id.metal-96xl	32	128	1536
r8i-flex.large	1	1	3
r8i-flex.xlarge	2	2	8
r8i-flex.2xlarge	4	4	16
r8i-flex.4xlarge	4	8	32
r8i-flex.8xlarge	4	16	64
r8i-flex.12xlarge	8	32	96
r8i-flex.16xlarge	8	32	128
r8in.large	2	2	8
r8in.xlarge	4	4	16
r8in.2xlarge	8	8	32
r8in.4xlarge	8	16	64
r8in.8xlarge	16	32	128
r8in.12xlarge	16	64	192
r8in.16xlarge	16	64	256
r8in.24xlarge	16	128	256
r8in.32xlarge	32	128	512
r8in.48xlarge	32	128	768

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
r8in.96xlarge	32	128	1536 *
r8in.metal-48xl	32	128	768
r8in.metal-96xl	32	128	1536 *
r8idn.large	2	2	8
r8idn.xlarge	4	4	16
r8idn.2xlarge	8	8	32
r8idn.4xlarge	8	16	64
r8idn.8xlarge	16	32	128
r8idn.12xlarge	16	64	192
r8idn.16xlarge	16	64	256
r8idn.24xlarge	16	128	256
r8idn.32xlarge	32	128	512
r8idn.48xlarge	32	128	768
r8idn.96xlarge	32	128	1536 *
r8idn.metal-48xl	32	128	768
r8idn.metal-96xl	32	128	1536 *
r8ib.large	2	2	8
r8ib.xlarge	4	4	16

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
r8ib.2xlarge	8	8	32
r8ib.4xlarge	8	16	64
r8ib.8xlarge	16	32	128
r8ib.12xlarge	16	64	192
r8ib.16xlarge	16	64	256
r8ib.24xlarge	16	128	256
r8ib.32xlarge	32	128	512
r8ib.48xlarge	32	128	768
r8ib.96xlarge	32	128	1536 *
r8ib.metal-48xl	32	128	768
r8ib.metal-96xl	32	128	1536 *
r8idb.large	2	2	8
r8idb.xlarge	4	4	16
r8idb.2xlarge	8	8	32
r8idb.4xlarge	8	16	64
r8idb.8xlarge	16	32	128
r8idb.12xlarge	16	64	192
r8idb.16xlarge	16	64	256

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
r8idb.24xlarge	16	128	256
r8idb.32xlarge	32	128	512
r8idb.48xlarge	32	128	768
r8idb.96xlarge	32	128	1536 *
r8idb.metal-48xl	32	128	768
r8idb.metal-96xl	32	128	1536 *
r9g.medium	1	1	2
r9g.large	2	2	6
r9g.xlarge	4	4	16
r9g.2xlarge	8	8	32
r9g.4xlarge	8	16	64
r9g.8xlarge	8	32	128
r9g.12xlarge	16	64	192
r9g.16xlarge	16	64	256
r9g.24xlarge	16	128	384
r9g.48xlarge	32	128	768
r9g.metal-48xl	32	128	768
r9gd.medium	1	1	2

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
r9gd.large	2	2	6
r9gd.xlarge	4	4	16
r9gd.2xlarge	8	8	32
r9gd.4xlarge	8	16	64
r9gd.8xlarge	8	32	128
r9gd.12xlarge	16	64	192
r9gd.16xlarge	16	64	256
r9gd.24xlarge	16	128	384
r9gd.48xlarge	32	128	768
r9gd.metal-48xl	32	128	768
x8aedz.large	2	2	8
x8aedz.xlarge	4	4	16
x8aedz.3xlarge	4	16	48
x8aedz.6xlarge	8	32	96
x8aedz.12xlarge	8	64	192
x8aedz.24xlarge	16	128	384
x8aedz.metal-12xl	8	64	192
x8aedz.metal-24xl	16	128	384

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
x8i.large	2	2	6
x8i.xlarge	4	4	16
x8i.2xlarge	8	8	32
x8i.4xlarge	8	16	64
x8i.8xlarge	8	32	128
x8i.12xlarge	16	64	192
x8i.16xlarge	16	64	256
x8i.24xlarge	16	128	384
x8i.32xlarge	16	128	512
x8i.48xlarge	32	128	768
x8i.64xlarge	32	128	1.024
x8i.96xlarge	32	128	1536
x8i.metal-48xl	32	128	768
x8i.metal-96xl	32	128	1536

Storage optimized

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
i8ge.large	2	2	6
i8ge.xlarge	4	4	16
i8ge.2xlarge	8	8	32
i8ge.3xlarge	8	16	48
i8ge.6xlarge	8	32	96
i8ge.12xlarge	16	64	192
i8ge.18xlarge	16	128	288
i8ge.24xlarge	16	128	384
i8ge.48xlarge	32	128	1536 *

Accelerated computing

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
g7.2xlarge	8	8	32
g7.4xlarge	8	16	64
g7.8xlarge	8	32	80
g7.12xlarge	16	64	192

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
g7.24xlarge	16	128	384
g7.48xlarge	32	128	768 *

High performance computing

Tipo di istanza	Code ENA predefinite per interfaccia	Numero massimo di code ENA per interfaccia	Numero massimo di code ENA per istanza
hpc8a.96xlarge	32	128	512 *

> **Note**
>
> * Questi tipi di istanze presentano più schede di rete. Altri tipi di istanza presentano un'unica scheda di rete. Per ulteriori informazioni, consulta Schede di rete.

Configura l'allocazione delle code ENA

Sui tipi di istanza supportati, è possibile configurare il numero di code ENA per ogni ENI. Usare Console di gestione AWS, AWS CLI, o. PowerShell In Console di gestione AWS, questa impostazione viene visualizzata in ciascuna interfaccia di rete.

> **Note**
>
> Prima di configurare le code ENA, tenete presente i seguenti requisiti:
>
> - L'istanza deve essere interrotta prima di configurare il numero di code ENA.
> - Il valore per le code ENA deve essere una potenza di 2, ad esempio 1, 2, 4, 8, 16 o 32.

- Il numero di code su ogni singolo ENI non può superare il numero di vCPU sull'istanza.

Prima di modificare il numero delle code, controllate il conteggio attuale con il seguente comando.

AWS CLI

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

PowerShell

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.NetworkInterfaces |
  Select-Object NetworkInterfaceId,
    @{N='DeviceIndex';E={$_.Attachment.DeviceIndex}},
    @{N='AttachmentId';E={$_.Attachment.AttachmentId}},
    @{N='EnaQueueCount';E={$_.Attachment.EnaQueueCount}}
```

Collegate un'interfaccia di rete con le code ENA

Nel seguente esempio, 16 code ENA sono configurate su un ENI.

AWS CLI

Per collegare un'interfaccia di rete alle code ENA

Usare il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/attach-network-interface.html attach-network-interface.

```
aws ec2 attach-network-interface \
  --network-interface-id eni-abcdef01234567890 \
  --instance-id i-1234567890abcdef0 \
  --device-index 1 \
  --ena-queue-count 16
```

PowerShell

Per collegare un'interfaccia di rete alle code ENA

Utilizza il cmdlet Add-EC2NetworkInterface.

```
Add-EC2NetworkInterface `
  -NetworkInterfaceId eni-abcdef01234567890 `
  -InstanceId i-1234567890abcdef0 `
  -DeviceIndex 1 `
  -EnaQueueCount 16
```

Avviare un'istanza con code ENA

Nell'esempio seguente, 16 code ENA sono configurate ciascuna su 3 ENI.

AWS CLI

Per avviare un'istanza con code ENA

Utilizzare il comando run-instances.

```
aws ec2 run-instances \
  --image-id ami-1234567890abcdef0 \
  --instance-type c8i.4xlarge \
  --network-interfaces \
    "[{\"DeviceIndex\":0,\"SubnetId\":\"subnet-abcdef01234567890\",\"EnaQueueCount
\":16},
      {\"DeviceIndex\":1,\"SubnetId\":\"subnet-abcdef01234567890\",\"EnaQueueCount
\":16},
      {\"DeviceIndex\":2,\"SubnetId\":\"subnet-abcdef01234567890\",\"EnaQueueCount
\":16}]"
```

PowerShell

Per avviare un'istanza con code ENA

Utilizza il cmdlet New-EC2Instance.

```
New-EC2Instance `
  -ImageId ami-1234567890abcdef0 `
  -InstanceType c8i.4xlarge `
  -NetworkInterface @(
    @{DeviceIndex=0; SubnetId="subnet-abcdef01234567890"; EnaQueueCount=16},
    @{DeviceIndex=1; SubnetId="subnet-abcdef01234567890"; EnaQueueCount=16},
    @{DeviceIndex=2; SubnetId="subnet-abcdef01234567890"; EnaQueueCount=16}
  )
```

Modificare le code ENA su un'interfaccia di rete esistente

Nel seguente esempio, 16 code ENA sono configurate su un ENI.

AWS CLI

Per modificare le code ENA su un'interfaccia di rete

Utilizzare il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-network-interface-attribute.html modify-network-interface-attribute.

```
aws ec2 modify-network-interface-attribute \
  --network-interface-id eni-1234567890abcdef0 \
  --attachment AttachmentId=eni-attach-1234567890abcdef0,EnaQueueCount=16
```

PowerShell

Per modificare le code ENA su un'interfaccia di rete

Utilizza il cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
  -NetworkInterfaceId eni-1234567890abcdef0 `
  -Attachment_AttachmentId eni-attach-1234567890abcdef0 `
  -Attachment_EnaQueueCount 16
```

Nell'esempio seguente, il numero di ENA viene ripristinato al valore predefinito.

AWS CLI

```
aws ec2 modify-network-interface-attribute \
  --network-interface-id eni-1234567890abcdef0 \
  --attachment AttachmentId=eni-attach-1234567890abcdef0,DefaultEnaQueueCount=true
```

PowerShell

```
Edit-EC2NetworkInterfaceAttribute `
  -NetworkInterfaceId eni-1234567890abcdef0 `
  -Attachment_AttachmentId eni-attach-1234567890abcdef0 `
  -Attachment_DefaultEnaQueueCount $true
```

Risolvere i problemi relativi al driver ENA kernel su Linux

L'Adattatore elastico di rete (ENA) è progettato per migliorare lo stato del sistema operativo e ridurre le possibilità di interruzione a lungo termine a causa di un comportamento inatteso dell'hardware e/o di guasti. La struttura dell'ENA rende i guasti dei dispositivi o dei driver il più chiari possibile al sistema. Questo argomento fornisce le informazioni relative alla risoluzione dei problemi dell'ENA.

Se è impossibile connettersi all'istanza, iniziare dalla sezione Risolvere i problemi di connettività.

Se si verifica un peggioramento delle prestazioni dopo la migrazione a un tipo di istanza di sesta generazione, consultare l'articolo Cosa devo fare prima di eseguire la migrazione della mia istanza EC2 a un'istanza di sesta generazione per assicurarmi di ottenere le massime prestazioni di rete?

Se è possibile connettersi all'istanza, è possibile raccogliere informazioni diagnostiche utilizzando i meccanismi di rilevamento e riparazione dei guasti descritti nelle sezioni successive di questo argomento.

Indice

- Risolvere i problemi di connettività
- Keep-alive meccanismo
- Timeout lettura registro
- Statistiche
- Log di errore driver in Syslog
- Sub-optimal notifiche di configurazione

Risolvere i problemi di connettività

Se si perde la connettività durante l'abilitazione della rete avanzata, il modulo `ena` potrebbe essere incompatibile con il kernel dell'istanza attualmente in esecuzione. Questo può accadere se si installa il modulo per una specifica versione del kernel (senza dkms o con un file dkms.conf non configurato correttamente), quindi il kernel di istanza viene aggiornato. Se il kernel di istanza caricato al momento dell'avvio non ha il modulo `ena` correttamente installato, l'istanza non riconoscerà l'adattatore di rete e l'istanza diventerà irraggiungibile.

Se si attivano le reti avanzate per un'istanza PV o AMI, l'istanza può risultare irraggiungibile.

Se l'istanza diventa irraggiungibile dopo aver abilitato le reti avanzate con l'ENA, è possibile disattivare l'attributo `enaSupport` per l'istanza e quest'ultima tornerà all'adattatore di rete originale.

Per disattivare la rete avanzata con ENA (EBS-backed istanze)

1. Dal computer locale, interrompi l'istanza utilizzando la console Amazon EC2, il comando stop-instances () o il AWS CLI cmdlet (). Stop-EC2Instance AWS Strumenti per PowerShell
2. Dal computer locale, disabilita l'attributo di rete avanzato utilizzando il comando modify-instance-attribute con l'opzione o il cmdlet con il parametro. `--no-ena-support` Edit-EC2InstanceAttribute `-EnaSupport $false`
3. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2, il comando start-instances o il cmdlet. https://docs.aws.amazon.com/cli/latest/reference/ec2/start-instances.html Start-EC2Instance
4. (Facoltativo) Connettersi all'istanza e provare a reinstallare il modulo `ena` con la versione del kernel attuale seguendo i passaggi in Abilitazione delle reti avanzate con ENA su istanze EC2.

Disattivare le reti avanzate con l'ENA (istanze supportate da instance store)

1. Creare una nuova AMI come descritto in Crea un' S3-backed AMI Amazon.
2. Quando registri l'AMI, assicurati di includere l'`--no-ena-support`opzione nel comando stop-instances () o il parametro nel cmdlet.AWS CLI`-EnaSupport $false` Register-EC2Image

Keep-alive meccanismo

Il dispositivo ENA segnala gli eventi keep-alive con una frequenza fissa (di solito una volta al secondo). Il driver dell'ENA è dotato di un meccanismo watchdog che controlla la presenza di questi messaggi keep-alive. Se sono presenti uno o più messaggi, il watchdog viene riarrestato, altrimenti il driver ritiene che il dispositivo abbia subito un guasto e procede come segue:

- Scarica le sue statistiche attuali su syslog
- Reimposta il dispositivo ENA
- Reimposta lo stato del driver ENA

La procedura di ripristino sopra descritta può provocare una perdita di traffico per un breve periodo di tempo (le connessioni TCP devono poter essere ripristinate), ma non dovrebbe influire in altro modo sull'utente.

Il dispositivo ENA può anche richiedere indirettamente una procedura di ripristino del dispositivo, non inviando una notifica keep-alive, per esempio se il dispositivo ENA raggiunge uno stato sconosciuto dopo aver caricato una configurazione irrecuperabile.

Di seguito è riportato un esempio della procedura di ripristino:

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog
 process initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current
 statistics
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.......
........
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the
 end of the down process, the driver discards incomplete packets.
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The
 driver begins its up process
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1
 implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date
 [Wed Apr  6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
```

```
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset
 process is complete
```

Timeout lettura registro

L'architettura ENA suggerisce un uso limitato delle operazioni di lettura mappate in memoria I/O (MMIO). I registri MMIO sono accessibili dal driver del dispositivo ENA solo durante la procedura di inizializzazione.

Se i log del driver (disponibili nell'output dmesg) indicano errori nelle operazioni di lettura, ciò può essere causato da un driver incompatibile o compilato in modo errato, da un dispositivo hardware occupato o da un guasto hardware.

Le voci di log intermittenti che indicano errori nelle operazioni di lettura non devono essere considerate un problema; in questo caso il driver le riproverà. Tuttavia, una sequenza di voci di log contenenti errori di lettura indica un problema al driver o all'hardware.

Di seguito è riportato un esempio di voce di log del driver che indica un errore nell'operazione di lettura dovuto a un timeout:

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[2] offset[8] actual: req id[57007] offset[0]
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

Statistiche

Se si verificano prestazioni di rete insufficienti o problemi di latenza, è necessario recuperare le statistiche del dispositivo ed esaminarle. Si possono ottenere tali statistiche utilizzando ethtool, come mostrato di seguito.

```
[ec2-user ~]$ ethtool -S ethN
NIC statistics:
 tx_timeout: 0
 suspend: 0
 resume: 0
 wd_expired: 0
 interface_up: 1
 interface_down: 0
 admin_q_pause: 0
 bw_in_allowance_exceeded: 0
```

```
  bw_out_allowance_exceeded: 0
  pps_allowance_exceeded: 0
  conntrack_allowance_available: 450878
  conntrack_allowance_exceeded: 0
  linklocal_allowance_exceeded: 0
  queue_0_tx_cnt: 4329
  queue_0_tx_bytes: 1075749
  queue_0_tx_queue_stop: 0
  ...
```

I seguenti parametri di output del comando sono descritti di seguito:

`tx_timeout`: *N*

Numero di volte in cui il watchdog Netdev è stato attivato.

`suspend`: *N*

Numero di volte in cui il driver ha eseguito un'operazione di sospensione.

`resume`: *N*

Numero di volte in cui il driver ha eseguito un'operazione di ripresa.

`wd_expired`: *N*

Numero di volte in cui il driver non ha ricevuto l'evento keep-alive nei tre secondi precedenti.

`interface_up`: *N*

Numero di volte in cui l'interfaccia ENA è stata attivata.

`interface_down`: *N*

Numero di volte in cui l'interfaccia ENA è stata disattivata.

`admin_q_pause`: *N*

Numero di volte in cui la coda di amministrazione non è stata trovata in uno stato di esecuzione.

`bw_in_allowance_exceeded`: *N*

Il numero di pacchetti accordati o rilasciati perché la larghezza di banda aggregata in ingresso ha superato il valore massimo per l'istanza.

`bw_out_allowance_exceeded`: *N*

Il numero di pacchetti accodati o rilasciati perché la larghezza di banda aggregata in uscita ha superato il valore massimo per l'istanza.

`pps_allowance_exceeded`: *N*

Il numero di pacchetti accodati o rilasciati perché il PPS bidirezionale ha superato il valore massimo per l'istanza. *

`conntrack_allowance_available`: *N*

Il numero di connessioni tracciate che possono essere stabilite dall'istanza prima di raggiungere il limite Connessioni tracciate di quel tipo di istanza. Disponibile solo per le istanze Nitro-based . Non supportato con le istanze FreeBSD o gli ambienti DPDK.

`conntrack_allowance_exceeded`: *N*

Il numero di pacchetti accodati o rilasciati perché il rilevamento delle connessioni ha superato il valore massimo per l'istanza e non è stato possibile stabilire nuove connessioni. Ciò può comportare la perdita di pacchetti per il traffico da o verso l'istanza.

`linklocal_allowance_exceeded`: *N*

Il numero di pacchetti accodati o rilasciati perché il PPS del traffico verso i servizi proxy locali ha superato il valore massimo per l'interfaccia di rete. Ciò influisce sul traffico verso il servizio Amazon DNS, il servizio di metadati dell'istanza e il servizio di sincronizzazione oraria di Amazon, ma non influisce sul traffico verso i resolver DNS personalizzati.

`queue_`*N*`_tx_cnt`: *N*

Numero di pacchetti trasmessi per questa coda.

`queue_`*N*`_tx_bytes`: *N*

Numero di byte trasmessi per questa coda.

`queue_`*N*`_tx_queue_stop`: *N*

Il numero di volte in cui la coda *N* è stata piena e interrotta.

`queue_`*N*`_tx_queue_wakeup`: *N*

Il numero di volte in cui la coda è stata *N* ripresa dopo essere stata interrotta.

`queue_`*N*`_tx_dma_mapping_err`: *N*

Conteggio errori di accesso diretto alla memoria. Se questo valore non è pari a 0, significa che le risorse di sistema sono scarse.

`queue_`*N*`_tx_linearize`: *N*

Numero di volte in cui è stata tentata la linearizzazione SKB per questa coda.

`queue_N_tx_linearize_failed`: *N*

Numero di volte in cui la linearizzazione SKB non è andata a buon fine per questa coda.

`queue_N_tx_napi_comp`: *N*

Numero di volte in cui il gestore `napi` ha chiamato `napi_complete` per questa coda.

`queue_N_tx_tx_poll`: *N*

Numero di volte in cui il gestore `napi` è stato programmato per questa coda.

`queue_N_tx_doorbells`: *N*

Numero di campanelli di trasmissione per questa coda.

`queue_N_tx_prepare_ctx_err`: *N*

Numero di volte in cui `ena_com_prepare_tx` non è andato a buon fine per questa coda.

`queue_N_tx_bad_req_id`: *N*

`req_id` non valido per questa coda. Il `req_id` valido è zero, meno la `queue_size`, meno 1.

`queue_N_tx_llq_buffer_copy`: *N*

Numero di pacchetti la cui dimensione delle intestazioni è maggiore della voce llq per questa coda.

`queue_N_tx_missed_tx`: *N*

Numero di pacchetti trasmessi lasciati incompleti per questa coda.

`queue_N_tx_unmask_interrupt`: *N*

Numero di volte in cui l'interrupt tx è stato smascherato per questa coda.

`queue_N_rx_cnt`: *N*

Numero di pacchetti ricevuti per questa coda.

`queue_N_rx_bytes`: *N*

Numero di byte ricevuti per questa coda.

`queue_N_rx_rx_copybreak_pkt`: *N*

Numero di volte in cui la coda rx ha ricevuto un pacchetto inferiore alla dimensione del pacchetto rx_copybreak per questa coda.

`queue_N_rx_csum_good`: *N*

Numero di volte in cui la coda rx ha ricevuto un pacchetto in cui il checksum è stato controllato ed era corretto per questa coda.

`queue_N_rx_refil_partial`: *N*

Numero di volte in cui il driver non è riuscito a riempire la parte vuota della coda rx con i buffer per questa coda. Se questo valore non è pari a 0, significa che le risorse di memoria sono scarse.

`queue_N_rx_bad_csum`: *N*

Numero di volte che la coda `rx` ha avuto un checksum negativo per questa coda (solo se è supportato l'offload del checksum).

`queue_N_rx_page_alloc_fail`: *N*

Numero di volte in cui l'assegnazione della pagina non è andata a buon fine per questa coda. Se questo valore non è pari a 0, significa che le risorse di memoria sono scarse.

`queue_N_rx_skb_alloc_fail`: *N*

Numero di volte in cui l'assegnazione dell'SKB non è andata a buon fine per questa coda. Se questo valore non è pari a 0, significa che le risorse di sistema sono scarse.

`queue_N_rx_dma_mapping_err`: *N*

Conteggio errori di accesso diretto alla memoria. Se questo valore non è pari a 0, significa che le risorse di sistema sono scarse.

`queue_N_rx_bad_desc_num`: *N*

Troppi buffer per pacchetto. Se questo valore non è pari a 0, significa che si utilizzano buffer molto piccoli.

`queue_N_rx_bad_req_id`: *N*

Il req_id per questa coda non è valido. Il req_id valido è compreso tra [0, queue_size - 1].

`queue_N_rx_empty_rx_ring`: *N*

Numero di volte in cui la coda rx è stata vuota per questa coda.

`queue_N_rx_csum_unchecked`: *N*

Numero di volte in cui la coda rx ha ricevuto un pacchetto il cui checksum non è stato controllato per questa coda.

`queue_N_rx_xdp_aborted`: *N*

Numero di volte in cui un pacchetto XDP è stato classificato come XDP_ABORT.

`queue_N_rx_xdp_drop`: *N*

Numero di volte in cui un pacchetto XDP è stato classificato come XDP_DROP.

`queue_N_rx_xdp_pass`: *N*

Numero di volte in cui un pacchetto XDP è stato classificato come XDP_PASS.

`queue_N_rx_xdp_tx`: *N*

Numero di volte in cui un pacchetto XDP è stato classificato come XDP_TX.

`queue_N_rx_xdp_invalid`: *N*

Numero di volte in cui il codice restituito da XDP per il pacchetto non era valido.

`queue_N_rx_xdp_redirect`: *N*

Numero di volte in cui un pacchetto XDP è stato classificato come XDP_REDIRECT.

`queue_N_xdp_tx_cnt`: *N*

Numero di pacchetti trasmessi per questa coda.

`queue_N_xdp_tx_bytes`: *N*

Numero di byte trasmessi per questa coda.

`queue_N_xdp_tx_queue_stop`: *N*

Numero di volte in cui questa coda era piena e si è arrestata.

`queue_N_xdp_tx_queue_wakeup`: *N*

Numero di volte in cui questa coda ha ripreso dopo essersi arrestata.

`queue_N_xdp_tx_dma_mapping_err`: *N*

Conteggio errori di accesso diretto alla memoria. Se questo valore non è pari a 0, significa che le risorse di sistema sono scarse.

`queue_N_xdp_tx_linearize`: *N*

Numero di volte in cui è stata tentata la linearizzazione del buffer XDP per questa coda.

`queue_N_xdp_tx_linearize_failed`: *N*

Numero di volte in cui la linearizzazione del buffer XDP non è andata a buon fine per questa coda.

`queue_N_xdp_tx_napi_comp`: *N*

Numero di volte in cui il gestore napi ha chiamato napi_complete per questa coda.

`queue_N_xdp_tx_tx_poll`: *N*

Numero di volte in cui il gestore napi è stato programmato per questa coda.

`queue_N_xdp_tx_doorbells`: *N*

Numero di campanelli di trasmissione per questa coda.

`queue_N_xdp_tx_prepare_ctx_err`: *N*

Numero di volte in cui ena_com_prepare_tx non è andato a buon fine per questa coda. Questo valore deve essere sempre zero; altrimenti, consultare i log del driver.

`queue_N_xdp_tx_bad_req_id`: *N*

Il req_id per questa coda non è valido. Il req_id valido è compreso tra [0, queue_size - 1].

`queue_N_xdp_tx_llq_buffer_copy`: *N*

Numero di pacchetti che hanno copiato le intestazioni utilizzando la copia del buffer llq per questa coda.

`queue_N_xdp_tx_missed_tx`: *N*

Numero di volte in cui una voce di coda tx ha perso un timeout di completamento per questa coda.

`queue_N_xdp_tx_unmask_interrupt`: *N*

Numero di volte in cui l'interrupt tx è stato smascherato per questa coda.

`ena_admin_q_aborted_cmd`: *N*

Il numero di comandi di amministrazione che sono stati interrotti. Questo solitamente accade durante la procedura di auto-ripristino.

`ena_admin_q_submitted_cmd`: *N*

Numero di campanelli di coda di amministrazione.

`ena_admin_q_completed_cmd`: *N*

Numero di completamenti di coda di amministrazione.

`ena_admin_q_out_of_space`: *N*

Numero di volte in cui il driver ha tentato di inviare un nuovo comando di amministrazione, ma la coda era piena.

`ena_admin_q_no_completion: N`

Numero di volte in cui il driver non ha ricevuto un completamento di amministrazione per un comando.

Log di errore driver in Syslog

Il driver ENA scrive messaggi di log a syslog durante l'avvio del sistema. In caso di problemi, è possibile esaminare questi log per cercare errori. Di seguito è riportato un esempio di informazioni registrate dal driver ENA in syslog durante l'avvio del sistema, insieme ad alcune annotazioni per la selezione dei messaggi.

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.416939] [ENA_COM:
 ena_com_validate_version] ena device version: 0.10
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.420915] [ENA_COM:
 ena_com_validate_version] ena controller version: 0.0.1 implementation version 1
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.256831] ena 0000:00:03.0: Device
 watchdog is Enabled
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.672947] ena 0000:00:03.0: creating 8 io
 queues. queue size: 1024
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.680885] [ENA_COM:
 ena_com_init_interrupt_moderation] Feature 20 isn't supported  // Interrupt moderation
 is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.691609] [ENA_COM:
 ena_com_get_feature_ex] Feature 10 isn't supported // RSS HASH function configuration
 is not supported by the
 device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.694583] [ENA_COM:
 ena_com_get_feature_ex] Feature 18 isn't supported //RSS HASH input source
 configuration is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.697433] [ENA_COM:
 ena_com_set_host_attributes] Set host attribute isn't supported
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.701064] ena 0000:00:03.0 (unnamed
 net_device) (uninitialized): Cannot set host attributes
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.704917] ena 0000:00:03.0: Elastic
 Network Adapter (ENA) found at mem f3000000, mac addr 02:8a:3c:1e:13:b5 Queues 8
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  480.805037] EXT4-fs (xvda1): re-mounted.
 Opts: (null)
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  481.025842] NET: Registered protocol family
 10
```

Quali errori posso ignorare?

I seguenti avvisi, che possono apparire nei log di errore del sistema, possono essere ignorati per l'Adattatore elastico di rete:

Set host attribute isn't supported (L'impostazione dell'attributo dell'host non è supportata)

Gli attributi dell'host non sono supportati da questo dispositivo.

failed to alloc buffer for rx queue (allocazione del buffer per la coda rx non riuscita)

Si tratta di un errore recuperabile, che indica che potrebbe essersi verificato un problema di pressione di memoria quando l'errore è stato generato.

La funzionalità non è supportata *X*

La funzionalità a cui si fa riferimento non è supportata dall'Adattatore elastico di rete. I valori possibili per *X* includono:

- 10: la configurazione della funzione Hash RSS non è supportata per questo dispositivo.
- 12: la configurazione della tabella di Riferimento indiretto RSS non è supportata per questo dispositivo.
- 18: la configurazione dell'Input Hash RSS non è supportata per questo dispositivo.
- 20: la moderazione dell'interruzione non è supportata per questo dispositivo.
- 27: il driver dell'Adattatore elastico di rete non supporta il polling delle funzionalità Ethernet da snmpd.

Failed to config AENQ (Impossibile configurare AENQ)

L'Adattatore elastico di rete non supporta la configurazione AENQ.

Trying to set unsupported AENQ events (Tentativo di impostare eventi AENQ non supportati)

Questo errore indica un tentativo di impostare un gruppo di eventi AENQ non supportato dall'Adattatore elastico di rete.

Sub-optimal notifiche di configurazione

Il dispositivo ENA rileva le impostazioni di configurazione non ottimali nel driver che è possibile modificare. Il dispositivo notifica il driver ENA e registra un avviso sulla console. Nell'esempio seguente viene illustrato il formato del messaggio di avviso.

```
Sub-optimal configuration notification code: 1. Refer to AWS ENA documentation for
 additional details and mitigation options.
```

L'elenco seguente mostra i dettagli del codice di notifica e le operazioni consigliate per gli esiti di configurazione non ottimali.

- Codice 1: non è consigliato utilizzare ENA Express con la configurazione LLQ estesa

  ENA Express ENI è configurato con LLQ esteso. Questa configurazione non è ottimale e potrebbe influire sulle prestazioni di ENA Express. Si consiglia di disabilitare le impostazioni LLQ estese quando si utilizzano ENI ENA Express, come indicato di seguito.

  ```
  sudo rmmod ena && sudo modprobe ena force_large_llq_header=0
  ```

  Per ulteriori informazioni sulla configurazione ottimale di ENA Express, consulta la pagina Migliora le prestazioni di rete tra le istanze EC2 con ENA Express.

- Codice 2: non è consigliato utilizzare ENI ENA Express con una profondità di coda Tx non ottimale

  ENI ENA Express è configurato con una profondità di coda Tx non ottimale. Questa configurazione potrebbe influire sulle prestazioni di ENA Express. Si consiglia di estendere tutte le code Tx al valore massimo per l'interfaccia di rete quando si utilizzano ENI ENA Express, come indicato di seguito.

  Per regolare le dimensioni della LLQ, è possibile eseguire i seguenti comandi ethtool. Per ulteriori informazioni su come controllare, interrogare e abilitare Wide-LLQ, consulta l'argomento Large Low-Latency Queue (Large LLQ) della documentazione del driver del kernel Linux per ENA nel repository Amazon Drivers. GitHub

  ```
  ethtool -g interface
  ```

  Imposta le code Tx alla profondità massima:

  ```
  ethtool -G interface tx depth
  ```

  Per ulteriori informazioni sulla configurazione ottimale di ENA Express, consulta la pagina Migliora le prestazioni di rete tra le istanze EC2 con ENA Express.

- Codice 3: un file ENA con dimensioni LLQ regolari e traffico di pacchetti Tx supera la dimensione massima supportata dall'intestazione

  Per impostazione predefinita, ENA LLQ supporta intestazioni del pacchetto Tx di dimensioni fino a 96 byte. Se la dimensione dell'intestazione del pacchetto è maggiore di 96 byte, il pacchetto viene

eliminato. Per mitigare questo problema, si consiglia di abilitare una LLQ estesa, che aumenta la dimensione dell'intestazione del pacchetto Tx supportata fino a un massimo di 224 byte.

Tuttavia, quando abiliti Wide-LLQ, la dimensione massima dell'anello Tx viene ridotta da 1000 a 512 voci. Wide-LLQ è abilitato per impostazione predefinita per tutti i tipi di istanze di Nitro v4 e versioni successive.

- I tipi di istanza Nitro v4 hanno una dimensione massima predefinita dell'anello Tx con LLQ estesa di 512 voci, che non può essere modificata.
- I tipi di istanza Nitro v5 hanno una dimensione predefinita dell'anello Tx con LLQ estesa di 512 voci, che può essere aumentata fino a 1000 voci.

Per regolare le dimensioni della LLQ, è possibile eseguire i seguenti comandi ethtool. Per ulteriori informazioni su come controllare, interrogare e abilitare Wide-LLQ, consulta l'argomento Large Low-Latency Queue (Large LLQ) della documentazione del driver del kernel Linux per ENA nel repository Amazon Drivers. GitHub

Trova la profondità massima delle code:

```
ethtool -g interface
```

Imposta le code Tx alla profondità massima:

```
ethtool -G interface tx depth
```

Risoluzione dei problemi del driver dell'Adattatore elastico di rete per Windows

L'Adattatore elastico di rete (ENA) è progettato per migliorare lo stato del sistema operativo e ridurre le possibilità di interruzione a causa di un comportamento inatteso dell'hardware e/o di guasti che può alterare il funzionamento dell'istanza Windows. La struttura dell'ENA rende i guasti dei dispositivi o dei driver il più chiari possibile al sistema operativo.

Raccogliere informazioni diagnostiche sull'istanza

I passaggi per aprire gli strumenti del sistema operativo Windows (OS) variano a seconda della versione del sistema operativo installata nell'istanza. Nelle seguenti sezioni, utilizziamo la finestra di dialogo Esegui per aprire gli strumenti, che funziona allo stesso modo in tutte le versioni del sistema operativo. Tuttavia, è possibile accedere a questi strumenti utilizzando qualsiasi metodo si preferisca.

Accesso alla finestra di dialogo Esegui

- Utilizzando la combinazione di tasti logo Windows: `Windows` + `R`
- Utilizzando la barra di ricerca:
  - Inserire `run` nella barra di ricerca.
  - Selezionare l'applicazione Esegui dai risultati di ricerca.

Alcuni passaggi richiedono che il menu contestuale acceda alle proprietà o alle azioni sensibili al contesto. Esistono diversi modi per eseguire questa operazione, a seconda della versione del sistema operativo e dell'hardware.

Accesso al menu contestuale

- Utilizzando il mouse: fare clic con il pulsante destro del mouse su un elemento per visualizzare il menu contestuale.
- Utilizzando la tastiera:
  - A seconda della versione del sistema operativo, utilizzare `Shift` + `F10`, oppure `Ctrl` + `Shift` + `F10`.
  - Se la tastiera presenta il tasto contestuale (tre linee orizzontali in una casella), seleziona l'elemento desiderato e premi il tasto contestuale.

Se è possibile connettersi all'istanza, utilizzare le seguenti tecniche per raccogliere informazioni diagnostiche per la risoluzione dei problemi.

Controllo dello stato del dispositivo ENA

Per controllare lo stato del driver ENA per Windows utilizzando Gestione dispositivi in Windows, attenersi alla seguente procedura:

1. Aprire la finestra di dialogo Esegui utilizzando uno dei metodi descritti nella sezione precedente.
2. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
4. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
5. Scegliere il nome o aprire il menu contestuale per Adattatore elastico di rete Amazon e quindi Proprietà. In questo modo si apre la finestra di dialogo Proprietà di Amazon Elastic Network Adapter.

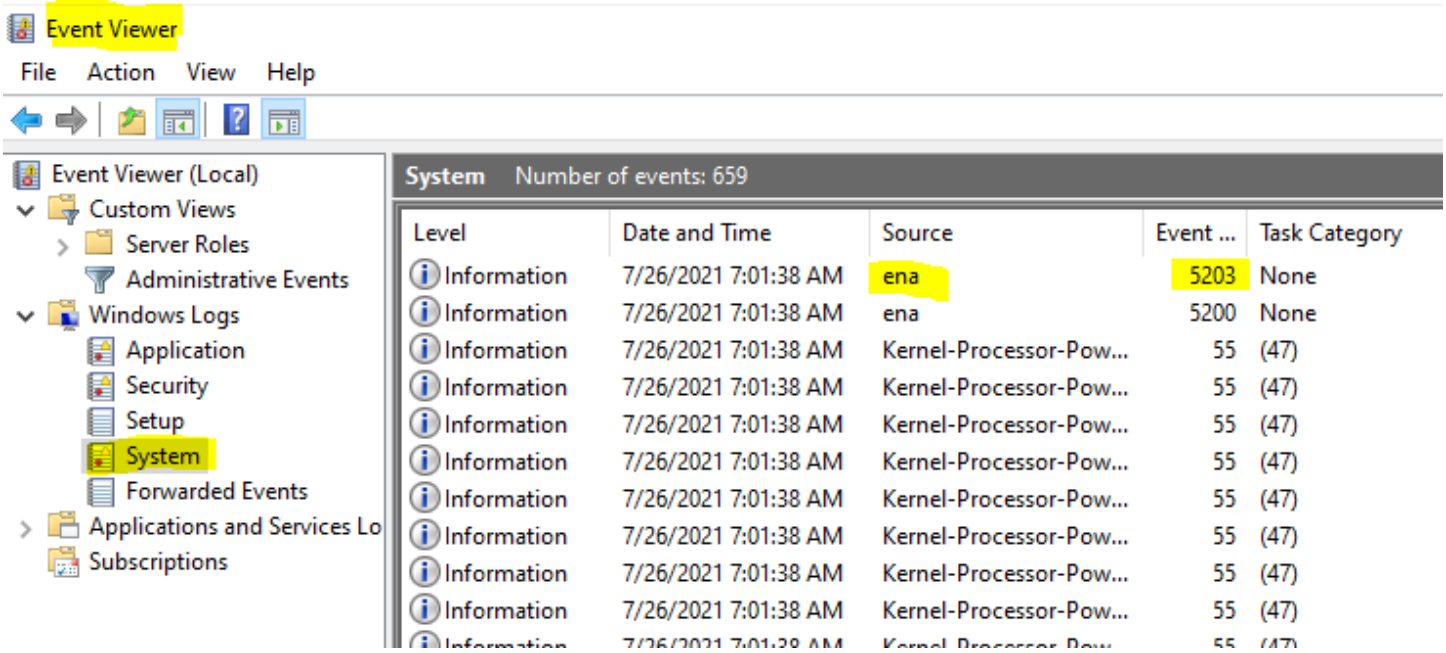
6. Verificare che il messaggio nella scheda Generale mostri "Questo dispositivo funziona correttamente".

Indagare sui messaggi di evento del driver

Per esaminare i registri degli eventi del driver ENA per Windows utilizzando il Visualizzatore eventi di Windows, attenersi alla seguente procedura:

1. Aprire la finestra di dialogo Esegui utilizzando uno dei metodi descritti nella sezione precedente.
2. Per aprire Visualizzatore eventi in Windows, inserire `eventvwr.msc` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra del Visualizzatore eventi di Windows.
4. Espandere il menu Eventi di Windows, quindi scegliere Sistema.
5. In Operazioni, nel pannello in alto a destra, scegliere Filtra log corrente. Viene visualizzata la finestra di dialogo di filtro.
6. Nel campo Origine eventi, inserire `ena`. Ciò limita i risultati agli eventi generati dal driver ENA per Windows.
7. Scegli OK. Ciò mostra i risultati del log degli eventi filtrati nelle sezioni di dettaglio della finestra.
8. Per espandere i dettagli, selezionare un messaggio di evento dall'elenco.

L'esempio seguente mostra un evento driver ENA nell'elenco degli eventi di sistema del Visualizzatore eventi di Windows:



Sintesi del messaggio di evento

La tabella seguente mostra i messaggi di evento generati dal driver ENA per Windows.

Input

ID evento	Descrizione dell'evento del driver ENA	Tipo
5001	Le risorse del hardware sono esaurite	Errore
5002	L'adattatore ha rilevato un errore hardware	Errore
5005	Il timeout impostato sull'adattatore per un'operazione NDIS non completata in modo tempestivo è scaduto.	Errore
5032	Impossibile ripristinare il dispositivo	Errore
5200	L'adattatore è stato inizializzato	Messaggio informativo
5201	L'adattatore è stato arrestato	Messaggio informativo
5202	L'adattatore è stato sospeso	Messaggio informativo
5203	L'adattatore è stato riavviato	Messaggio informativo
5204	L'adattatore è stato spento	Messaggio informativo
5205	L'adattatore è stato ripristinato	Errore
5206	L'adattatore è stato rimosso inaspettatamente	Errore
5208	La routine di inizializzazione dell'adattatore non è riuscita	Errore

ID evento	Descrizione dell'evento del driver ENA	Tipo
5210	L'adattatore ha riscontrato e risolto con successo un problema interno	Errore

Visualizzazione dei parametri relativi alle prestazioni

Il driver ENA per Windows pubblica i parametri delle prestazioni di rete dalle istanze in cui sono attivati. È possibile visualizzare e abilitare le metriche sull'istanza utilizzando l'applicazione nativa Performance Monitor (Monitor di sistema). Per ulteriori informazioni sui parametri prodotti dal driver ENA per Windows, consultare Monitoraggio delle prestazioni di rete per le impostazioni ENA dell'istanza EC2.

Nelle istanze in cui le metriche ENA sono abilitate e l' CloudWatch agente Amazon è installato, CloudWatch raccoglie le metriche associate ai contatori in Windows Performance Monitor, oltre ad alcune metriche avanzate per ENA. Queste parametri vengono raccolti in aggiunta ai parametri abilitati per impostazione predefinita nelle istanze EC2. Per ulteriori informazioni sulle metriche, consulta le metriche raccolte dall'agente nella Amazon User Guide. CloudWatch CloudWatch

> **Note**
>
> I parametri delle prestazioni sono disponibili per le versioni 2.4.0 e successive dei driver ENA (anche per la versione 2.2.3). È stato eseguito il ripristino dello stato precedente del driver ENA versione 2.2.4 a causa del potenziale peggioramento delle prestazioni nelle istanze EC2 di sesta generazione. Si consiglia di eseguire l'aggiornamento alla versione corrente del driver per assicurarsi di disporre degli aggiornamenti più recenti.

Alcuni dei modi in cui è possibile utilizzare i parametri delle prestazioni includono:

- Risoluzione dei problemi di prestazioni delle istanze.
- Scegliere la dimensione dell'istanza corretta per un dato carico di lavoro.
- Pianificare in modo proattivo le attività di dimensionamento.
- Applicazioni di benchmark per determinare se le prestazioni sono massimizzate sono disponibili su un'istanza.

Frequenza di aggiornamento

Per impostazione predefinita, il driver aggiorna i parametri utilizzando un intervallo di 1 secondo. Tuttavia, l'applicazione che raccoglie i parametri potrebbe utilizzare un intervallo diverso per il polling. È possibile modificare l'intervallo di aggiornamento in Gestione dispositivi, utilizzando le proprietà avanzate per il driver.

Per modificare l'intervallo di aggiornamento dei parametri per il driver ENA per Windows, attenersi alla seguente procedura:

1. Aprire la finestra di dialogo Esegui utilizzando uno dei metodi descritti nella sezione precedente.
2. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
4. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
5. Scegliere il nome o aprire il menu contestuale per Adattatore elastico di rete Amazon e quindi Proprietà. In questo modo si apre la finestra di dialogo Proprietà di Amazon Elastic Network Adapter.
6. Apertura della scheda Avanzate nella finestra popup.
7. Dalla Proprietà, scegliere Intervallo di aggiornamento dei parametri per modificare il valore.
8. Al termine, scegliere OK.

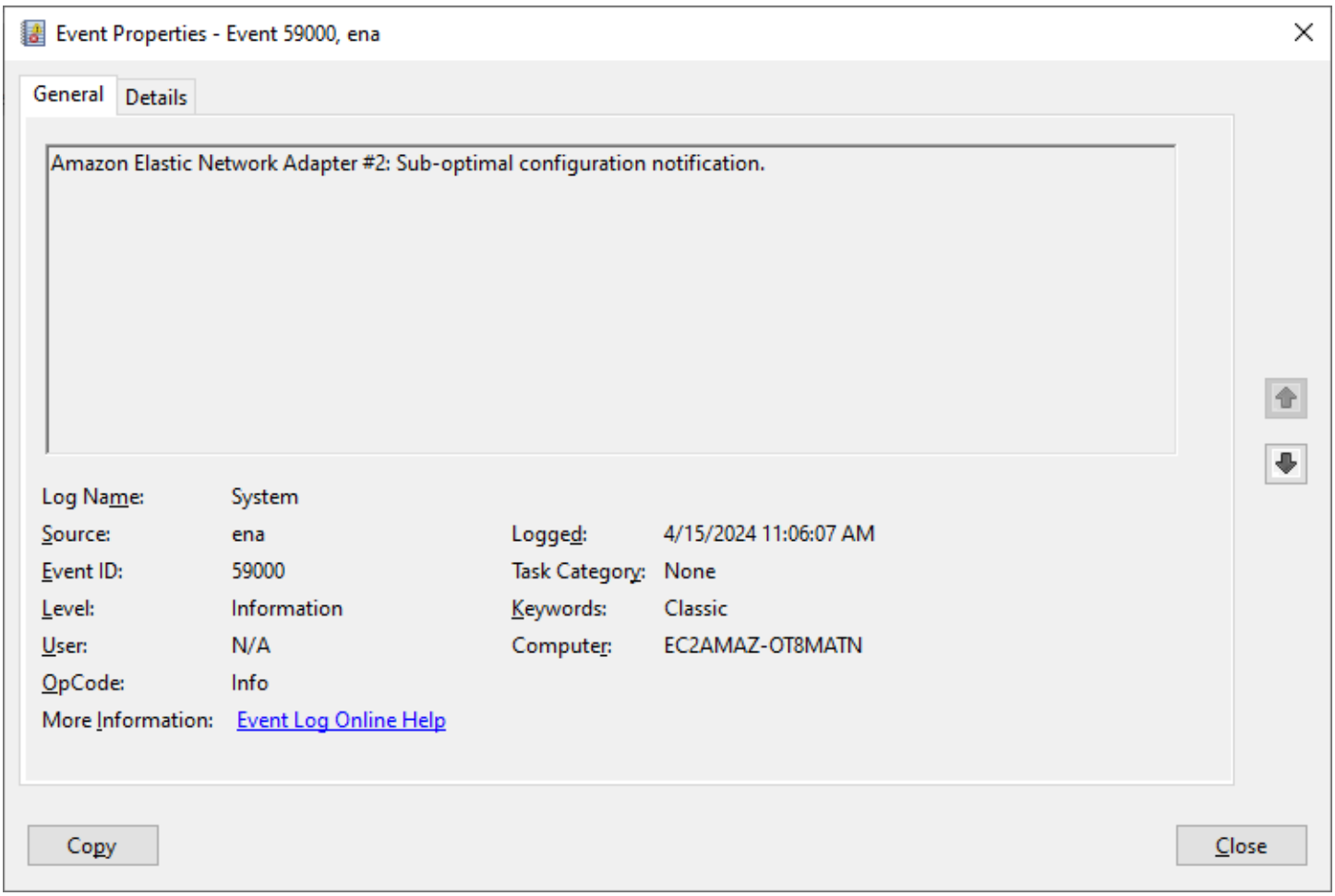
Analizzare le notifiche di configurazione non ottimali

Il dispositivo ENA rileva le impostazioni di configurazione non ottimali nel driver che è possibile modificare. Il dispositivo notifica il driver ENA e registra una notifica di evento. Esaminare gli eventi non ottimali in Visualizzatore eventi di Windows

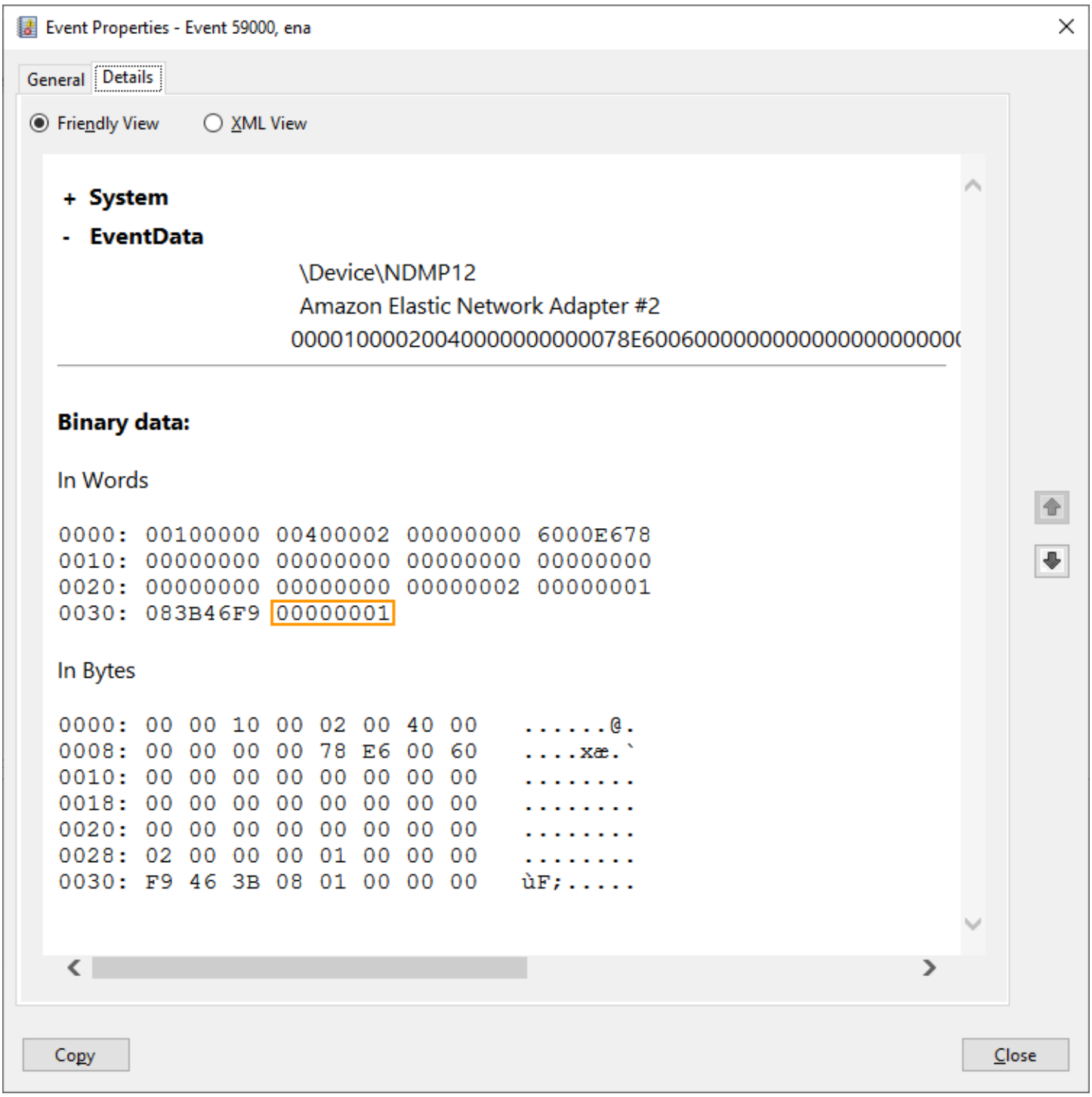
1. Aprire la finestra di dialogo Esegui utilizzando uno dei metodi descritti nella sezione precedente.
2. Per aprire Visualizzatore eventi in Windows, inserire `eventvwr.msc` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra del Visualizzatore eventi di Windows.
4. Espandere il menu Eventi di Windows, quindi scegliere Sistema.
5. In Operazioni, nel pannello in alto a destra, scegliere Filtra log corrente. Viene visualizzata la finestra di dialogo di filtro.
6. Nel campo Origine eventi, inserire `ena`. Ciò limita i risultati agli eventi generati dal driver ENA per Windows.

7. Scegli OK. Ciò mostra i risultati del log degli eventi filtrati nelle sezioni di dettaglio della finestra.

Gli eventi con ID `59000` notificano all'utente esiti di configurazione non ottimali. Apri il menu contestuale (clic con il pulsante destro del mouse) per un evento e scegli Proprietà dell'evento per aprire una vista dettagliata, oppure seleziona Riquadro di anteprima dal menu Visualizza per visualizzare lo stesso dettaglio.



Aprire la scheda Dettagli per visualizzare il codice dell'evento. Nella sezione Dati binari: in parole, l'ultima parola è il codice.



L'elenco seguente mostra i dettagli del codice di notifica e le operazioni consigliate per gli esiti di configurazione non ottimali.

- Codice **1**: non è consigliato utilizzare ENA Express con la configurazione LLQ estesa

ENA Express ENI è configurato con LLQ esteso. Questa configurazione non è ottimale e potrebbe influire sulle prestazioni di ENA Express. Si consiglia di disabilitare le impostazioni LLQ estese quando si utilizzano ENI ENA Express, come indicato di seguito.

1. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.
2. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
3. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
4. Aprire le proprietà del dispositivo per `Amazon Elastic Network Adapter`.
5. Per apportare le modifiche, aprire la scheda Avanzate.
6. Selezionare la proprietà Policy relativa alla dimensione dell'intestazione LLQ e impostare il valore su `Normal (128 Bytes)`.
7. Scegliere OK per salvare le modifiche.

- Codice **2**: ENI ENA Express con una profondità di coda Tx non ottimale non è consigliato

  ENI ENA Express è configurato con una profondità di coda Tx non ottimale. Questa configurazione potrebbe influire sulle prestazioni di ENA Express. Si consiglia di estendere tutte le code Tx al valore massimo per l'interfaccia di rete quando si utilizzano ENI ENA Express, come indicato di seguito.

  Attenersi alla seguente procedura per estendere le code Tx alla profondità massima:

  1. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.
  2. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
  3. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
  4. Aprire le proprietà del dispositivo per `Amazon Elastic Network Adapter`.
  5. Per apportare le modifiche, aprire la scheda Avanzate.
  6. Selezionare la proprietà Trasmetti Buffer e impostarne il valore sul valore massimo supportato.
  7. Scegliere OK per salvare le modifiche.

Ripristino dell'adattatore ENA

Il processo di ripristino viene avviato quando il driver ENA per Windows rileva un errore su una scheda di rete e contrassegna l'adattatore come non integro. Il driver non può ripristinarsi da solo, quindi dipende dal sistema operativo controllare lo stato di integrità dell'adattatore e invocare il gestore di ripristino per il driver ENA per Windows. Il processo di ripristino potrebbe comportare

un breve periodo di tempo in cui si verifica una perdita di traffico. Tuttavia, le connessioni TCP dovrebbero essere in grado di essere ripristinate.

L'adattatore ENA potrebbe anche richiedere indirettamente una procedura di ripristino del dispositivo, in caso di mancato invio di una notifica keep-alive. Ad esempio, se l'adattatore ENA raggiunge uno stato non riconosciuto dopo aver caricato una configurazione non ripristinabile, potrebbe interrompere l'invio di notifiche keep-alive.

Cause comuni del ripristino dell'adattatore ENA

- Keep-alive mancano i messaggi

  L'adattatore ENA segnala gli eventi keep-alive con una frequenza fissa (di solito una volta al secondo). Il driver ENA per Windows è dotato di un meccanismo watchdog che controlla periodicamente la presenza di questi messaggi keep-alive. Se uno o più nuovi messaggi vengono rilevati dall'ultima volta in cui sono stati controllati, registra un risultato positivo. In caso contrario, il driver conclude che il dispositivo ha riscontrato un utilizzo fuori limite e avvia una sequenza di ripristino.
- Pacchetti bloccati nelle code di trasmissione

  L'adattatore ENA verifica che i pacchetti scorrano attraverso le code di trasmissione come previsto. Il driver ENA per Windows rileva se i pacchetti si bloccano e avvia una sequenza di ripristino, nel caso in cui questo si verifichi.
- Timeout di lettura per i registri Memory Mapped I/O (MMIO)

  Per limitare le operazioni di lettura MMIO I/O (Memory Mapped), il driver ENA Windows accede ai registri MMIO solo durante i processi di inizializzazione e ripristino. Se il driver rileva un timeout, richiede una delle seguenti azioni, a seconda del processo in esecuzione:

  - Se viene rilevato un timeout durante l'inizializzazione, il flusso viene interrotto, il che comporta la visualizzazione di un punto esclamativo giallo accanto all'adattatore ENA in Gestione dispositivi di Windows.
  - Se viene rilevato un timeout durante il ripristino, il flusso viene interrotto. Il sistema operativo avvia quindi una rimozione inaspettata dell'adattatore ENA e lo ripristina arrestando e avviando l'adattatore che è stato rimosso. Per ulteriori informazioni sulla rimozione inaspettata di una scheda di interfaccia di rete (NIC), consultare Gestione della rimozione inaspettata di una NIC nella documentazione Sviluppatore hardware di Microsoft Windows.

Scenari per la risoluzione dei problemi

Gli scenari seguenti possono essere utili per risolvere i problemi che possono verificarsi con il driver ENA per Windows. Si consiglia di iniziare con l'aggiornamento del driver ENA, se non si dispone della versione più recente. Per trovare il driver più recente per la versione del sistema operativo Windows, consultare Traccia rilasci della versione del driver ENA Windows.

Versione del driver ENA installata non prevista

Description

Dopo aver eseguito i passaggi per installare una versione specifica del driver ENA, Windows Device Manager mostra che Windows ha installato una versione diversa del driver ENA.

Causa

Quando si esegue l'installazione di un pacchetto driver, Windows classifica tutti i pacchetti driver validi per il dispositivo specificato nel Archivio driver locale prima di iniziare. Quindi seleziona il pacchetto con il valore più basso come migliore abbinamento. Può essere diverso dal pacchetto che intendevi installare. Per ulteriori informazioni sul processo di selezione dei pacchetti driver del dispositivo, consulta Modalità con cui Windows seleziona un pacchetto driver per un dispositivo nel sito web della documentazione Microsoft.

Soluzione

Per assicurarti che Windows installi la versione del pacchetto driver scelta, puoi rimuovere i pacchetti driver di livello inferiore dall'Archivio driver con lo strumento da riga di comando PNPUtil.

Segui questi passaggi per aggiornare il driver ENA:

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. Aprire la finestra delle proprietà Gestione dispositivi, come descritto nella sezione Controllo dello stato del dispositivo ENA. In questo modo si apre la scheda Generale della finestra Proprietà di Amazon Elastic Network Adapter.
3. Apertura della scheda Driver.
4. Scegliere Update Driver (Aggiorna driver). Si apre la finestra di dialogo Aggiornamento del software del driver — Amazon Elastic Network Adapter.

    a. Nella pagina Modalità di ricerca software driver?, scegli Cerca driver nel computer.

b. Nella pagina Cerca il software dei driver sul computer, scegli Fammi scegliere da un elenco di driver di periferica sul mio computer, situato sotto la barra di ricerca.

c. Nella pagina Seleziona il driver del dispositivo che desideri installare per questo hardware, scegli Disco... .

d. Nella finestra Installa da disco, scegli Cerca... , accanto alla posizione di file dall'elenco discesa

e. Accedere alla posizione in cui è stato scaricato il pacchetto driver ENA di destinazione. Scegli il file `ena.inf` e seleziona Apri.

f. Per avviare l'installazione, scegli OK, quindi scegli Avanti.

5. Se il programma di installazione non riavvia automaticamente l'istanza, esegui il cmdlet. Restart-Computer PowerShell

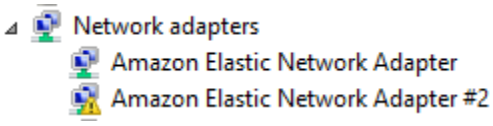
```
PS C:\> Restart-Computer
```

Avviso dispositivo per driver ENA

Description

L'icona dell'adattatore ENA in Gestione dispositivi nella sezione Schede di rete visualizza un segnale di avviso (un triangolo giallo con un punto esclamativo all'interno).

L'esempio seguente mostra un adattatore ENA con l'icona di avviso in Gestione dispositivi di Windows:



Causa

Questo avviso del dispositivo è comunemente causato da problemi di ambiente, che potrebbero richiedere ulteriori ricerche e spesso richiedono un procedimento per esclusione per determinare la causa sottostante. Per un elenco completo degli errori del dispositivo, consulta Device Manager Error Messages nella documentazione Microsoft.

Soluzione

La soluzione per questo avviso del dispositivo dipende dalla causa principale. Il procedimento per esclusione qui descritto include alcuni passaggi fondamentali per aiutare a identificare e risolvere i

problemi più comuni che potrebbero avere una soluzione semplice. Un'ulteriore analisi della causa principale è necessaria quando questi passaggi non risolvono il problema.

Seguire questi passaggi per identificare e risolvere i problemi più comuni:

1. Avviare e arrestare il dispositivo

   Aprire la finestra delle proprietà Gestione dispositivi, come descritto nella sezione Controllo dello stato del dispositivo ENA. In questo modo si apre la scheda Generale della finestra Proprietà di Amazon Elastic Network Adapter, dove lo Stato del dispositivo visualizza il codice di errore e un breve messaggio.

   a. Apertura della scheda Driver.
   b. Scegliere Disabilitare il dispositivo e selezionare Sì al messaggio di avviso visualizzato.
   c. Scegliere Abilitare dispositivo.

2. Arrestare e avviare l'istanza EC2

   Se l'adattatore mostra ancora l'icona di avviso in Gestione dispositivi, il passo successivo consiste nell'arrestare e avviare l'istanza EC2. Questo passo rilancia l'istanza su un hardware diverso nella maggior parte dei casi.

3. Indagare il possibile problema delle risorse dell'istanza

   Se l'istanza EC2 si è interrotta e avviata e il problema persiste, potrebbe indicare un problema di risorse sull'istanza, ad esempio memoria insufficiente.

Timeout di connessione con ripristino dell'adattatore (codici di errore 5007, 5205)

Description

Il visualizzatore eventi di Windows mostra il timeout dell'adattatore e gli eventi di ripristino verificati in combinazione per gli adattatori ENA. I messaggi sono simili ai seguenti esempi:

- ID evento 5007: Adattatore Amazon Elastic Network: timeout scaduto durante un'operazione.
- ID evento 5205: Adattatore Amazon Elastic Network: il ripristino dell'adattatore è stato avviato.

I ripristini dell'adattatore causano un'interruzione minima del traffico. Anche quando ci sono più ripristini, sarebbe insolito causare gravi interruzioni della rete.

Causa

Questa sequenza di eventi indica che il driver ENA per Windows ha avviato un ripristino per una scheda ENA che non rispondeva. Tuttavia, il meccanismo utilizzato dal driver del dispositivo per rilevare questo problema è soggetto a falsi positivi derivanti dalla starvation della CPU 0.

Soluzione

Se questa combinazione di errori si verifica frequentemente, controllare le allocazioni delle risorse per vedere dove potrebbero essere utile effettuare degli aggiustamenti.

1. Aprire la finestra di dialogo Esegui utilizzando uno dei metodi descritti nella sezione precedente.
2. Per aprire il Resource Monitor di Windows, inserire `resmon` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra di Resource Monitor.
4. Aprire la scheda CPU. Per-CPU i grafici di utilizzo sono mostrati lungo il lato destro della finestra Resource Monitor.
5. Controllare i livelli di utilizzo della CPU 0 per vedere se sono troppo alti.

Si consiglia di configurare RSS per escludere la CPU 0 per l'adattatore ENA su tipi di istanza più grandi (più di 16 vCPU). Per i tipi di istanza più piccoli, la configurazione di RSS potrebbe migliorare l'esperienza, ma a causa del minor numero di core disponibili, è necessario eseguire test per garantire che il vincolo dei core della CPU non influisca negativamente sulle prestazioni.

Utilizzare il comando Set-NetAdapterRss per configurare RSS per l'adattatore ENA, come illustrato nell'esempio seguente.

```
Set-NetAdapterRss -name (Get-NetAdapter | Where-Object {$_.InterfaceDescription -like
 "*Elastic*"}).Name -Baseprocessorgroup 0 -BaseProcessorNumber 1
```

La migrazione a un'infrastruttura di istanza di sesta generazione influisce sulle prestazioni o sull'allegato

Description

Se si esegue la migrazione a un'istanza EC2 di sesta generazione, è possibile che si verifichino prestazioni ridotte o errori degli allegati ENA nel caso in cui la versione del driver ENA per Windows non sia stata aggiornata.

Causa

I tipi di istanze EC2 di sesta generazione richiedono la seguente versione minima del driver ENA Windows, basata sul sistema operativo (SO) dell'istanza.

Versione minima

Versione di Windows Server	Versione driver ENA
Windows Server 2008 R2	2.2.3 o 2.4.0
Windows Server 2012 e versioni successive	Versione 2.2.3 e successive
Workstation Windows	Versione 2.2.3 e successive

Soluzione

Prima di eseguire l'aggiornamento a un'istanza EC2 di sesta generazione, assicurati che l'AMI da cui esegui l'avvio disponga di driver compatibili basati sul sistema operativo dell'istanza, come mostrato nella tabella precedente. Per ulteriori informazioni, consulta l'articolo Cosa devo fare prima di eseguire la migrazione della mia istanza EC2 a un'istanza di sesta generazione per assicurarmi di ottenere le massime prestazioni di rete? nel Knowledge Center di AWS re:Post .

Prestazioni non ottimali per l'interfaccia di rete elastica (ENI)

Description

L'interfaccia ENA non funziona come previsto.

Causa

L'analisi della causa principale per i problemi di prestazioni è un procedimento per esclusione. Ci sono troppe variabili coinvolte per identificare una causa comune.

Soluzione

Il primo passo nell'analisi della causa principale consiste nell'esaminare le informazioni diagnostiche per l'istanza che non funziona come previsto, per determinare se ci sono errori che potrebbero

causare il problema. Per ulteriori informazioni, consulta la sezione Raccogliere informazioni diagnostiche sull'istanza.

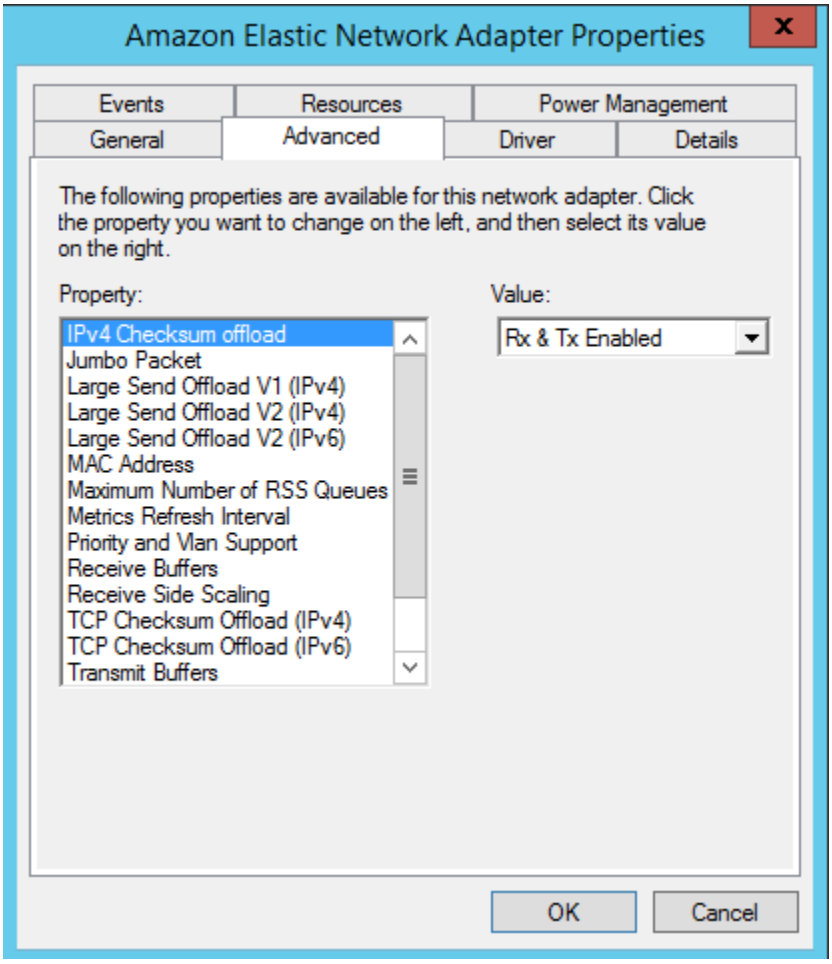
Per ottenere le massime prestazioni di rete sulle istanze con reti avanzate, potrebbe essere necessario modificare la configurazione del sistema operativo predefinita. Alcune ottimizzazioni (come ad esempio l'attivazione dell'offload del checksum e l'abilitazione di RSS) sono configurate sulle AMI ufficiali di Windows per impostazione predefinita. Per altre ottimizzazioni che è possibile applicare all'adattatore ENA, vedere le regolazioni delle prestazioni mostrate in Regolazione delle prestazioni dell'adattatore ENA.

Ti consigliamo di procedere con cautela e di limitare le modifiche alle proprietà del dispositivo a quelle elencate in questa sezione o alle modifiche specifiche consigliate dal team di AWS supporto.

Per modificare le proprietà dell'adattatore ENA, attenersi alla seguente procedura:

1. Aprire la finestra di dialogo Esegui utilizzando uno dei metodi descritti nella sezione precedente.
2. Per aprire Gestione dispositivi in Windows, inserire `devmgmt.msc` nel campo Esegui.
3. Scegli OK. Viene visualizzata la finestra Gestione dispositivi.
4. Selezionare la freccia visualizzata a sinistra di Schede di rete per espandere l'elenco.
5. Scegliere il nome o aprire il menu contestuale per Adattatore elastico di rete Amazon e quindi Proprietà. In questo modo si apre la finestra di dialogo Proprietà di Amazon Elastic Network Adapter.
6. Per apportare le modifiche, apri la scheda Avanzate.
7. Al termine, scegli OK per salvare le modifiche.

L'esempio seguente mostra una proprietà dell'adattatore ENA in Gestione dispositivi di Windows:



Regolazione delle prestazioni dell'adattatore ENA

La tabella seguente include le proprietà che possono essere regolate per migliorare le prestazioni dell'interfaccia ENA.

Input

Proprietà	Description	Valore predefinito	Regolazione
Buffer di ricezione	Controlla il numero di voci nelle code di ricezione del software.	1.024	Questa quota può essere aumentata fino a un massimo di 8192.
Receive Side Scaling (RSS)	Consente la distribuzione efficiente	Abilitato	È possibile distribuire il carico su più

Proprietà	Description	Valore predefinito	Regolazione
	dell'elaborazione della ricezione di rete su più CPU nei sistemi multiprocessore.		processori. Per ulteriori informazioni, consulta Ottimizza le prestazioni di rete sulle istanze Windows EC2.

Proprietà	Description	Valore predefinito	Regolazione
Numero massimo di code RSS	Imposta il numero massimo di code RSS consentite quando RSS è abilitato.	32	Il numero di code RSS viene determinato durante l'inizializzazione del driver e include, tra le altre, le seguenti limitazioni: • Limite di coda RSS impostato da questa proprietà • Limiti di istanza (numero vCPU) • Limiti di generazione hardware (fino a 8 code RSS in ENAv1 e fino a 32 code RSS in ENAv2) È possibile impostare il valore da 1 a 32, a seconda dei limiti di generazione dell'istanza e dell'hardware. Per ulteriori informazioni, consulta Ottimizza le prestazioni di rete sulle istanze Windows EC2.

Proprietà	Description	Valore predefinito	Regolazione
Pacchetti Jumbo	Consente l'utilizzo di frame jumbo ethernet (oltre 1500 byte di payload).	Disabilitato (questo limita il payload a 1500 byte o meno)	Il valore può essere impostato su `9015`, che si traduce in 9001 byte di payload. Questo è il payload massimo per i frame jumbo ethernet. Per informazioni, consulta Considerazioni sull'utilizzo dei frame jumbo ethernet.

Considerazioni sull'utilizzo dei frame jumbo ethernet

I frame jumbo consentono più di 1500 byte di dati aumentando la dimensione di payload per pacchetto, aumentando quindi la percentuale del pacchetto che non suppone un sovraccarico del pacchetto. È quindi necessario un numero minore di pacchetti per inviare la stessa quantità di dati utilizzabili. Tuttavia, il traffico è limitato a un MTU massimo di 1500 nei seguenti casi:

- Traffico al di fuori di una determinata AWS regione per EC2 Classic.
- Traffico esterno a un singolo VPC.
- Traffico su una connessione di peering VPC tra regioni.
- Traffico su connessioni VPN.
- Traffico su un gateway Internet.

> **Note**
>
> I pacchetti superiori a 1500 byte sono frammentati. Se hai flag `Don't Fragment` è impostato nell'intestazione IP, questi pacchetti vengono eliminati.
> I frame jumbo devono essere utilizzati con cautela per il traffico vincolato a Internet o qualsiasi traffico che esca da un VPC. I pacchetti vengono frammentati da sistemi intermedi, i quali rallentano tale traffico. Per utilizzare i frame jumbo all'interno di un VPC senza influire sul traffico in uscita dal VPC, provare una delle seguenti opzioni:

- Configurare la dimensione MTU per routing.
- Puoi usare più interfacce di rete con dimensioni MTU diverse e instradamenti diversi.

Casi d'uso consigliati per frame jumbo

I frame jumbo possono essere utili per il traffico all'interno e tra i VPC. Si consiglia di utilizzare i frame jumbo per i seguenti casi d'uso:

- Per le istanze collocate in un gruppo di posizionamento cluster, i frame jumbo aiutano a raggiungere il massimo throughput della rete possibile. Per ulteriori informazioni, consulta Gruppi di collocamento per le tue istanze Amazon EC2.
- È possibile utilizzare i frame jumbo per il traffico tra i VPC e le proprie reti on-premises su Direct Connect. Per ulteriori informazioni sull'utilizzo Direct Connect e sulla verifica della funzionalità dei jumbo frame, vedere MTU per interfacce virtuali private o interfacce virtuali di transito nella Guida per l'utente. Direct Connect
- Per ulteriori informazioni sulle dimensioni MTU supportate per i Transit Gateway, consultare Quote per Transit Gateway in Amazon VPC Transit Gateway.

Migliora le prestazioni di rete tra le istanze EC2 con ENA Express

ENA Express è alimentato dalla tecnologia AWS Scalable Reliable Datagram (SRD). SRD è un protocollo di trasporto di rete ad alte prestazioni che utilizza l'instradamento dinamico per aumentare il throughput e ridurre al minimo la latenza di coda. Con ENA Express, è possibile comunicare tra due istanze EC2 nella stessa zona di disponibilità o tra zone di disponibilità all'interno della stessa regione.

Vantaggi di ENA Express

- Aumenta la larghezza di banda massima che un singolo flusso può utilizzare da 5 Gbps a 25 Gbps all'interno della stessa regione, fino al limite aggregato delle istanze.
- Riduce la latenza di coda del traffico di rete tra le istanze EC2 nella stessa zona di disponibilità, specialmente durante i periodi di elevato carico di rete.
- Rileva ed evita i percorsi di rete congestionati.

- Gestisce alcune attività direttamente a livello di rete, come il riordino dei pacchetti sul lato di ricezione e la maggior parte delle ritrasmissioni necessarie. Questo libera il livello dell'applicazione per altre attività.

> **Note**
>
> - Se la tua applicazione ha requisiti elevati di pacchetti al secondo e deve ottimizzare la latenza durante i periodi di non congestionamento, potrebbe essere la soluzione più adatta. Reti avanzate
> - Il traffico di ENA Express non può essere inviato in una zona locale.
> - Il supporto ENA Express per il traffico tra le zone di disponibilità non è disponibile in Sud America (San Paolo), Medio Oriente (Bahrain) e Medio Oriente (Emirati Arabi Uniti).

Dopo aver abilitato ENA Express per il collegamento dell'interfaccia di rete su un'istanza, l'istanza di invio avvia la comunicazione con l'istanza di ricezione e SRD rileva se ENA Express è in funzione sia sull'istanza di invio sia sull'istanza di ricezione. Se ENA Express è in funzione, la comunicazione può utilizzare la trasmissione SRD. Se ENA Express non è in funzione, la comunicazione torna alla trasmissione ENA standard.

Nei periodi di tempo in cui il traffico di rete è scarso, è possibile notare un leggero aumento della latenza media dei pacchetti (decine di microsecondi) quando il pacchetto utilizza ENA Express. In questi periodi, le applicazioni che danno priorità a specifiche caratteristiche prestazionali di rete possono trarre vantaggio da ENA Express come segue:

- I processi possono trarre vantaggio dall'aumento della larghezza di banda massima a flusso singolo da 5 Gbps a 25 Gbps all'interno della stessa regione, fino al limite di istanze aggregate. Ad esempio, se un tipo di istanza specifico supporta fino a 12,5 Gbps, anche la larghezza di banda a flusso singolo è limitata a 12,5 Gbps.
- I processi in esecuzione più lunghi nella stessa zona di disponibilità subiranno una latenza di coda ridotta durante i periodi di congestione della rete.
- I processi possono trarre vantaggio da una distribuzione più fluida e standard per i tempi di risposta della rete.

Argomenti

- Come funziona ENA Express
- Tipi di istanza supportati per ENA Express
- Ottimizza le prestazioni per le impostazioni ENA Express su istanze Linux
- Rivedi le impostazioni di ENA Express per la tua istanza EC2
- Configura le impostazioni di ENA Express per la tua istanza EC2

Come funziona ENA Express

ENA Express è basato sulla tecnologia AWS Scalable Reliable Datagram (SRD). Distribuisce i pacchetti per ogni flusso di rete su diversi percorsi di AWS rete e regola dinamicamente la distribuzione quando rileva segni di congestione. Gestisce anche il riordino dei pacchetti sul lato di ricezione.

Per garantire che ENA Express sia in grado di gestire il traffico di rete come previsto, le istanze di invio e ricezione e la comunicazione tra di esse devono soddisfare tutti i seguenti requisiti:

- Sono supportati i tipi sia delle istanze di invio sia di quelle di ricezione. Per ulteriori informazioni, consulta la tabella Tipi di istanza supportati per ENA Express.
- Sia le istanze di invio sia quelle di ricezione devono avere ENA Express configurato. Se esistono differenze nella configurazione, si possono verificare situazioni in cui il traffico è impostato automaticamente sulla trasmissione ENA standard. Lo scenario seguente mostra ciò che accade in questo caso.

  Scenario: differenze nella configurazione

Istanza	ENA Express abilitato	UDP utilizza ENA Express
Istanza 1	Sì	Sì
Istanza 2	Sì	No

  In questo caso, il traffico TCP tra le due istanze può utilizzare ENA Express, poiché è abilitato su entrambe le istanze. Tuttavia, poiché una delle istanze non utilizza ENA Express per il traffico UDP, la comunicazione tra queste due istanze tramite UDP utilizza la trasmissione ENA standard.
- Le istanze di invio e ricezione devono essere eseguite nella stessa regione.

- Il percorso di rete tra le istanze non deve includere box middleware (software intermediario). ENA Express attualmente non supporta i box middleware (software intermediario).
- (Solo istanze Linux) Per utilizzare tutto il potenziale della larghezza di banda, utilizza la versione 2.2.9 o successiva del driver.
- (Solo istanze Linux) Per produrre parametri, utilizza la versione 2.8 o successiva del driver.

Se un requisito non è soddisfatto, le istanze utilizzano il TCP/UDP protocollo standard ma senza SRD per comunicare.

Per assicurarti che il driver di rete dell'istanza sia configurato per prestazioni ottimali, consulta le best practice consigliate per i driver ENA. Queste best practice si applicano anche a ENA Express. Per ulteriori informazioni, consultate la guida ENA Linux Driver Best Practices and Performance Optimization Guide sul sito Web. GitHub

> **Note**
>
> Per Amazon EC2, una relazione tra un'istanza e un'interfaccia di rete a essa collegata è un collegamento. Le impostazioni di ENA Express si applicano al collegamento. Se l'interfaccia di rete è scollegata dall'istanza, il collegamento non esiste più e le impostazioni di ENA Express ad esso applicate non sono più valide. Lo stesso vale quando un'istanza viene terminata, anche se l'interfaccia di rete rimane.

Dopo avere abilitato ENA Express per i collegamenti dell'interfaccia di rete sia sull'istanza di invio sia sull'istanza di ricezione, è possibile utilizzare i parametri di ENA Express per garantire che le istanze traggano il massimo vantaggio dai miglioramenti delle prestazioni offerti dalla tecnologia SRD. Per ulteriori informazioni sui parametri di ENA Express, consulta la pagina Parametri di ENA Express.

Tipi di istanza supportati per ENA Express

I seguenti tipi di istanza supportano ENA Express.

General purpose

Tipo di istanza	Architecture
`m6a.12xlarge`	x86_64

Tipo di istanza	Architecture
m6a.16xlarge	x86_64
m6a.24xlarge	x86_64
m6a.32xlarge	x86_64
m6a.48xlarge	x86_64
m6a.metal	x86_64
m6i.8xlarge	x86_64
m6i.12xlarge	x86_64
m6i.16xlarge	x86_64
m6i.24xlarge	x86_64
m6i.32xlarge	x86_64
m6i.metal	x86_64
m6id.8xlarge	x86_64
m6id.12xlarge	x86_64
m6id.16xlarge	x86_64
m6id.24xlarge	x86_64
m6id.32xlarge	x86_64
m6id.metal	x86_64
m6idn.8xlarge	x86_64
m6idn.12xlarge	x86_64
m6idn.16xlarge	x86_64

Tipo di istanza	Architecture
m6idn.24xlarge	x86_64
m6idn.32xlarge	x86_64
m6idn.metal	x86_64
m6in.8xlarge	x86_64
m6in.12xlarge	x86_64
m6in.16xlarge	x86_64
m6in.24xlarge	x86_64
m6in.32xlarge	x86_64
m6in.metal	x86_64
m7a.12xlarge	x86_64
m7a.16xlarge	x86_64
m7a.24xlarge	x86_64
m7a.32xlarge	x86_64
m7a.48xlarge	x86_64
m7a.metal-48xl	x86_64
m7g.12xlarge	arm64
m7g.16xlarge	arm64
m7g.metal	arm64
m7gd.12xlarge	arm64
m7gd.16xlarge	arm64

Tipo di istanza	Architecture
m7gd.metal	arm64
m7i.12xlarge	x86_64
m7i.16xlarge	x86_64
m7i.24xlarge	x86_64
m7i.48xlarge	x86_64
m7i.metal-24xl	x86_64
m7i.metal-48xl	x86_64
m8a.16xlarge	x86_64
m8a.24xlarge	x86_64
m8a.48xlarge	x86_64
m8a.metal-24xl	x86_64
m8a.metal-48xl	x86_64
m8azn.12xlarge	x86_64
m8azn.24xlarge	x86_64
m8azn.metal-12xl	x86_64
m8azn.metal-24xl	x86_64
m8g.8xlarge	arm64
m8g.12xlarge	arm64
m8g.16xlarge	arm64
m8g.24xlarge	arm64

Tipo di istanza	Architecture
m8g.48xlarge	arm64
m8g.metal-24xl	arm64
m8g.metal-48xl	arm64
m8gb.4xlarge	arm64
m8gb.8xlarge	arm64
m8gb.12xlarge	arm64
m8gb.16xlarge	arm64
m8gb.24xlarge	arm64
m8gb.48xlarge	arm64
m8gb.metal-24xl	arm64
m8gb.metal-48xl	arm64
m8gd.8xlarge	arm64
m8gd.12xlarge	arm64
m8gd.16xlarge	arm64
m8gd.24xlarge	arm64
m8gd.48xlarge	arm64
m8gd.metal-24xl	arm64
m8gd.metal-48xl	arm64
m8gn.4xlarge	arm64
m8gn.8xlarge	arm64

Tipo di istanza	Architecture
m8gn.12xlarge	arm64
m8gn.16xlarge	arm64
m8gn.24xlarge	arm64
m8gn.48xlarge	arm64
m8gn.metal-24xl	arm64
m8gn.metal-48xl	arm64
m8i.8xlarge	x86_64
m8i.12xlarge	x86_64
m8i.16xlarge	x86_64
m8i.24xlarge	x86_64
m8i.32xlarge	x86_64
m8i.48xlarge	x86_64
m8i.96xlarge	x86_64
m8i.metal-48xl	x86_64
m8i.metal-96xl	x86_64
m8id.8xlarge	x86_64
m8id.12xlarge	x86_64
m8id.16xlarge	x86_64
m8id.24xlarge	x86_64
m8id.32xlarge	x86_64

Tipo di istanza	Architecture
m8id.48xlarge	x86_64
m8id.96xlarge	x86_64
m8id.metal-48xl	x86_64
m8id.metal-96xl	x86_64
m8in.8xlarge	x86_64
m8in.12xlarge	x86_64
m8in.16xlarge	x86_64
m8in.24xlarge	x86_64
m8in.32xlarge	x86_64
m8in.48xlarge	x86_64
m8in.96xlarge	x86_64
m8in.metal-48xl	x86_64
m8in.metal-96xl	x86_64
m8idn.8xlarge	x86_64
m8idn.12xlarge	x86_64
m8idn.16xlarge	x86_64
m8idn.24xlarge	x86_64
m8idn.32xlarge	x86_64
m8idn.48xlarge	x86_64
m8idn.96xlarge	x86_64

Tipo di istanza	Architecture
m8idn.metal-48xl	x86_64
m8idn.metal-96xl	x86_64
m8ib.8xlarge	x86_64
m8ib.12xlarge	x86_64
m8ib.16xlarge	x86_64
m8ib.24xlarge	x86_64
m8ib.32xlarge	x86_64
m8ib.48xlarge	x86_64
m8ib.96xlarge	x86_64
m8ib.metal-48xl	x86_64
m8ib.metal-96xl	x86_64
m8idb.8xlarge	x86_64
m8idb.12xlarge	x86_64
m8idb.16xlarge	x86_64
m8idb.24xlarge	x86_64
m8idb.32xlarge	x86_64
m8idb.48xlarge	x86_64
m8idb.96xlarge	x86_64
m8idb.metal-48xl	x86_64
m8idb.metal-96xl	x86_64

Tipo di istanza	Architecture
m9g.8xlarge	arm64
m9g.12xlarge	arm64
m9g.16xlarge	arm64
m9g.24xlarge	arm64
m9g.48xlarge	arm64
m9g.metal-48xl	arm64
m9gd.8xlarge	arm64
m9gd.12xlarge	arm64
m9gd.16xlarge	arm64
m9gd.24xlarge	arm64
m9gd.48xlarge	arm64
m9gd.metal-48xl	arm64

Compute optimized

Tipo di istanza	Architecture
c6a.12xlarge	x86_64
c6a.16xlarge	x86_64
c6a.24xlarge	x86_64
c6a.32xlarge	x86_64
c6a.48xlarge	x86_64

Tipo di istanza	Architecture
c6a.metal	x86_64
c6gn.4xlarge	arm64
c6gn.8xlarge	arm64
c6gn.12xlarge	arm64
c6gn.16xlarge	arm64
c6i.8xlarge	x86_64
c6i.12xlarge	x86_64
c6i.16xlarge	x86_64
c6i.24xlarge	x86_64
c6i.32xlarge	x86_64
c6i.metal	x86_64
c6id.8xlarge	x86_64
c6id.12xlarge	x86_64
c6id.16xlarge	x86_64
c6id.24xlarge	x86_64
c6id.32xlarge	x86_64
c6id.metal	x86_64
c6in.8xlarge	x86_64
c6in.12xlarge	x86_64
c6in.16xlarge	x86_64

Tipo di istanza	Architecture
c6in.24xlarge	x86_64
c6in.32xlarge	x86_64
c6in.metal	x86_64
c7a.12xlarge	x86_64
c7a.16xlarge	x86_64
c7a.24xlarge	x86_64
c7a.32xlarge	x86_64
c7a.48xlarge	x86_64
c7a.metal-48xl	x86_64
c7g.12xlarge	arm64
c7g.16xlarge	arm64
c7g.metal	arm64
c7gd.12xlarge	arm64
c7gd.16xlarge	arm64
c7gd.metal	arm64
c7gn.4xlarge	arm64
c7gn.8xlarge	arm64
c7gn.12xlarge	arm64
c7gn.16xlarge	arm64
c7gn.metal	arm64

Tipo di istanza	Architecture
c7i.12xlarge	x86_64
c7i.16xlarge	x86_64
c7i.24xlarge	x86_64
c7i.48xlarge	x86_64
c7i.metal-24xl	x86_64
c7i.metal-48xl	x86_64
c8a.16xlarge	x86_64
c8a.24xlarge	x86_64
c8a.48xlarge	x86_64
c8a.metal-24xl	x86_64
c8a.metal-48xl	x86_64
c8g.8xlarge	arm64
c8g.12xlarge	arm64
c8g.16xlarge	arm64
c8g.24xlarge	arm64
c8g.48xlarge	arm64
c8g.metal-24xl	arm64
c8g.metal-48xl	arm64
c8gb.4xlarge	arm64
c8gb.8xlarge	arm64

Tipo di istanza	Architecture
c8gb.12xlarge	arm64
c8gb.16xlarge	arm64
c8gb.24xlarge	arm64
c8gb.48xlarge	arm64
c8gb.metal-24xl	arm64
c8gb.metal-48xl	arm64
c8gd.8xlarge	arm64
c8gd.12xlarge	arm64
c8gd.16xlarge	arm64
c8gd.24xlarge	arm64
c8gd.48xlarge	arm64
c8gd.metal-24xl	arm64
c8gd.metal-48xl	arm64
c8gn.4xlarge	arm64
c8gn.8xlarge	arm64
c8gn.12xlarge	arm64
c8gn.16xlarge	arm64
c8gn.24xlarge	arm64
c8gn.48xlarge	arm64
c8gn.metal-24xl	arm64

Tipo di istanza	Architecture
c8gn.metal-48xl	arm64
c8i.8xlarge	x86_64
c8i.12xlarge	x86_64
c8i.16xlarge	x86_64
c8i.24xlarge	x86_64
c8i.32xlarge	x86_64
c8i.48xlarge	x86_64
c8i.96xlarge	x86_64
c8i.metal-48xl	x86_64
c8i.metal-96xl	x86_64
c8id.8xlarge	x86_64
c8id.12xlarge	x86_64
c8id.16xlarge	x86_64
c8id.24xlarge	x86_64
c8id.32xlarge	x86_64
c8id.48xlarge	x86_64
c8id.96xlarge	x86_64
c8id.metal-48xl	x86_64
c8id.metal-96xl	x86_64
c8in.8xlarge	x86_64

Tipo di istanza	Architecture
c8in.12xlarge	x86_64
c8in.16xlarge	x86_64
c8in.24xlarge	x86_64
c8in.32xlarge	x86_64
c8in.48xlarge	x86_64
c8in.96xlarge	x86_64
c8in.metal-48xl	x86_64
c8in.metal-96xl	x86_64
c8ib.8xlarge	x86_64
c8ib.12xlarge	x86_64
c8ib.16xlarge	x86_64
c8ib.24xlarge	x86_64
c8ib.32xlarge	x86_64
c8ib.48xlarge	x86_64
c8ib.96xlarge	x86_64
c8ib.metal-48xl	x86_64
c8ib.metal-96xl	x86_64
c9g.8xlarge	arm64
c9g.12xlarge	arm64
c9g.16xlarge	arm64

Tipo di istanza	Architecture
c9g.24xlarge	arm64
c9g.48xlarge	arm64
c9g.metal-48xl	arm64
c9gd.8xlarge	arm64
c9gd.12xlarge	arm64
c9gd.16xlarge	arm64
c9gd.24xlarge	arm64
c9gd.48xlarge	arm64
c9gd.metal-48xl	arm64

Memory optimized

Tipo di istanza	Architecture
r6a.12xlarge	x86_64
r6a.16xlarge	x86_64
r6a.24xlarge	x86_64
r6a.32xlarge	x86_64
r6a.48xlarge	x86_64
r6a.metal	x86_64
r6i.8xlarge	x86_64
r6i.12xlarge	x86_64

Tipo di istanza	Architecture
r6i.16xlarge	x86_64
r6i.24xlarge	x86_64
r6i.32xlarge	x86_64
r6i.metal	x86_64
r6id.8xlarge	x86_64
r6id.12xlarge	x86_64
r6id.16xlarge	x86_64
r6id.24xlarge	x86_64
r6id.32xlarge	x86_64
r6id.metal	x86_64
r6idn.8xlarge	x86_64
r6idn.12xlarge	x86_64
r6idn.16xlarge	x86_64
r6idn.24xlarge	x86_64
r6idn.32xlarge	x86_64
r6idn.metal	x86_64
r6in.8xlarge	x86_64
r6in.12xlarge	x86_64
r6in.16xlarge	x86_64
r6in.24xlarge	x86_64

Tipo di istanza	Architecture
r6in.32xlarge	x86_64
r6in.metal	x86_64
r7a.12xlarge	x86_64
r7a.16xlarge	x86_64
r7a.24xlarge	x86_64
r7a.32xlarge	x86_64
r7a.48xlarge	x86_64
r7a.metal-48xl	x86_64
r7g.12xlarge	arm64
r7g.16xlarge	arm64
r7g.metal	arm64
r7gd.12xlarge	arm64
r7gd.16xlarge	arm64
r7gd.metal	arm64
r7i.12xlarge	x86_64
r7i.16xlarge	x86_64
r7i.24xlarge	x86_64
r7i.48xlarge	x86_64
r7i.metal-24xl	x86_64
r7i.metal-48xl	x86_64

Tipo di istanza	Architecture
r7iz.8xlarge	x86_64
r7iz.12xlarge	x86_64
r7iz.16xlarge	x86_64
r7iz.32xlarge	x86_64
r7iz.metal-16xl	x86_64
r7iz.metal-32xl	x86_64
r8a.16xlarge	x86_64
r8a.24xlarge	x86_64
r8a.48xlarge	x86_64
r8a.metal-24xl	x86_64
r8a.metal-48xl	x86_64
r8g.8xlarge	arm64
r8g.12xlarge	arm64
r8g.16xlarge	arm64
r8g.24xlarge	arm64
r8g.48xlarge	arm64
r8g.metal-24xl	arm64
r8g.metal-48xl	arm64
r8gb.4xlarge	arm64
r8gb.8xlarge	arm64

Tipo di istanza	Architecture
r8gb.12xlarge	arm64
r8gb.16xlarge	arm64
r8gb.24xlarge	arm64
r8gb.48xlarge	arm64
r8gb.metal-24xl	arm64
r8gb.metal-48xl	arm64
r8gd.8xlarge	arm64
r8gd.12xlarge	arm64
r8gd.16xlarge	arm64
r8gd.24xlarge	arm64
r8gd.48xlarge	arm64
r8gd.metal-24xl	arm64
r8gd.metal-48xl	arm64
r8gn.4xlarge	arm64
r8gn.8xlarge	arm64
r8gn.12xlarge	arm64
r8gn.16xlarge	arm64
r8gn.24xlarge	arm64
r8gn.48xlarge	arm64
r8gn.metal-24xl	arm64

Tipo di istanza	Architecture
r8gn.metal-48xl	arm64
r8i.8xlarge	x86_64
r8i.12xlarge	x86_64
r8i.16xlarge	x86_64
r8i.24xlarge	x86_64
r8i.32xlarge	x86_64
r8i.48xlarge	x86_64
r8i.96xlarge	x86_64
r8i.metal-48xl	x86_64
r8i.metal-96xl	x86_64
r8id.8xlarge	x86_64
r8id.12xlarge	x86_64
r8id.16xlarge	x86_64
r8id.24xlarge	x86_64
r8id.32xlarge	x86_64
r8id.48xlarge	x86_64
r8id.96xlarge	x86_64
r8id.metal-48xl	x86_64
r8id.metal-96xl	x86_64
r8in.8xlarge	x86_64

Tipo di istanza	Architecture
r8in.12xlarge	x86_64
r8in.16xlarge	x86_64
r8in.24xlarge	x86_64
r8in.32xlarge	x86_64
r8in.48xlarge	x86_64
r8in.96xlarge	x86_64
r8in.metal-48xl	x86_64
r8in.metal-96xl	x86_64
r8idn.8xlarge	x86_64
r8idn.12xlarge	x86_64
r8idn.16xlarge	x86_64
r8idn.24xlarge	x86_64
r8idn.32xlarge	x86_64
r8idn.48xlarge	x86_64
r8idn.96xlarge	x86_64
r8idn.metal-48xl	x86_64
r8idn.metal-96xl	x86_64
r8ib.8xlarge	x86_64
r8ib.12xlarge	x86_64
r8ib.16xlarge	x86_64

Tipo di istanza	Architecture
r8ib.24xlarge	x86_64
r8ib.32xlarge	x86_64
r8ib.48xlarge	x86_64
r8ib.96xlarge	x86_64
r8ib.metal-48xl	x86_64
r8ib.metal-96xl	x86_64
r8idb.8xlarge	x86_64
r8idb.12xlarge	x86_64
r8idb.16xlarge	x86_64
r8idb.24xlarge	x86_64
r8idb.32xlarge	x86_64
r8idb.48xlarge	x86_64
r8idb.96xlarge	x86_64
r8idb.metal-48xl	x86_64
r8idb.metal-96xl	x86_64
r9g.8xlarge	arm64
r9g.12xlarge	arm64
r9g.16xlarge	arm64
r9g.24xlarge	arm64
r9g.48xlarge	arm64

Tipo di istanza	Architecture
r9g.metal-48xl	arm64
r9gd.8xlarge	arm64
r9gd.12xlarge	arm64
r9gd.16xlarge	arm64
r9gd.24xlarge	arm64
r9gd.48xlarge	arm64
r9gd.metal-48xl	arm64
u7i-6tb.112xlarge	x86_64
u7i-8tb.112xlarge	x86_64
u7i-12tb.224xlarge	x86_64
u7in-16tb.224xlarge	x86_64
u7in-24tb.224xlarge	x86_64
u7in-32tb.224xlarge	x86_64
u7inh-32tb.480xlarge	x86_64
x2idn.16xlarge	x86_64
x2idn.24xlarge	x86_64
x2idn.32xlarge	x86_64
x2idn.metal	x86_64
x2iedn.8xlarge	x86_64
x2iedn.16xlarge	x86_64

Tipo di istanza	Architecture
x2iedn.24xlarge	x86_64
x2iedn.32xlarge	x86_64
x2iedn.metal	x86_64
x8g.8xlarge	arm64
x8g.12xlarge	arm64
x8g.16xlarge	arm64
x8g.24xlarge	arm64
x8g.48xlarge	arm64
x8g.metal-24xl	arm64
x8g.metal-48xl	arm64
x8aedz.24xlarge	x86_64
x8aedz.metal-24xl	x86_64
x8i.8xlarge	x86_64
x8i.12xlarge	x86_64
x8i.16xlarge	x86_64
x8i.24xlarge	x86_64
x8i.32xlarge	x86_64
x8i.48xlarge	x86_64
x8i.64xlarge	x86_64
x8i.96xlarge	x86_64

Tipo di istanza	Architecture
x8i.metal-48xl	x86_64
x8i.metal-96xl	x86_64

Accelerated computing

Tipo di istanza	Architecture
g6.48xlarge	x86_64
g6e.12xlarge	x86_64
g6e.24xlarge	x86_64
g6e.48xlarge	x86_64
g7.24xlarge	x86_64
g7.48xlarge	x86_64
g7e.12xlarge	x86_64
g7e.24xlarge	x86_64
g7e.48xlarge	x86_64
p5.4xlarge	x86_64
p5.48xlarge	x86_64
p5e.48xlarge	x86_64
p5en.48xlarge	x86_64
p6-b200.48xlarge	x86_64
p6-b300.48xlarge	x86_64

Tipo di istanza	Architecture
p6e-gb200.36xlarge	arm64

Storage optimized

Tipo di istanza	Architecture
i4g.4xlarge	arm64
i4g.8xlarge	arm64
i4g.16xlarge	arm64
i4i.8xlarge	x86_64
i4i.12xlarge	x86_64
i4i.16xlarge	x86_64
i4i.24xlarge	x86_64
i4i.32xlarge	x86_64
i4i.metal	x86_64
i7i.12xlarge	x86_64
i7i.16xlarge	x86_64
i7i.24xlarge	x86_64
i7i.48xlarge	x86_64
i7i.metal-24xl	x86_64
i7i.metal-48xl	x86_64
i7ie.6xlarge	x86_64

Tipo di istanza	Architecture
i7ie.12xlarge	x86_64
i7ie.18xlarge	x86_64
i7ie.24xlarge	x86_64
i7ie.48xlarge	x86_64
i7ie.metal-24xl	x86_64
i7ie.metal-48xl	x86_64
i8g.8xlarge	arm64
i8g.12xlarge	arm64
i8g.16xlarge	arm64
i8g.24xlarge	arm64
i8g.48xlarge	arm64
i8g.metal-24xl	arm64
i8g.metal-48xl	arm64
i8ge.6xlarge	arm64
i8ge.12xlarge	arm64
i8ge.18xlarge	arm64
i8ge.24xlarge	arm64
i8ge.48xlarge	arm64
i8ge.metal-24xl	arm64
i8ge.metal-48xl	arm64

Tipo di istanza	Architecture
im4gn.4xlarge	arm64
im4gn.8xlarge	arm64
im4gn.16xlarge	arm64

Ottimizza le prestazioni per le impostazioni ENA Express su istanze Linux

Per garantire che ENA Express possa funzionare in modo efficace, l'istanza Linux deve soddisfare diversi requisiti di configurazione di rete.

Anziché configurare ogni impostazione manualmente, puoi scaricare ed eseguire lo script di controllo delle impostazioni ENA Express dal GitHub repository Amazon. Lo script convalida l'istanza rispetto alle impostazioni richieste e consigliate per ENA Express e genera i comandi esatti per risolvere eventuali problemi rilevati.

https://github.com/amzn/amzn-ec2-ena-utilities/blob/main/ena-express/check-ena-express-settings.sh

Lo script controlla le seguenti impostazioni e configurazioni:

- Dimensioni MTU: ENA Express richiede un MTU inferiore a quello predefinito per contenere intestazioni SRD aggiuntive AWS . Le nuove connessioni TCP bloccano automaticamente l'MSS per mitigare questo problema, ma il traffico UDP richiede comunque un MTU inferiore.
- Limite di dimensione della coda di uscita TCP: verifica che il limite di byte in volo per socket sia sufficiente a sostenere un throughput elevato. Gli ambienti con una maggiore latenza di rete richiedono un limite più elevato.
- Limite di coda di byte: conferma che il limite di coda di byte (BQL) è disabilitato sull'interfaccia di rete. BQL può limitare la quantità di dati in coda per la trasmissione a livello di dispositivo, il che limita le prestazioni di ENA Express.

> **Note**
>
> Il driver ENA per la distribuzione Amazon Linux disattiva i limiti delle code di byte per impostazione predefinita.

- TCP autocorking: controlla se l'autocorking TCP è disabilitato. La disattivazione dell'autocorking può ridurre la latenza per determinati modelli di traffico TCP ENA Express, come i carichi di lavoro richiesta-risposta. Ciò potrebbe comportare un aumento minimo del sovraccarico di elaborazione dei pacchetti.
- Dimensione della coda TX e Large LLQ: verifica che la dimensione della coda di trasmissione per l'interfaccia di rete sia sufficientemente grande per prestazioni ottimali. Lo script verifica inoltre se il parametro del modulo ENA disabilita esplicitamente la funzione Large Low Latency Queue (Large LLQ), in quanto può ridurre la profondità della coda TX disponibile. Per ulteriori informazioni su Large LLQ e sul suo impatto sulla dimensione della coda TX, vedere Large Low Latency Queue (Large LLQ) su. https://github.com/amzn/amzn-drivers/tree/master/kernel/linux/ena#large-low-latency-queue-large-llq GitHub
- Dimensione della coda RX: verifica che il buffer ad anello di ricezione per l'interfaccia di rete sia sufficientemente grande da gestire il traffico in entrata in modo efficiente ed evitare perdite di pacchetti sotto carico.
- Dimensioni del buffer TCP e del socket di rete: verifica che le dimensioni massime del buffer di ricezione e di invio TCP, nonché i valori predefiniti e massimi del buffer del socket di rete principale, siano sufficientemente grandi da sostenere un throughput elevato. Queste impostazioni sono importanti in ambienti con una maggiore latenza di rete, in cui sono necessari buffer più grandi per utilizzare la connessione.
- Controllo della congestione TCP: verifica che la configurazione di controllo della congestione TCP sia ottimizzata per l'uso con ENA Express in ambienti con maggiore latenza di rete.

Lo script riporta anche informazioni diagnostiche aggiuntive, tra cui la versione del driver ENA, le statistiche ENA SRD, le impostazioni di moderazione delle interruzioni, la configurazione della coda e le dimensioni del buffer dei socket. Queste informazioni possono essere utili per risolvere i problemi di prestazioni di ENA Express.

Per assicurarti che il driver di rete della tua istanza sia configurato per prestazioni ottimali, consulta anche la Guida alle best practice e all'ottimizzazione delle prestazioni dei driver di ENA Linux suGitHub.

Rivedi le impostazioni di ENA Express per la tua istanza EC2

Puoi verificare le impostazioni di ENA Express per istanza o per interfaccia di rete. Per aggiornare le impostazioni di ENA Express, consulta the section called “Configura impostazioni dell'istanza”.

Console

Per visualizzare le impostazioni di ENA Express per un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione a sinistra, scegli Network interfaces (Interfacce di rete).
3. Seleziona un'interfaccia di rete per visualizzare i dettagli relativi a quell'istanza. Puoi scegliere il collegamento Network interface ID (ID interfaccia di rete) per aprire la pagina dei dettagli oppure puoi selezionare la casella di controllo alla sinistra dell'elenco per visualizzare i dettagli nel riquadro dei dettagli in fondo alla pagina.
4. Nella sezione Collegamento dell'interfaccia di rete della scheda Dettagli o della pagina dei dettagli, rivedi le impostazioni per ENA Express ed ENA Express UDP

Per visualizzare le impostazioni di ENA Express per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Istanze.
3. Seleziona un'istanza per visualizzarne i dettagli. Puoi scegliere il collegamento Instance ID (ID dell'istanza) per aprire la pagina dei dettagli oppure puoi selezionare la casella di controllo alla sinistra dell'elenco per visualizzare i dettagli nel riquadro dei dettagli in fondo alla pagina.
4. Nella sezione Network interfaces (Interfacce di rete) della schedaNetworking (Reti), scorri verso destra per rivedere le impostazioni per ENA Express ed ENA Express UDP.

AWS CLI

Per ottenere le impostazioni di ENA Express per un'istanza

Utilizza il comando describe-instances. Questo esempio di comando restituisce un elenco di configurazioni ENA Express per le interfacce di rete collegate a ciascuna delle istanze in esecuzione specificate dal parametro `--instance-ids`.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7 \
    --query 'Reservations[*].Instances[*].[InstanceId,
 NetworkInterfaces[*].Attachment.EnaSrdSpecification]'
```

Di seguito è riportato un output di esempio.

```
[
    [
        [
            "i-1234567890abcdef0",
            [
                {
                    "EnaSrdEnabled": true,
                    "EnaSrdUdpSpecification": {
                        "EnaSrdUdpEnabled": false
                    }
                }
            ]
        ]
    ],
    [
        [
            "i-0598c7d356eba48d7",
            [
            {
                    "EnaSrdEnabled": true,
                    "EnaSrdUdpSpecification": {
                        "EnaSrdUdpEnabled": false
                    }
                }
            ]
        ]
    ]
]
```

Per ottenere le impostazioni di ENA Express per un'interfaccia di rete

Utilizza il comando describe-network-interfaces.

```
aws ec2 describe-network-interfaces \
    --network-interface-ids eni-1234567890abcdef0 \
    --query NetworkInterfaces[].[NetworkInterfaceId,Attachment.EnaSrdSpecification]
```

Di seguito è riportato un output di esempio.

```
[
    [
        "eni-1234567890abcdef0",
```

```
        {
            "EnaSrdEnabled": true,
            "EnaSrdUdpSpecification": {
                "EnaSrdUdpEnabled": false
            }
        }
    ]
]
```

PowerShell

Per ottenere le impostazioni di ENA Express per un'interfaccia di rete

Utilizza il cmdlet Get-EC2NetworkInterface.

```
Get-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 | `
Select-Object `
    Association,
    NetworkInterfaceId,
    OwnerId,
    @{Name = 'AttachTime'; Expression = { $_.Attachment.AttachTime } },
    @{Name = 'AttachmentId'; Expression = { $_.Attachment.AttachmentId } },
    @{Name = 'DeleteOnTermination'; Expression =
 { $_.Attachment.DeleteOnTermination } },
    @{Name = 'NetworkCardIndex'; Expression = { $_.Attachment.NetworkCardIndex } },
    @{Name = 'InstanceId'; Expression = { $_.Attachment.InstanceId } },
    @{Name = 'InstanceOwnerId'; Expression = { $_.Attachment.InstanceOwnerId } },
    @{Name = 'Status'; Expression = { $_.Attachment.Status } },
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled } },
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled } }
```

Di seguito è riportato un output di esempio.

```
Association         :
NetworkInterfaceId  : eni-0d1234e5f6a78901b
OwnerId             : 111122223333
AttachTime          : 6/11/2022 1:13:11 AM
AttachmentId        : eni-attach-0d1234e5f6a78901b
DeleteOnTermination : True
NetworkCardIndex    : 0
```

```
InstanceId          : i-1234567890abcdef0
InstanceOwnerId     : 111122223333
Status              : attached
EnaSrdEnabled       : True
EnaSrdUdpEnabled    : False
```

Configura le impostazioni di ENA Express per la tua istanza EC2

È possibile configurare ENA Express per i tipi di istanze EC2 supportati senza dover installare alcun software aggiuntivo. Per ulteriori informazioni, consulta the section called "Tipi di istanza supportati per ENA Express".

Console

Per gestire ENA Express per un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione a sinistra, scegli Network interfaces (Interfacce di rete).
3. Seleziona un'interfaccia di rete collegata a un'istanza. Puoi scegliere il collegamento Network interface ID (ID interfaccia di rete) per aprire la pagina dei dettagli oppure puoi selezionare la casella di controllo alla sinistra dell'elenco.
4. Scegli Manage ENA Express (Gestisci ENA Express) dal menu Action (Operazione) in alto a destra della pagina. Si apre la finestra di dialogo Manage ENA Express (Gestisci ENA Express), dove vengono visualizzati l'ID dell'interfaccia di rete selezionata e le impostazioni correnti.

   Se l'interfaccia di rete selezionata non è collegata a un'istanza, questa operazione non viene visualizzata nel menu.
5. Per utilizzare ENA Express, seleziona la casella di spunta Abilita.
6. Quando ENA Express è abilitato, puoi configurare le impostazioni UDP. Per utilizzare ENA Express UDP, seleziona la casella di controllo Abilita.
7. Per salvare le impostazioni, scegli Save (Salva).

Per gestire ENA Express per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Istanze.

3. Seleziona il tipo di istanza che vuoi gestire. Puoi scegliere il collegamento Instance ID (ID dell'istanza) per aprire la pagina dei dettagli oppure puoi selezionare la casella di controllo alla sinistra dell'elenco.
4. Seleziona la Network interface (Interfaccia di rete) da configurare per l'istanza.
5. Scegli Manage ENA Express (Gestisci ENA Express) dal menu Action (Operazione) in alto a destra della pagina.
6. Per configurare ENA Express per un'interfaccia di rete collegata all'istanza, selezionala dall'elenco Network interface (Interfaccia di rete).
7. Per utilizzare ENA Express per il collegamento dell'interfaccia di rete selezionato, seleziona la casella di controllo Abilita.
8. Quando ENA Express è abilitato, puoi configurare le impostazioni UDP. Per utilizzare ENA Express UDP, seleziona la casella di controllo Abilita.
9. Per salvare le impostazioni, scegli Save (Salva).

Per configurare ENA Express durante il collegamento di un'interfaccia di rete

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione a sinistra, scegli Network interfaces (Interfacce di rete).
3. Seleziona un'interfaccia di rete non collegata a un'istanza, dove Status (Stato) è Available (Disponibile). Puoi scegliere il collegamento Network interface ID (ID interfaccia di rete) per aprire la pagina dei dettagli oppure puoi selezionare la casella di controllo alla sinistra dell'elenco.
4. Seleziona l'Instance (Istanza) a cui collegarti.
5. Per utilizzare ENA Express dopo il collegamento dell'interfaccia di rete all'istanza, seleziona la casella di controllo Abilita.
6. Quando ENA Express è abilitato, puoi configurare le impostazioni UDP. Per utilizzare ENA Express UDP, seleziona la casella di controllo Abilita.
7. Per collegare l'interfaccia di rete all'istanza e salvare le impostazioni di ENA Express, scegli Collega.

AWS CLI

Per configurare ENA Express durante il collegamento di un'interfaccia di rete

Utilizza il comando attach-network-interface come visualizzato negli esempi seguenti.

Esempio 1: Utilizza ENA Express per il traffico TCP ma non per il traffico UDP

Questo esempio configura `EnaSrdEnabled` come `true` e consente l'impostazione predefinita di `EnaSrdUdpEnabled` su `false`.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-1234567890abcdef0 \
    --instance-id i-1234567890abcdef0 \
    --device-index 1 \
    --ena-srd-specification 'EnaSrdEnabled=true'
```

Esempio 2: utilizzo di ENA Express sia per il traffico TCP sia per il traffico UDP

Questo esempio configura sia `EnaSrdEnabled` sia `EnaSrdUdpEnabled` come `true`.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-1234567890abcdef0 \
    --instance-id i-1234567890abcdef0 \
    --device-index 1 \
    --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Per aggiornare le impostazioni di ENA Express per il collegamento dell'interfaccia di rete

Utilizza il comando modify-network-interface-attribute come mostrato negli esempi seguenti.

Esempio 1: Utilizza ENA Express per il traffico TCP ma non per il traffico UDP

Questo esempio configura `EnaSrdEnabled` come `true` e consente l'impostazione predefinita di `EnaSrdUdpEnabled` su `false`, se non è stato fatto in precedenza.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --ena-srd-specification 'EnaSrdEnabled=true'
```

Esempio 2: utilizzo di ENA Express sia per il traffico TCP sia per il traffico UDP

Questo esempio configura sia `EnaSrdEnabled` sia `EnaSrdUdpEnabled` come `true`.

```
aws ec2 modify-network-interface-attribute \
```

```
    --network-interface-id eni-1234567890abcdef0 \
    --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Esempio 3: abbandono dell'utilizzo di ENA Express per il traffico UDP

Questo esempio configura `EnaSrdUdpEnabled` come `false`.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --ena-srd-specification 'EnaSrdUdpSpecification={EnaSrdUdpEnabled=false}'
```

PowerShell

Per configurare ENA Express durante il collegamento di un'interfaccia di rete

Utilizza il cmdlet Add-EC2NetworkInterface come mostrato negli esempi seguenti.

Esempio 1: Utilizza ENA Express per il traffico TCP ma non per il traffico UDP

Questo esempio configura `EnaSrdEnabled` come `true` e consente l'impostazione predefinita di `EnaSrdUdpEnabled` su `false`.

```
Add-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -InstanceId i-1234567890abcdef0 `
    -DeviceIndex 1 `
    -EnaSrdSpecification_EnaSrdEnabled $true
```

Esempio 2: utilizzo di ENA Express sia per il traffico TCP sia per il traffico UDP

Questo esempio configura sia `EnaSrdEnabled` sia `EnaSrdUdpEnabled` come `true`.

```
Add-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -InstanceId i-1234567890abcdef0 `
    -DeviceIndex 1 `
    -EnaSrdSpecification_EnaSrdEnabled $true `
    -EnaSrdUdpSpecification_EnaSrdUdpEnabled $true
```

Per configurare le impostazioni di ENA Express per il collegamento dell'interfaccia di rete

Utilizza il cmdlet Edit-EC2NetworkInterfaceAttribute come mostrato negli esempi seguenti.

Esempio 1: Utilizza ENA Express per il traffico TCP ma non per il traffico UDP

Questo esempio configura `EnaSrdEnabled` come `true` e consente l'impostazione predefinita di `EnaSrdUdpEnabled` su `false`, se non è stato fatto in precedenza.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -EnaSrdSpecification_EnaSrdEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List
```

Esempio 2: utilizzo di ENA Express sia per il traffico TCP sia per il traffico UDP

Questo esempio configura sia `EnaSrdEnabled` sia `EnaSrdUdpEnabled` come `true`.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -EnaSrdSpecification_EnaSrdEnabled $true `
    -EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-1234567890abcdef0 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List
```

Esempio 3: abbandono dell'utilizzo di ENA Express per il traffico UDP

Questo esempio configura `EnaSrdUdpEnabled` come `false`.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-0123f4567890a1b23 `
```

```
    -EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $false ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List
```

Configura ENA Express al momento dell'avvio

Puoi utilizzare uno dei seguenti metodi per configurare direttamente ENA Express quando si avvia un'istanza. I collegamenti specificati rimandano alle Console di gestione AWS istruzioni per questi metodi.

- Procedura guidata di avvio dell'istanza: puoi configurare ENA Express all'avvio con la procedura guidata di avvio dell'istanza. Per maggiori informazioni, consulta Configurazione avanzata di rete nelle Impostazioni di rete per la procedura guidata di avvio dell'istanza.
- Modello di avvio: puoi configurare ENA Express all'avvio quando usi un modello di avvio. Per ulteriori informazioni, consulta la pagina Creare un modello di avvio Amazon EC2, quindi espandi la sezione Impostazioni di rete e rivedi la Configurazione di rete avanzata.

Reti avanzate con l'interfaccia VF Intel 82599 sulle istanze

Ad Xen-based esempio, l'interfaccia Intel 82599 Virtual Function (VF) offre funzionalità di rete avanzate. L'interfaccia utilizza il driver Intel `ixgbevf`.

Le schede seguenti mostrano come verificare il driver della scheda di rete installato per il sistema operativo dell'istanza.

Linux

Driver dell'interfaccia di rete Linux

Utilizza il comando seguente per verificare se il modulo viene utilizzato su un'interfaccia specifica, sostituendo il nome dell'interfaccia che desideri controllare. Se usi una singola interfaccia (impostazione predefinita), essa sarà `eth0`. Se il sistema operativo supporta nomi di rete prevedibili, questo potrebbe essere un nome simile a `ens5`.

Nell'esempio seguente, il modulo `ixgbevf` non viene caricato, perché il driver nell'elenco è `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

In questo esempio, viene caricato il modulo `ixgbevf`. Questa istanza dispone della funzionalità per reti avanzate adeguatamente configurata.

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 4.0.3
firmware-version: N/A
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: no
```

Windows

Adattatore di rete Windows

Per verificare se il driver è installato, connettiti all'istanza e apri Device Manager (Gestione dispositivi). Dovresti vedere `Intel(R) 82599 Virtual Function` elencato nella sezione Adattatori di rete.

Indice

- Prepara l'istanza per le reti avanzate
- Verifica dell'abilitazione delle reti avanzate
- Abilitazione delle reti avanzate su un'istanza

- Risolvere i problemi di connettività

Prepara l'istanza per le reti avanzate

Per preparare la configurazione delle funzionalità delle reti avanzate tramite l'interfaccia VF Intel 82599, configura l'istanza nel seguente modo:

- Verifica che il tipo di istanza sia uno dei seguenti: C3, C4, D2, I2, M4 (esclusi`m4.16xlarge`) e R3.
- Verificare che l'istanza disponga di connettività Internet.
- Se sull'istanza sono presenti dati importanti che devono essere conservati, è consigliabile eseguire una copia di backup di tali dati ora mediante la creazione di un'AMI dall'istanza. L'aggiornamento dei kernel e dei relativi moduli, nonché l'abilitazione dell'attributo `sriovNetSupport`, potrebbero rendere non compatibili le istanze o irraggiungibili i sistemi operativi. Se disponi di un backup recente, i tuoi dati saranno mantenuti.
- Istanze Linux: avvia l'istanza da un'AMI HVM tramite il kernel Linux versione 2.6.32 o successive. Per le AMI HVM di Amazon Linux i moduli necessari per le reti avanzate sono installati e gli attributi obbligatori sono impostati. Pertanto, se viene avviata un'istanza supportata da Amazon EBS e che include il supporto delle reti avanzate tramite un'AMI HVM di Amazon Linux corrente, le reti avanzate sono già abilitate per l'istanza.

  > **Warning**
  >
  > Le reti avanzate sono supportate solo per le istanze HVM. L'abilitazione delle reti avanzate con un'istanza PV potrebbe rendere irraggiungibile l'istanza. L'impostazione di questo attributo senza un modulo appropriato o una versione di modulo corretta può rendere irraggiungibile l'istanza.

- Istanze Windows: avvia l'istanza da un'AMI HVM a 64 bit. Non puoi abilitare le reti avanzate su Windows Server 2008. Le reti avanzate sono già abilitate per le AMI per Windows Server 2012 R2 e Windows Server 2016 e versioni successive. Windows Server 2012 R2 include il driver Intel 1.0.15.3 e si consiglia di aggiornare tale driver alla versione più recente utilizzando l'utilità. Pnputil.exe
- Utilizzalo AWS CloudShell da Console di gestione AWS, oppure installa e configura il AWS CLI o il AWS Tools for Windows PowerShell su qualsiasi computer tu scelga, preferibilmente sul desktop o sul laptop locale. Per ulteriori informazioni, consulta Accesso a Amazon EC2 o la Guida per l'utente di AWS CloudShell. Le reti avanzate non possono essere gestite dalla console Amazon EC2.

Verifica dell'abilitazione delle reti avanzate

Verifica che l'attributo `sriovNetSupport` sia impostato sull'istanza o sull'immagine.

AWS CLI

Per controllare l'attributo di istanza (sriovNetSupport)

Utilizza il seguente comando describe-instance-attribute. Se l'attributo è impostato, il valore è `simple`.

```
aws ec2 describe-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --attribute sriovNetSupport
```

Per controllare l'attributo image (sriov) NetSupport

Utilizza il seguente comando describe-images. Se l'attributo è impostato, il valore è `simple`.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query "Images[].SriovNetSupport"
```

PowerShell

Per controllare l'attributo di istanza (sriov) NetSupport

Utilizzare il cmdlet Get-EC2InstanceAttribute. Se l'attributo è impostato, il valore è `simple`.

```
Get-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -Attribute sriovNetSupport
```

Per controllare l'attributo image (sriov) NetSupport

Utilizza il seguente comando describe-images. Se l'attributo è impostato, il valore è `simple`.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).SriovNetSupport
```

Abilitazione delle reti avanzate su un'istanza

La procedura utilizzata dipende dal sistema operativo dell'istanza.

> **Warning**
>
> Non sono disponibili procedure per disabilitare l'attributo delle reti avanzate dopo averlo abilitato.

Amazon Linux

Per le AMI HVM di Amazon Linux più recenti, il modulo `ixgbevf` necessario per le reti avanzate è installato e l'attributo `sriovNetSupport` è impostato. Pertanto, se avvii un tipo di istanza tramite un'AMI HVM di Amazon Linux corrente, le reti avanzate sono già abilitate per l'istanza. Per ulteriori informazioni, consulta Verifica dell'abilitazione delle reti avanzate.

Se l'istanza è stata avviata utilizzando una AMI Amazon Linux più vecchia che non dispone delle reti avanzate già abilitate, utilizzare la seguente procedura per abilitare le reti avanzate.

Per abilitare le reti avanzate

1. Connettiti alla tua istanza.
2. Dall'istanza, esegui il seguente comando per aggiornare l'istanza in base al nuovo kernel e ai nuovi moduli kernel, compreso `ixgbevf`:

   ```
   [ec2-user ~]$ sudo yum update
   ```

3. Dal computer locale, riavvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: reboot-instances (AWS CLI) o Restart-EC2Instance (AWS Tools for Windows PowerShell).
4. Ricollegati all'istanza e verifica che il modulo `ixgbevf` sia installato con la versione minima consigliata utilizzando il comando modinfo ixgbevf disponibile in Verifica dell'abilitazione delle reti avanzate.
5. [EBS-backed istanza] Dal tuo computer locale, interrompi l'istanza utilizzando la console Amazon EC2 o uno dei seguenti comandi: stop-instances (AWS CLI) o Stop-EC2Instance ().AWS Tools for Windows PowerShell

   [Istanza supportata da instance store] Non è possibile arrestare l'istanza per modificare l'attributo. Passa invece alla procedura successiva.
6. Dal computer locale, abilita l'attributo relativo alle reti avanzate utilizzando uno dei seguenti comandi:

AWS CLI

Utilizza il comando modify-instance-attribute come riportato di seguito.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --sriov-net-support simple
```

PowerShell

Utilizza il cmdlet Edit-EC2InstanceAttribute come riportato di seguito.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -SriovNetSupport "simple"
```

7. (Facoltativo) Crea un'AMI dall'istanza, come descritto in Crea un' EBS-backed AMI Amazon. L'AMI eredita l'attributo relativo alle reti avanzate dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con le reti avanzate abilitate per impostazione di default.
8. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI) o Start-EC2Instance (AWS Tools for Windows PowerShell).
9. Connettiti all'istanza e verifica che il modulo `ixgbevf` sia installato e caricato sull'interfaccia di rete in uso tramite il comando ethtool -i eth***n*** disponibile in Verifica dell'abilitazione delle reti avanzate.

Per abilitare le reti avanzate (istanze supportate da instance store)

Segui la procedura precedente fino al punto in cui si arresta l'istanza. Crea una nuova AMI come descritto in Crea un' S3-backed AMI Amazon, assicurandoti di abilitare l'attributo relativo alle reti avanzate durante la registrazione dell'AMI.

AWS CLI

Utilizza il comando register-image come riportato di seguito.

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Utilizza Register-EC2Image come segue.

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Ubuntu

Prima di iniziare, controlla se le reti avanzate sono già abilitate nell'istanza.

L'AMI HVM Quick Start Ubuntu (Avvio rapido Ubuntu) include i driver necessari per le reti avanzate. Se hai una versione di `ixgbevf` precedente alla 2.16.4, puoi installare il pacchetto kernel `linux-aws` per avere i driver di rete ottimizzati più recenti.

La seguente procedura descrive le fasi generali necessarie per compilare il modulo `ixgbevf` su un'istanza Ubuntu.

Per installare il pacchetto del kernel **`linux-aws`**

1. Connettiti alla tua istanza.
2. Aggiorna la cache dei pacchetti e i pacchetti.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Se durante il processo di aggiornamento viene richiesto di installare `grub`, utilizza `/dev/xvda` per installare `grub`, quindi scegli di conservare la versione corrente di `/boot/grub/menu.lst`.

Altre distribuzioni Linux

Prima di iniziare, controlla se le reti avanzate sono già abilitate nell'istanza. L'AMI HVM Quick Start (Avvio rapido) più recente include i driver necessari per le reti avanzate. Non devi pertanto eseguire procedure aggiuntive.

La procedura seguente descrive le fasi generali da eseguire se devi abilitare le reti avanzate con l'interfaccia VF Intel 82599 su una distribuzione Linux diversa da Amazon Linux o Ubuntu. Per

ulteriori informazioni, ad esempio sintassi dettagliata dei comandi, posizione dei file o supporto di pacchetti e strumenti, consulta la documentazione specifica per la distribuzione Linux in uso.

Per abilitare le reti avanzate su Linux

1. Connettiti alla tua istanza.
2. Scarica il codice sorgente del `ixgbevf` modulo sulla tua istanza da Sourceforge all'indirizzo %20stable/. https://sourceforge.net/projects/e1000/files/ixgbevf

   Le versioni di `ixgbevf` precedenti alla 2.16.4, compresa la versione 2.14.2, non vengono compilate correttamente su alcune distribuzioni Linux, comprese determinate versioni di Ubuntu.
3. Compila e installa il modulo `ixgbevf` sull'istanza.

   > **Warning**
   >
   > Se si esegue la compilazione del modulo `ixgbevf` per il kernel corrente e quindi si aggiorna il kernel senza ricompilare il driver per il nuovo kernel, al successivo riavvio il sistema potrebbe ripristinare il modulo `ixgbevf` specifico della distribuzione. Questo potrebbe rendere irraggiungibile il sistema se la versione specifica della distribuzione è incompatibile con la rete migliorata.
4. Esegui il comando sudo depmod per aggiornare le dipendenze del modulo.
5. Aggiorna `initramfs` sull'istanza in modo che il nuovo modulo venga caricato in fase di avvio.
6. Determina se il sistema utilizza nomi di interfaccia di rete prevedibili per impostazione di default. I sistemi che utilizzano systemd o udev versione 197 o successive possono rinominare i dispositivi Ethernet e pertanto non garantiscono che la singola interfaccia di rete venga rinominata in `eth0`. Questo comportamento potrebbe causare problemi durante la connessione all'istanza. Per ulteriori informazioni e per informazioni sulle altre opzioni di configurazione disponibili, consulta l'argomento relativo ai nomi di interfaccia di rete prevedibili sul sito Web freedesktop.org.

   a. Puoi controllare le udev versioni systemd o sui sistemi con il seguente comando: RPM-based

      ```
      [ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
          systemd-208-11.el7_0.2.x86_64
      ```

      Nell'esempio precedente relativo a Red Hat Enterprise Linux 7, la versione di systemd è 208, pertanto, i nomi di interfaccia di rete prevedibili devono essere disabilitati.

b. Disabilitare i nomi di interfaccia di rete prevedibili aggiungendo l'opzione `net.ifnames=0` alla riga `GRUB_CMDLINE_LINUX` in `/etc/default/grub`.

```
[ec2-user ~]$ sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /
etc/default/grub
```

c. Ricompila il file di configurazione di grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [EBS-backed istanza] Dal tuo computer locale, interrompi l'istanza utilizzando la console Amazon EC2 o uno dei seguenti comandi: stop-instances (AWS CLI) o (). Stop-EC2InstanceAWS Tools for Windows PowerShell

   [Istanza supportata da instance store] Non è possibile arrestare l'istanza per modificare l'attributo. Passa invece alla procedura successiva.

8. Dal computer locale, abilita l'attributo relativo alle reti avanzate utilizzando uno dei seguenti comandi:

   AWS CLI

   Utilizza il comando modify-instance-attribute come riportato di seguito.

   ```
   aws ec2 modify-instance-attribute \
       --instance-id i-1234567890abcdef0 -\
       -sriov-net-support simple
   ```

   PowerShell

   Utilizza il cmdlet Edit-EC2InstanceAttribute come riportato di seguito.

   ```
   Edit-EC2InstanceAttribute `
       -InstanceId i-1234567890abcdef0 `
       -SriovNetSupport "simple"
   ```

9. (Facoltativo) Crea un'AMI dall'istanza, come descritto in Crea un' EBS-backed AMI Amazon. L'AMI eredita l'attributo relativo alle reti avanzate dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con le reti avanzate abilitate per impostazione di default.

Se il sistema operativo dell'istanza contiene un file `/etc/udev/rules.d/70-persistent-net.rules`, è necessario eliminarlo prima di creare l'AMI. Questo file contiene l'indirizzo MAC per la scheda Ethernet dell'istanza originale. Se un'altra istanza viene avviata con questo file, il sistema operativo non sarà in grado di trovare il dispositivo ed `eth0` potrebbe non funzionare causando problemi di avvio. Questo file viene rigenerato al successivo ciclo di avvio e qualsiasi istanza avviata dall'AMI crea la propria versione del file.

10. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI) o Start-EC2Instance (AWS Tools for Windows PowerShell).
11. (Facoltativo) Connettiti all'istanza e verifica che il modulo sia installato.

Per abilitare le reti avanzate (istanze supportate da archivio istanze)

Segui la procedura precedente fino al punto in cui si arresta l'istanza. Crea una nuova AMI come descritto in Crea un' S3-backed AMI Amazon, assicurandoti di abilitare l'attributo relativo alle reti avanzate durante la registrazione dell'AMI.

AWS CLI

Utilizza il comando register-image come riportato di seguito.

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Utilizza Register-EC2Image come segue.

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Windows

Se hai avviato l'istanza per la quale la funzionalità di reti avanzate non è già abilitata, devi scaricare e installare il driver per la scheda di rete richiesto sull'istanza e quindi impostare l'attributo `sriovNetSupport` dell'istanza in modo da attivare le reti avanzate. Puoi abilitare questo attributo solo sui tipi di istanza supportati. Per ulteriori informazioni, consulta Rete migliorata per le istanze Amazon EC2.

> **Important**
>
> Per visualizzare gli ultimi aggiornamenti dei driver nelle AMI di Windows, consulta la cronologia delle versioni di Windows AMI nel Riferimento Ami Windows AMI AWS .

Per abilitare le reti avanzate

1. Connettersi all'istanza ed eseguire l'accesso come amministratore locale.
2. [Windows Server 2016 e versioni successive] Esegui il seguente PowerShell script di avvio EC2 per configurare l'istanza dopo l'installazione del driver.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

> **Important**
>
> La password amministratore verrà reimpostata quando abiliti lo script EC2 Launch dell'istanza di inizializzazione. Puoi modificare il file di configurazione per disattivare la reimpostazione della password amministratore specificandolo nelle impostazioni delle attività di inizializzazione.

3. Dall'istanza, scaricare il driver della scheda di rete Intel per il sistema operativo in uso:
   - Windows Server 2022

     Visita la pagina di download e scarica `Wired_driver_version_x64.zip`.
   - Windows Server 2019 incluso per Server versione 1809 e successive*

     Visita la pagina di download e scarica `Wired_driver_version_x64.zip`.
   - Windows Server 2016 incluso per Server versione 1803 e precedenti*

     Visita la pagina di download e scarica `Wired_driver_version_x64.zip`.
   - Windows Server 2012 R2

     Visita la pagina di download e scarica `Wired_driver_version_x64.zip`.
   - Windows Server 2012

Visita la pagina di download e scarica `Wired_driver_version_x64.zip`.

- Windows Server 2008 R2

  Visita la pagina di download e scarica `PROWinx64Legacy.exe`.

*Le versioni Server 1803 e precedenti e 1809 e successive non sono specificatamente trattate nelle pagine Driver e Software Intel.

4. Installa il driver della scheda di rete Intel per il sistema operativo in uso.

   - Windows Server 2008 R2

     1. Nella cartella Downloads, individua il file `PROWinx64Legacy.exe` e rinominalo `PROWinx64Legacy.zip`.
     2. Estrai i contenuti del file `PROWinx64Legacy.zip`.
     3. Apri la riga di comando, passa alla cartella contenente i file estratti e utilizza l'utility `pnputil` per aggiungere e installare il file INF nell'archivio dei driver.

     ```
     C:\> pnputil -a PROXGB\Winx64\NDIS62\vxn62x64.inf
     ```

   - Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 e Windows Server 2012

     1. Nella cartella Downloads, estrarre i contenuti del file `Wired_driver_version_x64.zip`.
     2. Apri la riga di comando, passa alla cartella contenente i file estratti ed esegui uno dei seguenti comandi per utilizzare l'utility `pnputil` per aggiungere e installare il file INF nell'archivio dei driver.

        - Windows Server 2022

        ```
        pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
        ```

        - Windows Server 2019

        ```
        pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
        ```

        - Windows Server 2016

        ```
        pnputil -i -a PROXGB\Winx64\NDIS65\vxn65x64.inf
        ```

- Windows Server 2012 R2

```
pnputil -i -a PROXGB\Winx64\NDIS64\vxn64x64.inf
```

- Windows Server 2012

```
pnputil -i -a PROXGB\Winx64\NDIS63\vxn63x64.inf
```

5. Dal computer locale, abilita l'attributo relativo alle reti avanzate utilizzando uno dei seguenti comandi:

   AWS CLI

   Utilizza il comando modify-instance-attribute come riportato di seguito.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --sriov-net-support simple
```

   PowerShell

   Utilizza il cmdlet Edit-EC2InstanceAttribute come riportato di seguito.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -SriovNetSupport "simple"
```

6. (Facoltativo) Crea un'AMI dall'istanza, come descritto in Crea un' EBS-backed AMI Amazon. L'AMI eredita l'attributo relativo alle reti avanzate dall'istanza. Pertanto, è possibile utilizzare questa AMI per avviare un'altra istanza con le reti avanzate abilitate per impostazione di default.
7. Dal computer locale, avvia l'istanza utilizzando la console Amazon EC2 o uno dei comandi seguenti: start-instances (AWS CLI) o Start-EC2Instance (AWS Tools for Windows PowerShell).

Risolvere i problemi di connettività

Se si perde la connettività durante l'abilitazione delle reti avanzate, il modulo `ixgbevf` potrebbe non essere compatibile con il kernel. Prova a installare la versione del modulo `ixgbevf` inclusa nella distribuzione di Linux per l'istanza in uso.

Se si abilitano le reti avanzate per un'istanza PV o AMI, l'istanza può risultare irraggiungibile.

Per ulteriori informazioni, consulta Come abilitare e configurare le reti avanzate sulle mie istanze EC2?

Monitoraggio delle prestazioni di rete per le impostazioni ENA dell'istanza EC2

Il driver ENA (Elastic Network Adapter) pubblica i parametri delle prestazioni di rete dalle istanze in cui sono attivati. È possibile utilizzare questi parametri per risolvere i problemi relativi alle prestazioni delle istanze, scegliere la dimensione dell'istanza appropriata per un carico di lavoro, pianificare le attività di scalabilità in modo proattivo e confrontare le applicazioni per determinare se massimizzano le prestazioni disponibili in un'istanza.

Amazon EC2 definisce i valori massimi di rete a livello di istanza per garantire un'esperienza di rete di alta qualità, comprese prestazioni di rete costanti per tutte le dimensioni delle istanze. AWS fornisce i valori massimi per quanto segue per ogni istanza:

- Capacità di larghezza di banda: ogni istanza EC2 ha una larghezza di banda massima per il traffico aggregato in entrata e in uscita, in base al tipo e alle dimensioni dell'istanza. Alcune istanze utilizzano un meccanismo di I/O credito di rete per allocare la larghezza di banda di rete in base all'utilizzo medio della larghezza di banda. Amazon EC2 dispone inoltre di una larghezza di banda massima per il traffico verso e verso Internet. Direct Connect Per ulteriori informazioni, consulta Larghezza di banda di rete dell'istanza Amazon EC2.
- Packet-per-second Prestazioni (PPS): ogni istanza EC2 offre prestazioni PPS massime, in base al tipo e alla dimensione dell'istanza.
- Connessioni tracciate: il gruppo di sicurezza tiene traccia di ogni connessione stabilita per garantire che i pacchetti restituiti vengano consegnati come previsto. Per ciascuna istanza esiste un numero massimo di connessioni che possono essere monitorate. Per ulteriori informazioni, consulta Monitoraggio della connessione al gruppo di sicurezza Amazon EC2
- Link-local accesso al servizio: Amazon EC2 fornisce un PPS massimo per interfaccia di rete per il traffico verso servizi proxy locali come il servizio Amazon DNS, l'Instance Metadata Service e l'Amazon Time Sync Service.

Quando il traffico di rete per un'istanza supera un limite massimo, AWS modella il traffico che supera il limite massimo inserendo in coda e quindi eliminando i pacchetti di rete. Utilizzando i parametri delle prestazioni di rete è possibile monitorare quando il traffico supera un valore massimo. Questi parametri indicano in tempo reale l'impatto sul traffico di rete e i possibili problemi relativi alle prestazioni della rete.

Indice

- Requisiti
- Parametri per il driver ENA
- Visualizzare i parametri delle prestazioni di rete per l'istanza
- Parametri di ENA Express
- Parametri delle prestazioni di rete con il driver DPDK per ENA
- Metriche sulle istanze in esecuzione FreeBSD

Requisiti

Istanze Linux

- Installare il driver ENA versione 2.2.10 o successiva. Per verificare la versione installata, utilizzare il comando ethtool. Nell'esempio seguente, la versione soddisfa il requisito minimo.

  ```
  [ec2-user ~]$ ethtool -i eth0 | grep version
  version: 2.2.10
  ```

  Per aggiornare il driver ENA, consulta Reti avanzate.
- Per importare queste metriche su Amazon, installa l'agente. CloudWatch CloudWatch Per ulteriori informazioni, consulta Collect Network Performance Metrics nella Amazon CloudWatch User Guide.
- Per supportare la metrica `conntrack_allowance_available`, installa la versione 2.8.1 o successiva del driver ENA.
- Per ignorare il limite PPS del frammento di uscita di 1024, installa la versione 2.13.3 o successiva del driver ENA.

Istanze Windows

- Installare il driver ENA versione 2.2.2 o successiva. Per verificare la versione installata, utilizzare Gestione periferiche come segue.
  1. Aprire Gestione periferiche eseguendo `devmgmt.msc`.
  2. Espandere Network Adapters (Schede di rete).
  3. Scegliere Amazon Elastic Network Adapter (Adattatore di rete elastico di Amazon), quindi Properties (Proprietà).

4. Nella scheda Driver individuare Driver Version (Versione driver).

   Per aggiornare il driver ENA, consulta Reti avanzate.

- Per importare queste metriche su Amazon CloudWatch, installa l' CloudWatch agente. Per ulteriori informazioni, consulta Collect advanced network metrics nella Amazon CloudWatch User Guide.

Parametri per il driver ENA

Il driver ENA fornisce i seguenti parametri all'istanza in tempo reale. Questi forniscono il numero complessivo di pacchetti accodati o rilasciati su ciascuna interfaccia di rete dall'ultimo ripristino del driver.

Metrica	Description	Supportato su
`bw_in_allowance_exceeded`	Il numero di pacchetti accordati o rilasciati perché la larghezza di banda aggregata in ingresso ha superato il valore massimo per l'istanza.	Tutti i tipi di istanza
`bw_out_allowance_exceeded`	Il numero di pacchetti accodati o rilasciati perché la larghezza di banda aggregata in uscita ha superato il valore massimo per l'istanza.	Tutti i tipi di istanza
`conntrack_allowance_exceeded`	Il numero di pacchetti accodati o rilasciati perché il rilevamento delle connessioni ha superato il valore massimo per l'istanza e non è stato possibile stabilire nuove connessioni. Ciò può comportare la perdita di pacchetti per il traffico da o verso l'istanza.	Tutti i tipi di istanza
`conntrack_allowance_available`	Il numero di connessioni tracciate che possono essere	Nitro-based solo istanze

Metrica	Description	Supportato su
	stabilite dall'istanza prima di raggiungere il limite Connessioni tracciate di quel tipo di istanza.	
`linklocal_allowance_exceeded`	Il numero di pacchetti accodati o rilasciati perché il PPS del traffico verso i servizi proxy locali ha superato il valore massimo per l'interfaccia di rete. Ciò influisce sul traffico verso il servizio Amazon DNS, il servizio di metadati dell'istanza e il servizio di sincronizzazione oraria di Amazon, ma non influisce sul traffico verso i resolver DNS personalizzati.	Tutti i tipi di istanza
`pps_allowance_exceeded`	Il numero di pacchetti in coda o abbandonati perché il PPS bidirezionale ha superato il valore massimo per l'istanza. *	Tutti i tipi di istanza

* A seconda dell'impostazione della modalità proxy a frammenti per il driver ENA Linux v2.13.3 o successiva, tale limite può includere anche abbandono di frammenti in uscita superiori a 1024 PPS per l'interfaccia di rete. Se la modalità proxy a frammenti è abilitata per il driver Linux, gli abbandoni di frammenti in uscita aggirano il limite di 1024 PPS normalmente applicato e sono conteggiate entro le autorizzazioni PPS standard. Per impostazione predefinita, la modalità proxy a frammenti è disabilitata.

Visualizzare i parametri delle prestazioni di rete per l'istanza

La procedura utilizzata dipende dal sistema operativo dell'istanza.

Istanze Linux

È possibile pubblicare parametri negli strumenti preferiti per visualizzare i dati dei parametri. Ad esempio, puoi pubblicare le metriche su Amazon CloudWatch utilizzando l' CloudWatch agente. L'agente consente di selezionare singoli parametri e di controllare la pubblicazione.

Inoltre, è possibile utilizzare ethtool per recuperare i parametri per ogni interfaccia di rete, ad esempio eth0, come indicato di seguito.

```
[ec2-user ~]$ ethtool -S eth0
     bw_in_allowance_exceeded: 0
     bw_out_allowance_exceeded: 0
     pps_allowance_exceeded: 0
     conntrack_allowance_exceeded: 0
     linklocal_allowance_exceeded: 0
     conntrack_allowance_available: 136812
```

Istanze Windows

È possibile visualizzare i parametri utilizzando qualsiasi consumer di contatori delle prestazioni di Windows. I dati possono essere analizzati in base al manifesto. EnaPerfCounters Si tratta di un file XML che definisce il fornitore del contatore delle prestazioni e i relativi set di contatori.

Per installare il manifesto

Se l'istanza è stata avviata utilizzando una AMI contenente il driver ENA 2.2.2 o versione successiva, o si è utilizzato lo script di installazione nel pacchetto driver per il driver ENA 2.2.2, il manifest è già installato. Per installare manualmente il manifest, attenersi alla seguente procedura:

1. Rimuovere il manifest esistente utilizzando il seguente comando:

   ```
   unlodctr /m:EnaPerfCounters.man
   ```

2. Copiare il file manifest `EnaPerfCounters.man` dal pacchetto di installazione del driver a `%SystemRoot%\System32\drivers`.
3. Installare il nuovo manifest utilizzando il seguente comando:

   ```
   lodctr /m:EnaPerfCounters.man
   ```

Per visualizzare i parametri utilizzando Performance Monitor

1. Aprire Performance Monitor.
2. Premere Ctrl+N per aggiungere nuovi contatori.
3. Scegliere ENA Packets Shaping (Modellazione pacchetti ENA) dall'elenco.
4. Selezionare le istanze da monitorare e scegliere Add (Aggiungi).
5. Seleziona OK.

Parametri di ENA Express

ENA Express è basato sulla tecnologia AWS Scalable Reliable Datagram (SRD). SRD è un protocollo di trasporto di rete ad alte prestazioni che utilizza l'instradamento dinamico per aumentare il throughput e ridurre al minimo la latenza di coda. Se è stato abilitato ENA Express per i collegamenti dell'interfaccia di rete sia sull'istanza di invio sia sull'istanza di ricezione, è possibile utilizzare i parametri di ENA Express per garantire che le istanze traggano il massimo vantaggio dai miglioramenti delle prestazioni offerti dalla tecnologia SRD. Ad esempio:

- Valuta le tue risorse per assicurarti che abbiano una capacità sufficiente per stabilire più connessioni SRD.
- Identifica dove risiedono i potenziali problemi che impediscono ai pacchetti in uscita idonei di utilizzare SRD.
- Calcola la percentuale di traffico in uscita che utilizza SRD per l'istanza.
- Calcola la percentuale di traffico in entrata che utilizza SRD per l'istanza.

> **Note**
>
> Per produrre parametri, utilizza la versione 2.8 o successiva del driver.

Per visualizzare un elenco di parametri per l'istanza Linux filtrati per ENA Express, eseguire il comando ethtool per l'interfaccia di rete (mostrata qui come `eth0`). Prendere nota del valore del parametro `ena_srd_mode`.

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 1
```

```
ena_srd_tx_pkts: 0
ena_srd_eligible_tx_pkts: 0
ena_srd_rx_pkts: 0
ena_srd_resource_utilization: 0
```

I seguenti parametri sono disponibili per tutte le istanze con ENA Express abilitato.

ena_srd_mode

Descrive quali funzionalità ENA Express sono abilitate. I valori sono i seguenti:

- `0` = ENA Express disattivato, UDP disattivato
- `1` = ENA Express attivato, UDP disattivato
- `2` = ENA Express disattivato, UDP attivato

> **Note**
>
> Ciò accade solo quando ENA Express è stato abilitato in origine e UDP è stato configurato per il suo utilizzo. Il valore precedente viene mantenuto per il traffico UDP.

- `3` = ENA Express attivato, UDP attivato

ena_srd_eligible_tx_pkts

Il numero di rete è il seguente:

- Sono supportati i tipi sia delle istanze di invio sia di quelle di ricezione. Per ulteriori informazioni, consulta la tabella Tipi di istanza supportati per ENA Express.
- Sia le istanze di invio sia quelle di ricezione devono avere ENA Express configurato.
- Le istanze di invio e ricezione devono essere eseguite nella stessa regione.
- Il percorso di rete tra le istanze non deve includere box middleware (software intermediario). ENA Express attualmente non supporta i box middleware (software intermediario).

> **Note**
>
> Il parametro di idoneità ENA Express copre i requisiti di origine e destinazione e la rete tra i due endpoint. I pacchetti idonei possono comunque essere squalificati dopo che sono già stati contati. Ad esempio, se un pacchetto idoneo supera il limite massimo di unità di trasmissione (MTU), torna alla trasmissione ENA standard, sebbene il pacchetto sia comunque indicato come idoneo nel contatore.

ena_srd_tx_pkts

Il numero di pacchetti SRD trasmessi in un determinato periodo di tempo.

ena_srd_rx_pkts

Il numero di pacchetti SRD ricevuti in un determinato periodo di tempo.

ena_srd_resource_utilization

La percentuale di utilizzo massimo della memoria consentita per le connessioni SRD simultanee adoperate dall'istanza.

Per verificare se la trasmissione dei pacchetti utilizza SRD, è possibile confrontare il numero di pacchetti idonei (parametro `ena_srd_eligible_tx_pkts`) con il numero di pacchetti SRD trasmessi (parametro `ena_srd_tx_pkts`) durante un determinato periodo di tempo.

Traffico in uscita (pacchetti in uscita)

Per assicurarti che il traffico in uscita utilizzi SRD come previsto, confronta il numero di pacchetti SRD idonei (`ena_srd_eligible_tx_pkts`) con il numero di pacchetti SRD inviati (`ena_srd_tx_pkts`) in un determinato periodo di tempo.

Differenze significative tra il numero di pacchetti idonei e il numero di pacchetti SRD inviati sono spesso causate da problemi di utilizzo delle risorse. Quando la scheda di rete collegata all'istanza ha esaurito le sue risorse massime o se i pacchetti superano il limite MTU, i pacchetti idonei non sono in grado di trasmettere tramite SRD e devono ricorrere alla trasmissione ENA standard. I pacchetti possono rientrare in questa lacuna anche durante le migrazioni in tempo reale o gli aggiornamenti del server in tempo reale. È necessaria un'ulteriore risoluzione dei problemi per determinare la causa principale.

> **Note**
>
> È possibile ignorare le piccole differenze occasionali tra il numero di pacchetti idonei e il numero di pacchetti SRD. Tali differenze possono verificarsi, ad esempio, quando l'istanza stabilisce una connessione a un'altra istanza per il traffico SRD.

Per scoprire quale percentuale del traffico totale in uscita in un determinato periodo di tempo utilizza SRD, confronta il numero di pacchetti SRD inviati (`ena_srd_tx_pkts`) con il numero totale di pacchetti inviati per l'istanza (`NetworkPacketOut`) durante tale periodo.

Traffico in ingresso (pacchetti in entrata)

Per scoprire quale percentuale del traffico in entrata utilizza SRD, confronta il numero di pacchetti SRD ricevuti (`ena_srd_rx_pkts`) in un determinato periodo di tempo con il numero totale di pacchetti ricevuti per l'istanza (`NetworkPacketIn`) durante tale periodo.

Utilizzo delle risorse

L'utilizzo delle risorse si basa sul numero di connessioni SRD simultanee che una singola istanza può sostenere in un dato momento. Il parametro di utilizzo delle risorse (`ena_srd_resource_utilization`) tiene traccia dell'utilizzo corrente per l'istanza. A mano a mano che l'utilizzo si avvicina al 100%, puoi aspettarti di riscontrare problemi di prestazioni. ENA Express passa dalla trasmissione SRD alla trasmissione ENA standard e la possibilità di perdita di pacchetti aumenta. L'elevato utilizzo delle risorse indica che è giunto il momento di dimensionare l'istanza per migliorare le prestazioni della rete.

> **Note**
>
> Quando il traffico di rete per un'istanza supera il limite massimo, AWS modella il traffico che supera il limite massimo inserendo in coda e quindi eliminando i pacchetti di rete.

Persistenza

I parametri di uscita e ingresso si accumulano quando ENA Express è abilitato per l'istanza. I parametri smettono di accumularsi se ENA Express è disattivato, ma persistono fintantoché l'istanza è in esecuzione. I parametri vengono ripristinati se l'istanza si riavvia o viene terminata oppure se l'interfaccia di rete viene scollegata dall'istanza.

Parametri delle prestazioni di rete con il driver DPDK per ENA

Il driver ENA versione 2.2.0 e successive supporta il reporting dei parametri di rete. DPDK 20.11 include il driver ENA 2.2.0 ed è la prima versione di DPDK a supportare questa funzionalità.

Il driver DPDK v25.03 o versione successiva supporta la modalità proxy a frammenti. Se la modalità proxy a frammenti è abilitata per il driver DPDK, gli abbandoni di frammenti in uscita aggirano il limite di 1024 PPS normalmente applicato e sono conteggiate entro le autorizzazioni PPS standard. Per impostazione predefinita, la modalità proxy a frammenti è disabilitata.

È possibile utilizzare un'applicazione di esempio per visualizzare le statistiche DPDK. Per avviare una versione interattiva dell'applicazione di esempio, esegui il comando seguente.

```
./app/dpdk-testpmd -- -i
```

All'interno di questa sessione interattiva, è possibile immettere un comando per recuperare le statistiche estese per una porta. Il seguente comando di esempio recupera le statistiche per la porta 0.

```
show port xstats 0
```

Di seguito è riportato un esempio di sessione interattiva con l'applicazione di esempio DPDK.

```
[root@ip-192.0.2.0 build]# ./app/dpdk-testpmd -- -i
        EAL: Detected 4 lcore(s)
        EAL: Detected 1 NUMA nodes
        EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
        EAL: Selected IOVA mode 'PA'
        EAL: Probing VFIO support...
        EAL:   Invalid NUMA socket, default to 0
        EAL:   Invalid NUMA socket, default to 0
        EAL: Probe PCI driver: net_ena (1d0f:ec20) device: 0000:00:06.0
(socket 0)
        EAL: No legacy callbacks, legacy socket not created
        Interactive-mode selected

        Port 0: link state change event
        testpmd: create a new mbuf pool <mb_pool_0>: n=171456,
size=2176, socket=0
        testpmd: preferred mempool ops selected: ring_mp_mc

        Warning! port-topology=paired and odd forward ports number, the
last port will pair with itself.

        Configuring Port 0 (socket 0)
        Port 0: 02:C7:17:A2:60:B1
        Checking link statuses...
        Done
        Error during enabling promiscuous mode for port 0: Operation
not supported - ignore
        testpmd> show port xstats 0
        ###### NIC extended statistics for port 0
        rx_good_packets: 0
        tx_good_packets: 0
        rx_good_bytes: 0
```

```
        tx_good_bytes: 0
        rx_missed_errors: 0
        rx_errors: 0
        tx_errors: 0
        rx_mbuf_allocation_errors: 0
        rx_q0_packets: 0
        rx_q0_bytes: 0
        rx_q0_errors: 0
        tx_q0_packets: 0
        tx_q0_bytes: 0
        wd_expired: 0
        dev_start: 1
        dev_stop: 0
        tx_drops: 0
        bw_in_allowance_exceeded: 0
        bw_out_allowance_exceeded: 0
        pps_allowance_exceeded: 0
        conntrack_allowance_exceeded: 0
        linklocal_allowance_exceeded: 0
        rx_q0_cnt: 0
        rx_q0_bytes: 0
        rx_q0_refill_partial: 0
        rx_q0_bad_csum: 0
        rx_q0_mbuf_alloc_fail: 0
        rx_q0_bad_desc_num: 0
        rx_q0_bad_req_id: 0
        tx_q0_cnt: 0
        tx_q0_bytes: 0
        tx_q0_prepare_ctx_err: 0
        tx_q0_linearize: 0
        tx_q0_linearize_failed: 0
        tx_q0_tx_poll: 0
        tx_q0_doorbells: 0
        tx_q0_bad_req_id: 0
        tx_q0_available_desc: 1023
        testpmd>
```

Per ulteriori informazioni sull'applicazione di esempio e sul suo utilizzo per recuperare statistiche estese, consulta Testpmd Application User Guide nella documentazione di DPDK.

Metriche sulle istanze in esecuzione FreeBSD

A partire dalla versione 2.3.0, il driver ENA FreeBSD supporta la raccolta di parametri sulle prestazioni di rete su istanze che eseguono FreeBSD. Per abilitare la raccolta delle FreeBSD metriche, immetti il comando seguente e imposta *interval* un valore compreso tra 1 e 3600. Questo specifica la frequenza con cui, in pochi secondi, raccogliere i parametri di FreeBSD.

```
sysctl dev.ena.network_interface.eni_metrics.sample_interval=interval
```

Ad esempio, il seguente comando imposta il driver affinché raccolga i parametri di FreeBSD sull'interfaccia di rete 1 ogni 10 secondi:

```
sysctl dev.ena.1.eni_metrics.sample_interval=10
```

Per disattivare la raccolta di FreeBSD metriche, puoi eseguire il comando precedente e specificare come. `0` *interval*

Dopo aver abilitato la raccolta dei parametri di FreeBSD, è possibile recuperare l'ultima serie di parametri raccolti eseguendo il seguente comando.

```
sysctl dev.ena.network_interface.eni_metrics
```

Miglioramento della latenza di rete per le istanze EC2 basate su Linux

La latenza di rete è il tempo che un pacchetto di dati impiega per viaggiare dall'origine alla destinazione. Le applicazioni che inviano dati attraverso la rete dipendono da risposte tempestive per fornire un'esperienza utente positiva. Una latenza di rete elevata può portare a vari problemi, come i seguenti:

- Tempi di caricamento lenti per le pagine Web
- Ritardi nello streaming video
- Difficoltà di accesso alle risorse online

Questa sezione descrive le misure che puoi adottare per migliorare la latenza di rete sulle istanze Amazon EC2 in esecuzione su Linux. Per ottenere una latenza ottimale, segui questi passaggi per configurare le impostazioni dell'istanza, del kernel e del driver ENA. Per ulteriori indicazioni sulla configurazione, consulta la Guida alle best practice e all'ottimizzazione delle prestazioni dei driver ENA Linux suGitHub.

> **Note**
>
> I passaggi e le impostazioni possono variare leggermente a seconda dell'hardware di rete specifico, dell'AMI dalla quale hai avviato l'istanza e del caso d'uso dell'applicazione. Prima di apportare modifiche, verifica e monitora accuratamente le prestazioni della rete per assicurarti di ottenere i risultati desiderati.

Ridurre il numero di hop di rete per i pacchetti di dati

Ogni hop eseguito da un pacchetto di dati mentre si sposta da un router all'altro aumenta la latenza di rete. In genere, il traffico deve compiere più hop per raggiungere la destinazione. Esistono due modi per ridurre gli hop di rete per le istanze Amazon EC2, descritti di seguito:

- Gruppo di posizionamento cluster: quando specifichi un gruppo di posizionamento cluster, Amazon EC2 avvia le istanze che si trovano vicine l'una all'altra, fisicamente all'interno della stessa zona di disponibilità (AZ) con pacchetti più ristretti. La vicinanza fisica delle istanze del gruppo consente loro di sfruttare la connettività ad alta velocità, con conseguente bassa latenza ed elevato throughput a flusso singolo.
- Host dedicato: un host dedicato è un server fisico dedicato al tuo utilizzo. Con un host dedicato, puoi avviare le tue istanze per eseguirle sullo stesso server fisico. La comunicazione tra istanze eseguite sullo stesso host dedicato può avvenire senza hop di rete aggiuntivi.

In che modo la configurazione del kernel Linux influisce sulla latenza

La configurazione del kernel Linux può aumentare o diminuire la latenza di rete. Per raggiungere gli obiettivi di ottimizzazione della latenza, è importante ottimizzare la configurazione del kernel Linux in base ai requisiti specifici del tuo carico di lavoro.

Molte opzioni di configurazione per il kernel Linux potrebbero contribuire a ridurre la latenza di rete. Le opzioni che hanno un impatto maggiore sono le seguenti.

- Abilita la modalità polling occupato: la modalità polling occupato riduce la latenza sul percorso di ricezione della rete. Quando si abilita la modalità polling occupato, il codice del socket layer può interrogare direttamente la coda di ricezione di un dispositivo di rete. L'aspetto negativo del polling attivo è il maggiore utilizzo della CPU nell'host, derivante dall'analisi di nuovi dati in un ciclo ristretto. Esistono due impostazioni globali che controllano il numero di microsecondi di attesa per i pacchetti in tutte le interfacce.

`busy_read`

Un timeout di polling attivo a bassa latenza per le letture del socket. Controlla il numero di microsecondi di attesa concessi al socket layer per leggere i pacchetti nella coda del dispositivo. Per abilitare la funzionalità a livello globale con il comando sysctl, l'organizzazione del kernel Linux consiglia un valore di 50 microsecondi. Per ulteriori informazioni, consulta busy_read nella Guida per l'utente e l'amministratore del kernel Linux.

```
[ec2-user ~]$ sudo sysctl -w net.core.busy_read=50
```

`busy_poll`

Un timeout di polling attivo a bassa latenza per il polling e la selezione. Questo timeout controlla il numero di microsecondi di attesa per gli eventi. Il valore consigliato è tra 50-100 microsecondi, in base al numero di socket di cui esegui il polling. Più socket aggiungi, più alto dovrebbe essere il numero.

```
[ec2-user ~]$ sudo sysctl -w net.core.busy_poll=50
```

- Configura gli stati di alimentazione della CPU (C-states): C-states controlla i livelli di sonno che un core può raggiungere quando è inattivo. Potresti voler controllare per ottimizzare il sistema C-states in base alla latenza rispetto alle prestazioni. Più in dettaglio C-states, la CPU è essenzialmente «addormentata» e non può rispondere alle richieste finché non si riattiva e torna allo stato attivo. Inserire i core nello stato di sospensione richiedete del tempo. Sebbene un core sospeso consenta maggiore capacità aggiuntiva per un altro core per raggiungere una frequenza più elevata, è necessario del tempo affinché il core sospeso torni attivo e in funzione.

  Ad esempio, se un core assegnato per gestire le interruzioni di un pacchetto di rete è addormentato, potrebbe verificarsi un ritardo nel lavoro su tale interruzione. È possibile configurare il sistema in modo che non venga utilizzato più a fondo. C-states Tuttavia, questa configurazione non solo riduce la latenza della reazione del processore, ma anche la capacità disponibile negli altri core per il Turbo Boost.

  Per ridurre la latenza di reazione del processore, è possibile limitare più a fondo C-states. Per ulteriori informazioni, consulta High performance and low latency by limiting C-states in Amazon Linux 2 User Guide.

Moderazione delle interruzioni

Il driver di rete ENA consente la comunicazione tra un'istanza e una rete. Il driver elabora i pacchetti di rete e li trasmette allo stack di rete o alla scheda Nitro. Quando arriva un pacchetto di rete, la scheda Nitro genera un'interruzione per consentire alla CPU di notificare al software un evento.

Interruzione

Un'interruzione è un segnale che un dispositivo o un'applicazione invia al processore. L'interruzione indica al processore che si è verificato un evento o è stata soddisfatta una condizione che richiede un'attenzione immediata. Le interruzioni possono gestire attività urgenti come la ricezione di dati da un'interfaccia di rete, la gestione di eventi hardware o di richieste di assistenza da altri dispositivi.

Moderazione delle interruzioni

La moderazione delle interruzioni è una tecnica che riduce il numero di interruzioni generate da un dispositivo aggregandole o ritardandole. Lo scopo della moderazione delle interruzioni è migliorare le prestazioni del sistema riducendo il sovraccarico associato alla gestione di un numero elevato di interruzioni. Troppe interruzioni aumentano l'utilizzo della CPU, influendo negativamente sulil throughput, mentre un numero insufficiente di interruzioni aumenta la latenza.

Moderazione dinamica delle interruzioni

La moderazione dinamica delle interruzioni è una forma avanzata di moderazione delle interruzioni che regola dinamicamente la frequenza di interruzione in base al carico del sistema e ai modelli di traffico correnti. Ha l'obiettivo di trovare un equilibrio tra la riduzione del sovraccarico delle interruzioni e dei pacchetti al secondo e la larghezza di banda.

> **Note**
>
> La moderazione dinamica delle interruzioni è abilitata per impostazione predefinita in alcune AMI (ma può essere abilitata o disabilitata in tutte le AMI).

Per ridurre al minimo la latenza di rete, potrebbe essere necessario disabilitare la moderazione delle interruzioni. Tuttavia, ciò può anche aumentare il sovraccarico dato dall'elaborazione delle interruzioni. È importante trovare il giusto equilibrio tra riduzione della latenza e riduzione al minimo del sovraccarico. I comandi `ethtool` possono aiutarti a configurare la moderazione delle interruzioni. Per impostazione predefinita, `rx-usecs` è impostato su `20` e `tx-usecs` è impostato su `64`.

Per ottenere la configurazione di modifica dell'interruzione corrente, utilizza il comando seguente.

```
[ec2-user ~]$ ethtool -c interface | egrep "rx-usecs:|tx-usecs:|Adaptive RX"
Adaptive RX: on  TX: off
rx-usecs: 20
tx-usecs: 64
```

Per disabilitare la moderazione dell'interruzione e la moderazione dinamica dell'interruzione, utilizza il comando seguente.

```
[ec2-user ~]$ sudo ethtool -C interface adaptive-rx off rx-usecs 0 tx-usecs 0
```

Considerazioni sul sistema Nitro per l'ottimizzazione delle prestazioni

Il sistema Nitro è una raccolta di componenti hardware e software AWS creati per consentire alte prestazioni, alta disponibilità e alta sicurezza. Inoltre, Nitro System fornisce funzionalità simili a bare metal che eliminano gli impegni di virtualizzazione e supportano i carichi di lavoro che richiedono accesso completo per l'hosting di hardware. Per ulteriori informazioni dettagliate, consulta Nitro System AWS.

Tutti i tipi di istanze EC2 della generazione attuale eseguono l'elaborazione dei pacchetti di rete su schede Nitro EC2. Questo argomento illustra la gestione di pacchetti di alto livello sulla scheda Nitro, gli aspetti comuni dell'architettura e della configurazione di rete che influiscono sulle prestazioni di gestione dei pacchetti e le azioni che si possono intraprendere per ottenere le massime prestazioni per le istanze basate su Nitro.

Le schede Nitro gestiscono tutte le interfacce di input e output (I/O), come quelle necessarie per i Virtual Private Cloud (VPC). Per tutti i componenti che inviano o ricevono informazioni sulla rete, le schede Nitro fungono da dispositivo informatico autonomo per il I/O traffico fisicamente separato dalla scheda madre del sistema su cui vengono eseguiti i carichi di lavoro dei clienti.

Flusso di pacchetti di rete sulle schede Nitro

Le istanze EC2 basate sul sistema Nitro dispongono di funzionalità di accelerazione hardware che consentono un'elaborazione più rapida dei pacchetti, misurata in base al throughput dei pacchetti al secondo (PPS). Quando una scheda Nitro esegue la valutazione iniziale di un nuovo flusso, salva le informazioni condivise per tutti i pacchetti del flusso, come i gruppi di sicurezza, gli elenchi di controllo degli accessi e le voci della tabella di routing. Quando elabora pacchetti aggiuntivi per lo stesso flusso, può utilizzare le informazioni salvate per ridurre il sovraccarico di tali pacchetti.

La velocità di connessione è misurata in base alla metrica delle connessioni al secondo (CPS). Ogni nuova connessione richiede un sovraccarico di elaborazione aggiuntivo che deve essere tenuto in considerazione nelle stime di capacità del carico di lavoro. È importante considerare sia le metriche CPS che PPS durante la progettazione dei carichi di lavoro.

Come viene stabilita una connessione

Quando viene stabilita una connessione tra un'istanza basata su Nitro e un altro endpoint, la scheda Nitro valuta l'intero flusso per il primo pacchetto inviato o ricevuto tra i due endpoint. Per i pacchetti successivi dello stesso flusso, generalmente non è necessaria una rivalutazione completa. Tuttavia, ci sono alcune eccezioni. Per ulteriori informazioni sulle eccezioni, consulta Pacchetti che non utilizzano l'accelerazione hardware.

Le seguenti proprietà definiscono i due endpoint e il flusso di pacchetti tra di loro. Queste cinque proprietà insieme sono note come flusso a 5 tuple.

- IP di origine
- Porta sorgente
- IP di destinazione
- Porta di destinazione
- Protocollo di comunicazione

La direzione del flusso di pacchetti è nota come ingresso (in entrata) e uscita (in uscita). Le seguenti descrizioni generali riassumono il flusso di pacchetti di rete end-to-end.

- Ingresso: quando una scheda Nitro gestisce un pacchetto di rete in entrata, valuta il pacchetto rispetto alle regole del firewall stateful e agli elenchi di controllo degli accessi. Tiene traccia della connessione, la misura ed esegue altre azioni, a seconda dei casi. Poi inoltra il pacchetto alla sua destinazione sulla CPU host.
- Uscita: quando una scheda Nitro gestisce un pacchetto di rete in uscita, cerca la destinazione di interfaccia remota, valuta varie funzioni VPC, applica limiti di velocità ed esegue altre azioni pertinenti. Poi inoltra il pacchetto alla sua prossima destinazione dell'hopping sulla rete.

Progetta la tua rete per ottenere prestazioni ottimali

Per sfruttare le funzionalità prestazionali del sistema Nitro, devi capire quali sono le esigenze di elaborazione di rete e in che modo tali esigenze influiscono sul carico di lavoro delle risorse Nitro.

Quindi puoi progettare per ottenere prestazioni ottimali per il tuo panorama di rete. Le impostazioni dell'infrastruttura e la progettazione e configurazione del carico di lavoro delle applicazioni possono influenzare l'elaborazione dei pacchetti e le velocità di connessione. Ad esempio, se l'applicazione ha un'elevata velocità di creazione delle connessioni, come un servizio DNS, un firewall o un router virtuale, avrà meno possibilità di sfruttare l'accelerazione hardware che si verifica solo dopo aver stabilito la connessione.

Puoi configurare le impostazioni dell'applicazione e dell'infrastruttura per snellire i carichi di lavoro e migliorare le prestazioni di rete. Tuttavia, non tutti i pacchetti sono idonei all'accelerazione. Il sistema Nitro utilizza l'intero flusso di rete per nuove connessioni e per pacchetti non idonei all'accelerazione.

La parte restante di questa sezione si concentrerà sulle considerazioni relative alla progettazione di applicazioni e infrastruttura per aiutare a garantire che i pacchetti fluiscano il più possibile all'interno del percorso accelerato.

Considerazioni sulla progettazione di rete per il sistema Nitro

Quando si configura il traffico di rete per la tua istanza, occorre considerare molti aspetti che possono influenzare le prestazioni del PPS. Una volta stabilito un flusso, la maggior parte dei pacchetti regolarmente in entrata o uscita sono idonei all'accelerazione. Tuttavia, vi sono alcune eccezioni per garantire che i progetti dell'infrastruttura e i flussi di pacchetti continuino a soddisfare gli standard del protocollo.

Per ottenere le migliori prestazioni dalla tua scheda Nitro, occorre considerare attentamente i pro e i contro dei seguenti dettagli di configurazione per infrastruttura e applicazioni.

Considerazioni sull'infrastruttura

La configurazione dell'infrastruttura può influire sul flusso dei pacchetti e sull'efficienza di elaborazione. L'elenco seguente include alcune importanti considerazioni.

Configurazione dell'interfaccia di rete con asimmetria

I gruppi di sicurezza utilizzano il monitoraggio delle connessioni per tracciare le informazioni sul traffico che fluisce da e verso l'istanza. Il routing asimmetrico, in cui il traffico entra in un'istanza attraverso un'interfaccia di rete ed esce da un'altra interfaccia di rete, può ridurre le prestazioni di picco che un'istanza può raggiungere se i flussi vengono tracciati. Per ulteriori informazioni sul tracciamento delle connessioni dei gruppi di sicurezza, sulle connessioni non tracciate e sulle connessioni tracciate automaticamente, consulta Monitoraggio della connessione al gruppo di sicurezza Amazon EC2.

Driver di rete

I driver di rete vengono aggiornati e rilasciati periodicamente. Se i driver non sono aggiornati, ciò può influire in modo significativo sulle prestazioni. Mantieni aggiornati i driver per assicurarti di avere le patch più recenti e di poter sfruttare i miglioramenti delle prestazioni, come la funzionalità di percorso accelerato disponibile solo per i driver di ultima generazione. I driver precedenti non supportano la funzionalità di percorso accelerato.

Per sfruttare la funzionalità di percorso accelerato, ti consigliamo di installare il driver ENA più recente sulle tue istanze.

Istanze Linux – Driver ENA Linux 2.2.9 o versione successiva. Per installare o aggiornare il driver ENA Linux dal GitHub repository Amazon Drivers, consulta la sezione sulla compilazione dei driver del file readme.

Istanze Windows – Driver ENA Windows 2.0.0 o versione successiva. Per installare o aggiornare il driver ENA Windows, consulta Installa il driver ENA su istanze EC2 Windows.

Distanza tra endpoint

Una connessione tra due istanze nella stessa zona di disponibilità può elaborare più pacchetti al secondo rispetto a una connessione tra regioni per via della finestra TCP a livello di applicazione, che determina la quantità di dati che possono essere trasmessi in un dato momento. Le lunghe distanze tra le istanze aumentano la latenza e diminuiscono il numero di pacchetti che gli endpoint possono elaborare.

Limite di coda di byte (BQL)

BQL è una funzionalità che limita il numero di byte passati alla scheda Nitro per ridurre la coda. BQL è disabilitato per impostazione predefinita nei driver ENA, nei sistemi operativi Amazon Linux e nella maggior parte delle distribuzioni Linux. Se BQL e l'override del proxy a frammenti sono entrambi abilitati, ciò può comportare limitazioni delle prestazioni vincolando il numero di byte passati a Nitro prima che tutti i frammenti vengano elaborati.

Considerazioni sulla progettazione delle applicazioni

Vi sono alcuni aspetti della progettazione e della configurazione delle applicazioni che possono influire sull'efficienza di elaborazione. L'elenco seguente include alcune importanti considerazioni.

Dimensioni del pacchetto

Pacchetti di dimensioni maggiori possono aumentare il throughput dei dati che un'istanza è in grado di inviare e ricevere sulla rete. Amazon EC2 supporta frame jumbo da 9.001 byte, ma altri servizi possono imporre limiti diversi. Pacchetti di dimensioni minori possono aumentare la velocità di elaborazione dei pacchetti, ma ciò può ridurre la larghezza di banda massima ottenuta quando il numero di pacchetti supera le tolleranze PPS.

Se la dimensione di un pacchetto supera l'unità di trasmissione massima (MTU) di un hop di rete, un router lungo il percorso potrebbe frammentarlo. I frammenti di pacchetto risultanti sono considerati eccezioni e di norma vengono elaborati alla velocità standard (non accelerata). Ciò può causare variazioni nelle prestazioni. Tuttavia, puoi escludere il comportamento standard per i pacchetti frammentati in uscita con l'impostazione della modalità proxy a frammenti. Per ulteriori informazioni, consulta Massimizza le prestazioni di rete sul sistema Nitro. Consigliamo di valutare la topologia per la configurazione della MTU.

Compromessi del protocollo

I protocolli affidabili come TCP hanno un sovraccarico maggiore rispetto ai protocolli inaffidabili come UDP. Il minore sovraccarico e l'elaborazione di rete semplificata per il protocollo di trasporto UDP possono comportare un tasso di PPS più elevato, ma a scapito di una fornitura affidabile dei pacchetti. Se la fornitura affidabile dei pacchetti non è fondamentale per la tua applicazione, UDP potrebbe essere una buona opzione.

Micro-bursting

Micro-bursting si verifica quando il traffico supera le tolleranze per brevi periodi di tempo anziché essere distribuito uniformemente. Ciò si verifica in genere su una scala di microsecondi.

Ad esempio, supponiamo di avere un'istanza in grado di inviare fino a 10 Gbps e che l'applicazione invii tutti i 10 Gb in mezzo secondo. Questo micro-burst supera la tolleranza consentita durante il primo mezzo secondo e non lascia nulla per il resto del secondo. Anche se hai inviato 10 Gb nell'arco di tempo di 1 secondo, le tolleranze nel primo mezzo secondo possono far sì che i pacchetti vengano messi in coda o eliminati.

Puoi utilizzare uno strumento di pianificazione di rete come Linux Traffic Control per aiutare a velocizzare il throughput ed evitare che i pacchetti vengano messi in coda o persi a causa del micro-bursting.

Numero di flussi

Un singolo flusso è limitato a 5 Gbps a meno che non si trovi all'interno di un gruppo di posizionamento cluster che supporta fino a 10 Gbps o se utilizzi ENA Express, che supporta fino a 25 Gbps.

Allo stesso modo, una scheda Nitro può elaborare più pacchetti su molteplici flussi invece di utilizzare un singolo flusso. Per raggiungere la massima velocità di elaborazione dei pacchetti per istanza, consigliamo almeno 100 flussi su istanze con una larghezza di banda aggregata pari o superiore a 100 Gbps. Con l'aumento delle capacità di larghezza di banda aggregata, aumenta anche il numero di flussi necessari per raggiungere le velocità di elaborazione di picco. Il benchmarking aiuta a determinare la configurazione necessaria per raggiungere le velocità di picco sulla rete.

Code per Adattatore elastico di rete (ENA)

ENA (Elastic Network Adapter) utilizza più code di ricezione (Rx) e trasmissione (Tx) (code ENA) per migliorare le prestazioni e la scalabilità della rete sulle istanze EC2. Queste code gestiscono in modo efficiente il traffico di rete mediante il bilanciamento del carico di dati inviati e ricevuti tra le code disponibili.

Per ulteriori informazioni, consulta the section called "Code ENA".

Sovraccarico di elaborazione delle funzionalità

Funzionalità come Traffic Mirroring ed ENA Express possono aumentare il sovraccarico di elaborazione, il che può ridurre le prestazioni assolute di elaborazione dei pacchetti. Puoi limitare l'uso delle funzionalità o disabilitarle per aumentare la velocità di elaborazione dei pacchetti.

Monitoraggio della connessione per mantenere lo stato

I gruppi di sicurezza utilizzano il monitoraggio delle connessioni per archiviare le informazioni sul traffico da e verso l'istanza. Il tracciamento delle connessioni applica regole a ogni singolo flusso di traffico di rete per stabilire se il traffico è consentito o negato. La scheda Nitro usa il tracciamento del flusso per mantenere lo stato del flusso. Man mano che vengono applicate più regole del gruppo di sicurezza, è necessario più lavoro per valutare il flusso.

> **Note**
>
> Non vengono monitorati tutti i flussi di traffico di rete. Se una regola del gruppo di sicurezza è configurata con Connessioni non tracciate, non è necessario alcun lavoro

aggiuntivo, ad eccezione delle connessioni che vengono tracciate automaticamente per garantire un routing simmetrico in presenza di molteplici percorsi di risposta validi.

Pacchetti che non utilizzano l'accelerazione hardware

Non tutti i pacchetti possono sfruttare l'accelerazione hardware. La gestione di queste eccezioni comporta un sovraccarico di elaborazione, necessario per garantire l'integrità dei flussi di rete. I flussi di rete devono soddisfare in modo affidabile gli standard del protocollo, conformarsi alle modifiche nella progettazione del VPC ed effettuare il routing dei pacchetti solo verso destinazioni consentite. Tuttavia, il sovraccarico riduce le prestazioni.

Frammenti di pacchetti

Come indicato nella sezione Considerazioni sull'applicazione, i frammenti di pacchetti derivanti da pacchetti che superano l'MTU di rete vengono gestiti di norma come eccezioni e non possono sfruttare l'accelerazione hardware. Tuttavia, puoi aggirare i limiti dei frammenti in uscita con la modalità proxy a frammenti, a seconda della versione del driver. Per ulteriori informazioni, consulta le azioni che puoi intraprendere nella sezione Massimizza le prestazioni di rete sul sistema Nitro.

Connessioni inattive

Quando una connessione non ha attività per un certo periodo di tempo, anche se non ha raggiunto il limite di timeout, il sistema può sottoporla a un abbassamento della priorità. Quindi, se i dati arrivano dopo l'abbassamento della priorità della connessione, il sistema deve gestirli come un'eccezione per riconnettersi.

Per gestire le connessioni, puoi utilizzare i timeout di tracciamento delle connessioni per chiudere le connessioni inattive. Puoi anche utilizzare i keepalive TCP per mantenere aperte le connessioni inattive. Per ulteriori informazioni, consulta Timeout di tracciamento delle connessioni inattive.

Mutazione del VPC

Gli aggiornamenti ai gruppi di sicurezza, alle tabelle di routing e agli elenchi di controllo degli accessi devono essere tutti rivalutati nel percorso di elaborazione per garantire che le voci route e le regole dei gruppi di sicurezza continuino ad essere applicate come previsto.

Flussi ICMP

Internet Control Message Protocol (ICMP) è un protocollo a livello di rete utilizzato dai dispositivi di rete per diagnosticare i problemi di comunicazione di rete. Questi pacchetti usano sempre il flusso completo.

Flussi L2 asimmetrici

NitroV3 e le piattaforme precedenti non utilizzano l'accelerazione hardware per il traffico tra due ENI nella stessa sottorete, in cui una ENI utilizza il router gateway predefinito e l'altra non lo utilizza. Le piattaforme NitroV4 e successive utilizzano l'accelerazione hardware in questo scenario. Per prestazioni migliori su piattaforme NitroV3 o precedenti, assicurati che il router gateway predefinito utilizzato corrisponda a entrambe le ENI o che tali ENI si trovino in sottoreti diverse.

Massimizza le prestazioni di rete sul sistema Nitro

Puoi massimizzare le prestazioni di rete sul sistema Nitro modificando le impostazioni di rete.

Argomenti

- Considerazioni
- Ottimizzazione delle prestazioni PPS
- Configura l'allocazione delle code ENA
- Monitora le prestazioni sulle istanze Linux

Considerazioni

Prima di prendere decisioni di progettazione o modificare le impostazioni di rete sulla tua istanza, ti consigliamo di attenerti alla seguente procedura per aiutarti a ottenere il miglior risultato:

1. Scopri i pro e i contro delle azioni che puoi intraprendere per migliorare le prestazioni esaminando Considerazioni sulla progettazione di rete per il sistema Nitro.

   Per ulteriori considerazioni e best practice per la configurazione dell'istanza su Linux, consulta la Guida alle best practice e all'ottimizzazione delle prestazioni dei driver ENA Linux su. GitHub
2. Effettua un benchmark dei tuoi carichi di lavoro con il numero di flussi attivi di picco per determinare un riferimento per le prestazioni delle tue applicazioni. Con una linea di base delle prestazioni, puoi testare le variazioni nelle impostazioni o nella progettazione dell'applicazione

per capire quali considerazioni avranno l'impatto maggiore, soprattutto se prevedi di aumentare orizzontalmente o aumentare verticalmente.

Ottimizzazione delle prestazioni PPS

L'elenco seguente contiene le azioni che puoi intraprendere per ottimizzare le prestazioni del PPS, a seconda delle esigenze del sistema.

- Riduci la distanza fisica tra due istanze. Quando le istanze di invio e ricezione si trovano nella stessa zona di disponibilità o utilizzano gruppi di posizionamento cluster, puoi ridurre il numero di hop necessari a un pacchetto per viaggiare da un endpoint all'altro.
- Utilizza Connessioni non tracciate.
- Utilizza il protocollo UDP per il traffico di rete.
- Per le istanze EC2 con larghezza di banda aggregata pari o superiore a 100 Gbps, distribuisci il carico di lavoro su 100 o più flussi individuali per distribuire il lavoro in modo uniforme sulla scheda Nitro.
- Per superare il limite PPS dei frammenti in uscita sulle istanze EC2, puoi abilitare la modalità proxy a frammenti (in funzione della versione del driver). Questa impostazione consente di valutare i pacchetti frammentati nel percorso di elaborazione, superando in tal modo il limite PPS in uscita di 1.024. Durante il caricamento del driver, esegui uno dei seguenti comandi per abilitare o disabilitare la modalità proxy a frammenti:

  Abilita la modalità proxy a frammenti

  ```
  sudo insmod ena.ko enable_frag_bypass=1
  ```

  Disabilita la modalità proxy a frammenti

  ```
  sudo insmod ena.ko enable_frag_bypass=0
  ```

Configura l'allocazione delle code ENA

Sui tipi di istanze supportati, puoi allocare dinamicamente queste code tra interfacce di rete elastiche (ENI). L'allocazione flessibile delle code ENA ottimizza la distribuzione delle risorse, consentendo il massimo utilizzo della vCPU. I carichi di lavoro ad alte prestazioni di rete richiedono in genere molteplici code ENA. Per ulteriori informazioni, consulta Code ENA.

Monitora le prestazioni sulle istanze Linux

Puoi utilizzare le metriche Ethtool sulle istanze Linux per monitorare gli indicatori delle prestazioni di rete delle istanze, come larghezza di banda, velocità dei pacchetti e tracciamento della connessione. Per ulteriori informazioni, consulta Monitoraggio delle prestazioni di rete per le impostazioni ENA dell'istanza EC2.

Ottimizza le prestazioni di rete sulle istanze Windows EC2

Per ottenere le massime prestazioni di rete sulle istanze Windows con reti avanzate, potrebbe essere necessario modificare la configurazione del sistema operativo predefinita. Si consiglia di apportare le seguenti modifiche alla configurazione per le applicazioni che richiedono prestazioni di rete elevate. Altre ottimizzazioni (come ad esempio l'attivazione dell'offload del checksum e l'abilitazione di RSS) sono già configurate sulle AMI ufficiali di Windows.

> **Note**
>
> TCP chimney offload dovrebbe essere disabilitato nella maggior parti dei casi d'uso ed è stato reso obsoleto con Windows Server 2016.

Oltre a queste ottimizzazioni del sistema operativo, devi anche considerare l'unità di trasmissione massima (MTU) del traffico di rete e regolare in base al carico di lavoro e all'architettura di rete. Per ulteriori informazioni, consulta Unità massima di trasmissione (MTU) di rete per istanza EC2.

AWS misura regolarmente le latenze medie di andata e ritorno tra le istanze lanciate in un gruppo di collocamento del cluster di 50us e le latenze di coda di 200us al 99,9 percentile. Se le tue applicazioni richiedono costantemente latenze basse, consigliamo di utilizzare l'ultima versione dei driver ENA nelle istanze basate sul sistema Nitro con prestazioni fisse.

Configura l'affinità della CPU con Receive Side Scaling

Receive Side Scaling (RSS) viene utilizzato per distribuire il carico della CPU del traffico di rete su più processori. Come impostazione predefinita, le AMI Amazon Windows ufficiali sono configurate con RSS abilitato. Le interfacce di rete elastiche ENA forniscono fino a otto code RSS. Definendo l'affinità dei CPU per le code RSS, nonché per altri processi del sistema, è possibile distribuire il carico di lavoro della CPU su sistemi multi-core e consentire l'elaborazione di più traffico di rete. Sui tipi di istanza con più di 16 vCPU, si consiglia di utilizzare il `Set-NetAdapterRSS` PowerShell cmdlet,

che esclude manualmente il processore di avvio (processore logico 0 e 1 quando l'hyper-threading è abilitato) dalla configurazione RSS per tutte le interfacce di rete elastiche, per evitare conflitti con vari componenti di sistema.

Windows è compatibile con hyperthreading e garantisce che le code RSS di una singola scheda di interfaccia di rete vengano sempre posizionate su diversi core fisici. Pertanto, a meno che l'hyper-threading non sia disabilitato, per evitare completamente il conflitto con altre NIC, distribuisci la configurazione RSS di ciascuna NIC tra un intervallo di 16 processori logici. Il `Set-NetAdapterRss` cmdlet consente di definire l'intervallo per NIC di processori logici validi definendo i valori di,, e (opzionale). BaseProcessorGroup BaseProcessorNumber MaxProcessingGroup MaxProcessorNumber NumaNode Se non ci sono abbastanza core fisici per eliminare completamente conflitti inter-NIC, minimizza le gamme in sovrapposizione o riduci il numero di processori logici nelle gamme di interfaccia elastica di rete in base al carico di lavoro previsto dell'interfaccia (in altre parole, un'interfaccia di rete amministrativa di basso volume potrebbe non aver bisogno di così tante code RSS assegnate). Inoltre, come indicato precedentemente, i vari componenti devono essere eseguiti su CPU 0 e quindi è consigliabile escluderla da tutte le configurazioni RSS quando è disponibile un numero sufficiente di vCPU.

Ad esempio, quando sono presenti tre interfacce elastiche di rete su un'istanza a 72 vCPU con due nodi NUMA con l'hyper-threading abilitato, i comandi seguenti distribuiscono il carico di rete tra le due CPU senza sovrapposizione e impediscono completamente l'utilizzo del core 0.

```
Set-NetAdapterRss -Name NIC1 -BaseProcessorGroup 0 -BaseProcessorNumber 2 -
MaxProcessorNumber 16
Set-NetAdapterRss -Name NIC2 -BaseProcessorGroup 1 -BaseProcessorNumber 0 -
MaxProcessorNumber 14
Set-NetAdapterRss -Name NIC3 -BaseProcessorGroup 1 -BaseProcessorNumber 16 -
MaxProcessorNumber 30
```

Nota che queste impostazioni sono persistenti per ogni adattatore di rete. Se un'istanza viene ridimensionata a uno con un numero diverso di vCPU, devi rivalutare la configurazione RSS per ogni interfaccia elastica di rete abilitata. La documentazione Microsoft completa per il cmdlet è disponibile qui:. Set-NetAdapterRss

Nota speciale per i carichi di lavoro SQL: Ti consigliamo inoltre di rivedere le impostazioni di affinità dei I/O thread insieme alla configurazione RSS dell'interfaccia di rete elastica per ridurre al minimo i conflitti di rete per I/O le stesse CPU. Consulta Server configuration: affinity mask.

Elastic Fabric Adapter per AI/ML carichi di lavoro HPC su Amazon EC2

Elastic Fabric Adapter (EFA) è un dispositivo di rete che è possibile collegare all'istanza Amazon EC2 per accelerare le applicazioni di intelligenza artificiale (IA), machine learning (ML) e calcolo ad alte prestazioni (HPC). EFA consente di ottenere le prestazioni applicative di un cluster locale AI/ML o HPC, con la scalabilità, la flessibilità e l'elasticità fornite dal cloud. AWS

EFA garantisce valori di latenza più bassi e coerenti e un throughput più elevato rispetto al trasporto TCP generalmente utilizzato nei sistemi HPC basati su cloud. Migliora le prestazioni della comunicazione tra istanze, fondamentale per la scalabilità e le applicazioni HPC. AI/ML È ottimizzato per funzionare sull'infrastruttura di AWS rete esistente e può essere scalato in base ai requisiti dell'applicazione.

EFA si integra con Libfabric e supporta Nvidia Collective Communications Library (NCCL) e NVIDIA Inference Xfer Library (NIXL) per applicazioni AI e ML, Open MPI 4.1 e versioni successive e Intel MPI 2019 Update 5 e versioni successive per le applicazioni HPC. NCCL e MPI si integrano con Libfabric 1.7.0 e versioni successive. NIXL si integra con Libfabric 1.21.0 e versioni successive.

EFA supporta la scrittura RDMA (accesso diretto alla memoria remota) sulla maggior parte dei tipi di istanze supportati con Nitro versione 4 e successive. La lettura RDMA è supportata su tutte le istanze con Nitro versione 4 e successive. Per ulteriori informazioni, consulta Tipi di istanze supportati.

Indice

- Nozioni di base su EFA
- Librerie e interfacce supportate
- Tipi di istanze supportati
- Sistemi operativi supportati
- Limitazioni di EFA
- Prezzi EFA
- Nozioni di base su EFA e MPI per i carichi di lavoro HPC su Amazon EC2
- Nozioni di base su EFA e NCCL per i carichi di lavoro ML su Amazon EC2
- Inizia a usare EFA e NIXL per i carichi di lavoro di inferenza su Amazon EC2
- Ottimizzare la larghezza di banda della rete sulle istanze Amazon EC2 con più schede di rete
- Installare il software EFA in un contenitore

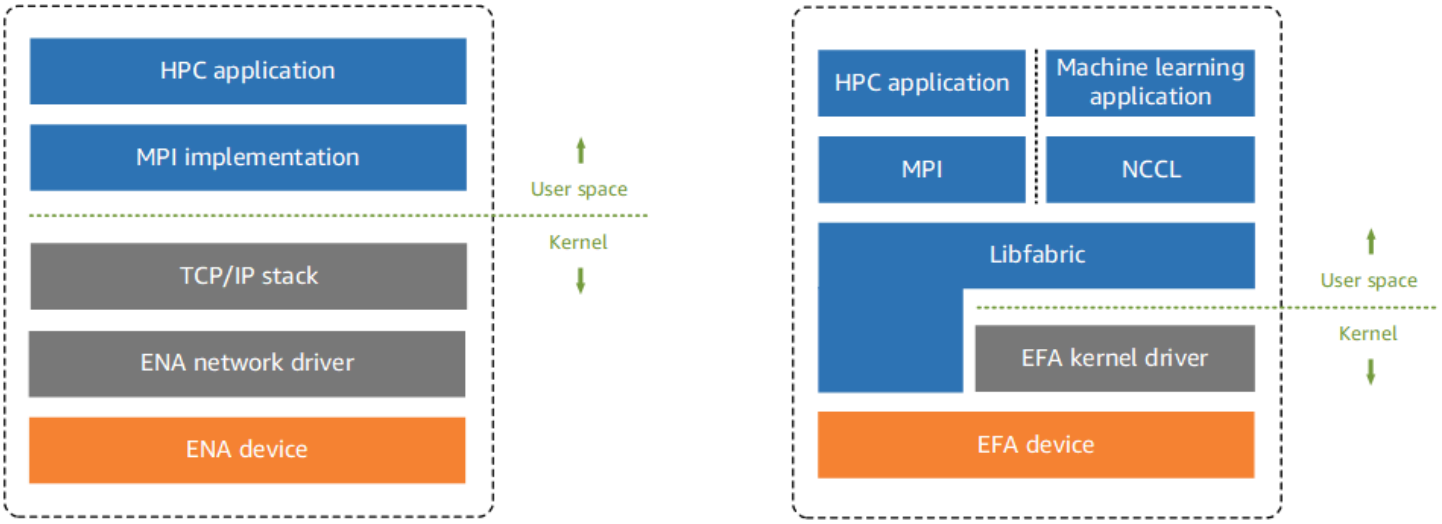
- Creare e collegare un Elastic Fabric Adapter a un'istanza Amazon EC2
- Scollegare ed eliminare un EFA da un'istanza Amazon EC2
- Monitorare un Elastic Fabric Adapter in Amazon EC2
- Verifica del programma di installazione EFA utilizzando un checksum
- Note sulla versione di Elastic Fabric Adapter

Nozioni di base su EFA

Un dispositivo EFA può essere collegato a un'istanza EC2 in due modi:

1. Tramite un'interfaccia EFA tradizionale, chiamata anche EFA con ENA, che crea sia un dispositivo EFA che un dispositivo ENA.
2. Utilizzando un' EFA-only interfaccia, che crea solo il dispositivo EFA.

Il dispositivo EFA offre funzionalità come il controllo integrato OS-bypass e la congestione tramite il protocollo Scalable Reliable Datagram (SRD). Le funzionalità del dispositivo EFA offrono una capacità di trasporto affidabile e a bassa latenza che consente all'interfaccia EFA di fornire migliori prestazioni applicative per le applicazioni HPC e ML su Amazon EC2. Il dispositivo ENA, invece, offre una rete IP tradizionale. Per indicazioni sulla configurazione dell'istanza da utilizzare in base al caso d'uso, consulta. Ottimizzare la larghezza di banda della rete



Traditional HPC software stack in EC2

HPC software stack in EC2 with EFA

Tradizionalmente, AI/ML le applicazioni utilizzano NCCL e NIXL (per l'inferenza disaggregata). Le applicazioni HPC utilizzano la Message Passing Interface (MPI) per interfacciarsi con il trasporto di

rete del sistema. Nel AWS cloud, ciò significa che le applicazioni si interfacciano con NCCL, NIXL o MPI, che utilizzano quindi lo TCP/IP stack del sistema operativo e il driver del dispositivo ENA per consentire la comunicazione di rete tra le istanze.

Con un' EFA-only interfaccia o EFA (EFA con ENA) tradizionale, le AI/ML applicazioni utilizzano NCCL e NIXL (per l'inferenza disaggregata). Le applicazioni HPC utilizzano MPI per interfacciarsi direttamente con l'API Libfabric. L'API di Libfabric bypassa il kernel del sistema operativo e comunica direttamente con il dispositivo EFA per immettere in rete i pacchetti. Ciò riduce il sovraccarico AI/ML e consente alle applicazioni HPC di funzionare in modo più efficiente.

> **Note**
>
> Libfabric è un componente fondamentale del framework OpenFabrics Interfaces (OFI), che definisce ed esporta l'API dello spazio utente di OFI. Per ulteriori informazioni, consulta il sito Web Libfabric. OpenFabrics

Differenze tra ENA, EFA e EFA-only interfacce di rete

Amazon EC2 offre due tipi di interfacce di rete:

- Le interfacce ENA offrono tutte le tradizionali funzionalità di rete e routing IP necessarie per supportare la rete IP per un VPC. Per ulteriori informazioni, consulta Abilitazione delle reti avanzate con ENA su istanze EC2.
- Le interfacce EFA (EFA con ENA) offrono sia il dispositivo ENA per le reti IP sia il dispositivo EFA per le comunicazioni a bassa latenza e a throughput elevato.
- EFA-onlyle interfacce supportano solo le funzionalità del dispositivo EFA, senza il dispositivo ENA per le reti IP tradizionali.

La tabella seguente fornisce un confronto tra ENA, EFA e EFA-only le interfacce di rete.

	ENA	EFA (EFA con ENA)	EFA-only
Supporto della funzionalità di rete IP	Sì	Sì	No

	ENA	EFA (EFA con ENA)	EFA-only
Possibilità di assegnare indirizzi IPv4 e IPv6	Sì	Sì	No
Possibilità di utilizzo come interfacc ia di rete principale per un'istanza	Sì	Sì	No
Conta per il limite di collegamento ENI dell'ista nza	Sì	Sì	Sì
Supporto dei tipi di istanze	Supportato su tutti i tipi di istanze Nitro-based	Tipi di istanze supportati	Tipi di istanze supportati
Denominaz ione dei parametri nelle API EC2	`interface`	`efa`	`efa-only`
Denominaz ione dei campi nella console EC2	Nessuna selezione	EFA con ENA	EFA-only

Librerie e interfacce supportate

Gli EFA supportano le seguenti interfacce e librerie:

- Apri MPI 4.1 e versioni successive
- Intel MPI 2019 aggiornamento 5 e successivi
- NVIDIA Collective Communications Library (NCCL) 2.4.2 e versioni successive
- NVIDIA Inference Xfer Library (NIXL) 1.0.0 e versioni successive
- AWS Neuron SDK versione 2.3 e successive

Tipi di istanze supportati

Tutti i seguenti tipi di istanza supportano EFA. Inoltre, le tabelle indicano il supporto per la lettura RDMA e la scrittura RDMA per i tipi di istanza.

Nitro v6 (EFA v4)

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
Uso generico		
m8a.48xlarge	Sì	Sì
m8a.metal-48xl	Sì	Sì
m8azn. 24x large	Sì	Sì
m8azn.metallo-24xl	Sì	Sì
m8 gb. 16x di grandi dimensioni	Sì	Sì
m8 gb.24x di grandi dimensioni	Sì	Sì
m8 gb.48x di grandi dimensioni	Sì	Sì
8 gb. in metallo - 24xl	Sì	Sì
m8 gb.metal-48xl	Sì	Sì
m8gn.16x grande	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
m8gn.24x grande	Sì	Sì
m8gn.48x grande	Sì	Sì
m8gn.metallo-24xl	Sì	Sì
m8gn.metallo-48xl	Sì	Sì
m8i.48xlarge	Sì	Sì
m8i.96xlarge	Sì	Sì
m8i.metal-48xl	Sì	Sì
m8i.metal-96xl	Sì	Sì
m8id.48x grande	Sì	Sì
m8id.96xlarge	Sì	Sì
m8id.metallo-48xl	Sì	Sì
m8id.metallo-96xl	Sì	Sì
m 8 pollici 48 x grande	Sì	Sì
m 8 pollici 96 x grande	Sì	Sì
metallo da 8 pollici - 48 xl	Sì	Sì
Metallo-96xl da 8 pollici	Sì	Sì
m8idn.48x grande	Sì	Sì
m8idn.96xlarge	Sì	Sì
m8idn.metallo-48xl	Sì	Sì
m8idn.metallo-96xl	Sì	Sì
m8ib.48x grande	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
m8ib.96x grande	Sì	Sì
m8ib.metallo-48xl	Sì	Sì
m8ib.metallo-96xl	Sì	Sì
m8idb.48xlarge	Sì	Sì
m8idb.96xlarge	Sì	Sì
m8idb.metallo-48xl	Sì	Sì
m8idb.metallo-96xl	Sì	Sì
m 9g. 48x grande	Sì	Sì
9g. Metallo-48xl	Sì	Sì
m 9 g. 48x grande	Sì	Sì
m9gd.metallo-48xl	Sì	Sì
Ottimizzata per il calcolo		
c8a.48xlarge	Sì	Sì
c8a.metallo-48xl	Sì	Sì
c8gb. 16x grande	Sì	Sì
c8 gb.24x grande	Sì	Sì
c8 gb.48x grande	Sì	Sì
c8gb.metallo-24xl	Sì	Sì
c8gb.metallo-48xl	Sì	Sì
c8gn.16xlarge	Sì	Sì
c8gn.24xlarge	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
c8gn.48xlarge	Sì	Sì
c8gn.metal-24xl	Sì	Sì
c8gn.metal-48xl	Sì	Sì
c8i.48x grande	Sì	Sì
c8i.96xlarge	Sì	Sì
c8i.metallo-48xl	Sì	Sì
c8i.metal-96xl	Sì	Sì
c8id.48x grande	Sì	Sì
c8id.96xlarge	Sì	Sì
c8id.metallo-48xl	Sì	Sì
c8id.metallo-96xl	Sì	Sì
c8 pollici. 48x grande	Sì	Sì
c8 pollici 96 x grande	Sì	Sì
Metallo da 8 pollici - 48xl	Sì	Sì
Metallo da 8 pollici - 96xl	Sì	Sì
c8ib.48x grande	Sì	Sì
c8ib.96x grande	Sì	Sì
c8ib.metallo-48xl	Sì	Sì
c8ib.metallo-96xl	Sì	Sì
c9g. 48x grande	Sì	Sì
c9g. metallo-48xl	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
c9g. 48x grande	Sì	Sì
c9gd.metallo-48xl	Sì	Sì
Ottimizzata per la memoria		
r8a.48xlarge	Sì	Sì
R8a. Metal-48xl	Sì	Sì
r8gb.16xlarge	Sì	Sì
r8gb.24xlarge	Sì	Sì
r8gb. 48x large	Sì	Sì
r8gb.metal-24xl	Sì	Sì
r8gb.metal-48xl	Sì	Sì
r8gn.16xlarge	Sì	Sì
r8gn.24xlarge	Sì	Sì
r8gn.48xlarge	Sì	Sì
r8gn.metal-24xl	Sì	Sì
r8gn.metal-48xl	Sì	Sì
r8i.48xlarge	Sì	Sì
r8i.96xlarge	Sì	Sì
r8i.metal-48xl	Sì	Sì
r8i.metal-96xl	Sì	Sì
r8id.48xlarge	Sì	Sì
r8id.96xlarge	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
r8id.metallo-48xl	Sì	Sì
r8id.metallo-96xl	Sì	Sì
r8in.48x grande	Sì	Sì
r8in.96x grande	Sì	Sì
R8 pollici in metallo - 48xl	Sì	Sì
R8in.metallo-96xl	Sì	Sì
r8idn.48xlarge	Sì	Sì
r8idn.96xlarge	Sì	Sì
r8idn.metallo-48xl	Sì	Sì
r8idn.metallo-96xl	Sì	Sì
r8ib.48x grande	Sì	Sì
r8ib.96x grande	Sì	Sì
r8ib.metallo-48xl	Sì	Sì
r8ib.metallo-96xl	Sì	Sì
r8idb.48xlarge	Sì	Sì
r8idb.96xlarge	Sì	Sì
r8idb.metallo-48xl	Sì	Sì
r8idb.metallo-96xl	Sì	Sì
r9g. 48x grande	Sì	Sì
r9g. metallo-48xl	Sì	Sì
r9gd.48x grande	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
r9gd.metallo-48xl	Sì	Sì
x8aedz.24x grande	Sì	Sì
x8aedz.metallo-24xl	Sì	Sì
x8i.48xlarge	Sì	Sì
x8i.64x grande	Sì	Sì
x8i.96x grande	Sì	Sì
x8i. Metallo - 48xl	Sì	Sì
x8i.metallo-96xl	Sì	Sì
Ottimizzata per l'archiviazione		
i8ge.48xlarge	Sì	Sì
i8ge.metal-48xl	Sì	Sì
Calcolo accelerato		
g 7.8x grande	Sì	Sì
g 7.12x grande	Sì	Sì
g 7.24x grande	Sì	Sì
g 7.48x grande	Sì	Sì
g7e.8x grande	Sì	Sì
g7e.12x grande	Sì	Sì
g7e.24x grande	Sì	Sì
g7e.48x grande	Sì	Sì
p6-b200.48xlarge	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
p6-b300.48x grande	Sì	Sì
High Performance Computing		
hpc8a.96xlarge	Sì	Sì

Nitro v5 (EFA v3)

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
Uso generico		
m8g.24xlarge	Sì	Sì
m8g.48xlarge	Sì	Sì
m8g.metal-24xl	Sì	Sì
m8g.metal-48xl	Sì	Sì
m8gd.24xlarge	Sì	Sì
m8gd.48xlarge	Sì	Sì
m8gd.metal-24xl	Sì	Sì
m8gd.metal-48xl	Sì	Sì
Ottimizzata per il calcolo		
c7gn.16xlarge	Sì	No
c7gn.metal	Sì	No
c8g.24xlarge	Sì	Sì
c8g.48xlarge	Sì	Sì
c8g.metal-24xl	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
c8g.metal-48xl	Sì	Sì
c8gd.24xlarge	Sì	Sì
c8gd.48xlarge	Sì	Sì
c8gd.metal-24xl	Sì	Sì
c8gd.metal-48xl	Sì	Sì
Ottimizzata per la memoria		
r8g.24xlarge	Sì	Sì
r8g.48xlarge	Sì	Sì
r8g.metal-24xl	Sì	Sì
r8g.metal-48xl	Sì	Sì
r8gd.24xlarge	Sì	Sì
r8gd.48xlarge	Sì	Sì
r8gd.metal-24xl	Sì	Sì
r8gd.metal-48xl	Sì	Sì
x8g.24xlarge	Sì	Sì
x8g.48xlarge	Sì	Sì
x8g.metal-24xl	Sì	Sì
x8g.metal-48xl	Sì	Sì
Ottimizzata per l'archiviazione		
i7ie.48xlarge	Sì	Sì
i7ie.metal-48xl	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
i8g.48xlarge	Sì	Sì
i8g. metallo-48xl	Sì	Sì
Calcolo accelerato		
p5en.48xlarge	Sì	Sì
p6e-gb200.36xlarge	Sì	Sì
trn 2,3 x grande	Sì	Sì
trn2.48xlarge	Sì	Sì
trn2u.48xlarge	Sì	Sì
High Performance Computing		
hpc7g.4xlarge	Sì	No
hpc7g.8xlarge	Sì	No
hpc7g.16xlarge	Sì	No

Nitro v4 (EFA v2)

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
Uso generico		
m6a.48xlarge	Sì	Sì
m6a.metal	Sì	Sì
m6i.32xlarge	Sì	Sì
m6i.metal	Sì	Sì
m6id.32xlarge	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
m6id.metal	Sì	Sì
m6idn.32xlarge	Sì	Sì
m6idn.metal	Sì	Sì
m6in.32xlarge	Sì	Sì
m6in.metal	Sì	Sì
m7a.48xlarge	Sì	Sì
m7a.metal-48xl	Sì	Sì
m7g.16xlarge	Sì	Sì
m7g.metal	Sì	Sì
m7gd.16xlarge	Sì	Sì
m7gd.metal	Sì	Sì
m7i.48xlarge	Sì	Sì
m7i.metal-48xl	Sì	Sì
Ottimizzata per il calcolo		
c6a.48xlarge	Sì	Sì
c6a.metal	Sì	Sì
c6gn.16xlarge	Sì	Sì
c6i.32xlarge	Sì	Sì
c6i.metal	Sì	Sì
c6id.32xlarge	Sì	Sì
c6id.metal	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
c6in.32xlarge	Sì	Sì
c6in.metal	Sì	Sì
c7a.48xlarge	Sì	Sì
m7a.metal-48xl	Sì	Sì
c7g.16xlarge	Sì	Sì
c7g.metal	Sì	Sì
c7gd.16xlarge	Sì	Sì
c7gd.metal	Sì	Sì
c7i.48xlarge	Sì	Sì
c7i.metal-48xl	Sì	Sì
Ottimizzata per la memoria		
r6a.48xlarge	Sì	Sì
r6a.metal	Sì	Sì
r6i.32xlarge	Sì	Sì
r6i.metal	Sì	Sì
r6id.32xlarge	Sì	Sì
r6id. Metallo	Sì	Sì
r6idn.32xlarge	Sì	Sì
r6idn.metal	Sì	Sì
r6in.32xlarge	Sì	Sì
r6in.metal	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
r7a.48xlarge	Sì	Sì
m7a.metal-48xl	Sì	Sì
r7g.16xlarge	Sì	Sì
r7g.metal	Sì	Sì
r7gd.16xlarge	Sì	Sì
r7gd.metal	Sì	Sì
r7i.48xlarge	Sì	Sì
r7i.metal-48xl	Sì	Sì
r7iz.32xlarge	Sì	Sì
r7iz.metal-32xl	Sì	Sì
u7i-6tb.112xlarge	Sì	Sì
u7i-8tb.112xlarge	Sì	Sì
u7i-12tb.224xlarge	Sì	Sì
u7in-16tb.224xlarge	Sì	Sì
u7in-24tb.224xlarge	Sì	Sì
u7in-32tb.224xlarge	Sì	Sì
u7inh-32tb.480xlarge	Sì	Sì
x2idn.32xlarge	Sì	Sì
x2idn.metal	Sì	Sì
x2iedn.32xlarge	Sì	Sì
x2iedn.metal	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
Ottimizzata per l'archiviazione		
i4i.16xlarge	Sì	Sì
i4i.32xlarge	Sì	Sì
i4i.metal	Sì	Sì
i7i.24xlarge	Sì	Sì
i7i.48xlarge	Sì	Sì
i7i.metal-48xl	Sì	Sì
im4gn.16xlarge	Sì	Sì
Calcolo accelerato		
f2.48xlarge	Sì	Sì
g6.8xlarge	Sì	Sì
g6.12xlarge	Sì	Sì
g6.16xlarge	Sì	Sì
g6.24xlarge	Sì	Sì
g6.48xlarge	Sì	Sì
g6e.8xlarge	Sì	Sì
g6e.12xlarge	Sì	Sì
g6e.16xlarge	Sì	Sì
g6e.24xlarge	Sì	Sì
g6e.48xlarge	Sì	Sì
gr6.8xlarge	Sì	Sì

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
p5.4xlarge	Sì	Sì
p5.48xlarge	Sì	Sì
p5e.48xlarge	Sì	Sì
trn1.32xlarge	Sì	Sì
trn1n.32xlarge	Sì	Sì
High Performance Computing		
hpc6a.48xlarge	Sì	Sì
hpc6id.32xlarge	Sì	Sì
hpc7a.12xlarge	Sì	Sì
hpc7a.24xlarge	Sì	Sì
hpc7a.48xlarge	Sì	Sì
hpc7a.96xlarge	Sì	Sì

Nitro v3 (EFA v1)

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
Uso generico		
m5dn.24xlarge	No	No
m5dn.metal	No	No
m5n.24xlarge	No	No
m5n.metal	No	No
m5zn.12xlarge	No	No

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
m5zn.metal	No	No
Ottimizzata per il calcolo		
c5n.9xlarge	No	No
c5n.18xlarge	No	No
c5n.metal	No	No
Ottimizzata per la memoria		
r5dn.24xlarge	No	No
r5dn.metal	No	No
r5n.24xlarge	No	No
r5n.metal	No	No
x2iezn.12xlarge	No	No
x2iezn.metal	No	No
Ottimizzata per l'archiviazione		
i3en.12xlarge	No	No
i3en.24xlarge	No	No
i3en.metal	No	No
Calcolo accelerato		
dl2q.24xlarge	No	No
g4dn.8xlarge	No	No
g4dn.12xlarge	No	No
g4dn.16xlarge	No	No

Tipo di istanza	Supporto di lettura RDMA	Supporto di scrittura RDMA
g4dn.metal	No	No
g5.8xlarge	No	No
g5.12xlarge	No	No
g5.16xlarge	No	No
g5.24xlarge	No	No
g5.48xlarge	No	No
inf1.24xlarge	No	No
p3dn.24xlarge	No	No
p4d.24xlarge	Sì	No
p4de.24xlarge	Sì	No
vt1.24xlarge	No	No
Generazione precedente		
p3dn.24xlarge	No	No

Per visualizzare i tipi di istanza disponibili che supportano gli EFA in una regione specifica

I tipi di istanza disponibili variano in base alla regione. Per visualizzare i tipi di istanza disponibili che supportano gli EFA in una regione, utilizza il comando describe-instance-types con il parametro `--region`. Includi il parametro `--filters` per assegnare i risultati ai tipi di istanza che supportano EFA e il parametro `--query` per assegnare l'output al valore di `InstanceType`.

```
aws ec2 describe-instance-types \
    --region us-east-1  \
    --filters Name=network-info.efa-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]"  \
    --output text | sort
```

Sistemi operativi supportati

Il supporto per i sistemi operativi cambia a seconda del tipo di processore. Nella tabella seguente sono indicati i sistemi operativi supportati.

Sistema operativo	Intel/AMD () tipi di istanza **x86_64**	AWS tipi di istanza Graviton (**arm64**)
Amazon Linux 2023	✓	✓
RHEL 8, 9 e 10	✓	✓
Debian 11, 12 e 13	✓	✓
Rocky Linux 8 e 9	✓	✓
Ubuntu 22.04, 24.04 e 26.04	✓	✓
SUSE Linux Enterprise 15 SP2 e versioni successive	✓	✓

> **Note**
>
> Alcuni dei sistemi operativi elencati potrebbero non essere supportati da Intel MPI. Se utilizzi Intel MPI, fai riferimento alla documentazione Intel MPI per verificare il supporto per il sistema operativo in uso.

Limitazioni di EFA

Gli EFA hanno le seguenti limitazioni:

- La scrittura RDMA non è supportata con tutti i tipi di istanze. Per ulteriori informazioni, consulta Tipi di istanze supportati.
- Il traffico EFA [1] tra P4d/P4de/DL1 istanze e altri tipi di istanze non è attualmente supportato.
- I tipi di istanza che supportano più schede di rete possono essere configurati con un EFA per scheda di rete. Tutti gli altri tipi di istanza supportati supportano solo un EFA per istanza.
- Le istanze dedicate `c7g.16xlarge`, `m7g.16xlarge` e `r7g.16xlarge`, e gli host dedicati non sono supportati quando è collegato un EFA.
- Il traffico EFA[1] non può attraversare zone di disponibilità o VPC. Questo non si applica al normale traffico IP dal dispositivo ENA di un'interfaccia EFA.
- Il traffico EFA[1] non è instradabile. Al contrario, è possibile instradare il normale traffico IP dal dispositivo ENA di un'interfaccia EFA.
- L'EFA non è supportato su. AWS Outposts
- Il dispositivo EFA di un'interfaccia EFA (EFA con ENA) è supportato su istanze Windows solo per AWS Cloud Digital Interface applicazioni basate su Software Development Kit (AWS CDI SDK). Se si collega un'interfaccia EFA (ovvero EFA con ENA) a un'istanza Windows per applicazioni non basate su CDI SDK, questa funziona come interfaccia ENA, senza le funzionalità aggiuntive del dispositivo EFA. L' EFA-only interfaccia non è supportata dalle applicazioni AWS CDI basate su Windows o Linux. Per ulteriori informazioni, consulta la Guida per l'utente del AWS Cloud Digital Interface Software Development Kit (AWS CDI SDK).

1 Il traffico EFA si riferisce al traffico trasmesso attraverso il dispositivo EFA di un EFA (EFA con ENA) o di un'interfaccia. EFA-only

Prezzi EFA

EFA è disponibile come funzionalità di rete Amazon EC2 opzionale che puoi abilitare su qualsiasi istanza supportata senza costi aggiuntivi.

Nozioni di base su EFA e MPI per i carichi di lavoro HPC su Amazon EC2

Questo tutorial ti aiuta a lanciare un EFA e un cluster di MPI-enabled istanze per carichi di lavoro HPC.

> **Note**
>
> Le istanze `u7i-12tb.224xlarge`, `u7in-16tb.224xlarge`, `u7in-24tb.224xlarge` e `u7in-32tb.224xlarge` possono eseguire fino a 128 processi MPI paralleli con Open MPI o fino a 256 processi MPI paralleli con Intel MPI.

Processi

- Fase 1: Preparare un gruppo di sicurezza EFA-enabled
- Fase 2: avviare un'istanza temporanea
- Fase 3: installare il software EFA
- Fase 4: (Facoltativo) Abilita Open MPI 5
- Fase 5: (Facoltativo) Installa Intel MPI
- Fase 6: disabilitare la protezione Ptrace
- Fase 7. Conferma dell'installazione
- Fase 8: installazione dell'applicazione HPC
- Fase 9: Creazione di un'AMI EFA-enabled
- Passaggio 10: avvia EFA-enabled le istanze in un gruppo di posizionamento del cluster
- Fase 11: terminare l'istanza temporanea
- Fase 12: abilitazione di SSH senza password

Fase 1: Preparare un gruppo di sicurezza EFA-enabled

Un EFA richiede un gruppo di sicurezza in cui sia consentito tutto il traffico in entrata e in uscita dal gruppo stesso. La procedura seguente crea un gruppo di sicurezza che consente tutto il traffico in entrata e in uscita da e verso se stesso e che consente il traffico SSH in entrata da qualsiasi indirizzo IPv4 per la connettività SSH.

> **Important**
>
> Questo gruppo di sicurezza è destinato esclusivamente a scopi di test. Per i tuoi ambienti di produzione, consigliamo di creare una regola SSH in entrata che consenta il traffico solo dall'indirizzo IP da cui ti connetti, ad esempio l'indirizzo IP del tuo computer o un intervallo di indirizzi IP nella tua rete locale.

Per altri scenari, consulta Regole del gruppo di sicurezza per diversi casi d'uso.

Per creare un gruppo EFA-enabled di sicurezza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Security Groups (Gruppi di sicurezza) e quindi Create Security Group (Crea gruppo di sicurezza).
3. Nella finestra Create Security Group (Crea gruppo di sicurezza) effettuare le operazioni seguenti:
   a. In Nome gruppo di sicurezza, immettere un nome descrittivo per il gruppo di sicurezza, ad esempio `EFA-enabled security group`.
   b. (Facoltativo) In Description (Descrizione), inserire una breve descrizione del gruppo di sicurezza.
   c. Per VPC, seleziona il VPC in cui intendi avviare le tue EFA-enabled istanze.
   d. Scegliere Create Security Group (Crea gruppo di sicurezza).
4. Seleziona il gruppo di sicurezza creato e nella scheda Details (Dettagli) copia il valore Security group ID (ID gruppo di sicurezza).
5. Dopo aver selezionato il gruppo di sicurezza, scegli Actions (Operazioni), Edit inbound rules (Modifica le regole in entrata) ed esegui le operazioni di seguito:
   a. Scegliere Add rule (Aggiungi regola).
   b. In Type (Tipo), selezionare All traffic (Tutto il traffico).
   c. Per Source type (Tipo di origine), scegli Custom (Personalizzata) e incolla nel campo l'ID del gruppo di sicurezza copiato in precedenza.
   d. Scegli Aggiungi regola.
   e. Per Type (Tipo) scegli SSH.
   f. Per Source (origine), scegli Anywhere-IPv4.
   g. Scegliere Salva regole.
6. Dopo aver selezionato il gruppo di sicurezza, scegli Actions (Operazioni), Edit outbound rules (Modifica le regole in uscita) ed esegui le operazioni di seguito:
   a. Scegliere Add rule (Aggiungi regola).
   b. In Type (Tipo), selezionare All traffic (Tutto il traffico).
   c. Per Destination type (Tipo di destinazione), scegli Custom (Personalizzata) e incolla nel campo l'ID del gruppo di sicurezza copiato in precedenza.

d. Scegliere Salva regole.

> **Important**
>
> Le regole autoreferenziali in entrata e in uscita (che consentono tutto il traffico da e verso il gruppo di sicurezza stesso) sono obbligatorie per il funzionamento dell'EFA. Senza queste regole, il traffico EFA tra le istanze verrà bloccato.

Fase 2: avviare un'istanza temporanea

Avvia un'istanza temporanea da utilizzare per installare e configurare i componenti software EFA. Utilizzi questa istanza per creare un' EFA-enabled AMI da cui avviare le tue EFA-enabled istanze.

Per avviare un'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e quindi scegli Launch instances (Avvia istanze) per aprire la nuova procedura guidata di avvio dell'istanza.
3. (Opzionale) Nella sezione Name and tags (Nome e tag), fornisci un nome per l'istanza, ad esempio `EFA-instance`. Il nome viene assegnato all'istanza come tag di risorsa (`Name=`*`EFA-instance`*).
4. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona un'AMI per uno dei sistemi operativi supportati.
5. Nella sezione Instance type (Tipo di istanza), seleziona un tipo di istanza supportato.
6. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da utilizzare per l'istanza.
7. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica) e quindi esegui le operazioni qui descritte:

   a. Per Subnet (Sottorete) seleziona la subnet in cui avviare l'istanza.

   > **Important**
   >
   > È necessario selezionare una sottorete. Se non selezioni una sottorete, non puoi abilitare l'istanza per l'EFA.

b. Per Firewall (security groups) (Firewall [gruppi di sicurezza]), scegli Select existing security group (Seleziona gruppo di sicurezza esistente) e quindi seleziona il gruppo di sicurezza creato nella fase precedente.

c. Espandi la sezione Configurazione avanzata.

   Come Interfaccia di rete 1, seleziona Indice della scheda di rete = 0, Indice dispositivo = 0 e Tipo di interfaccia = EFA con ENA.

   (Facoltativo) Se utilizzi un tipo di istanza con più schede, ad esempio `p4d.24xlarge` o `p5.48xlarge`, per ogni interfaccia di rete aggiuntiva richiesta, scegli Aggiungi interfaccia di rete, per Indice scheda di rete seleziona il successivo indice non utilizzato, quindi seleziona Indice dispositivo = 1 e Tipo di interfaccia = EFA con ENA o EFA-only

8. Nella sezione Storage (Archiviazione), configura i volumi secondo necessità.
9. Nel pannello Summary (Riepilogo) a destra, scegli Launch instance (Avvia istanza).

> **Note**
>
> Valuta la possibilità di richiedere l'uso di IMDSv2 per l'istanza temporanea, nonché per l'AMI che creerai alla Fase 9, a meno che tu non abbia già impostato IMDSv2 come predefinito per l'account. Per ulteriori informazioni sulla procedura di configurazione di IMDSv2, consulta Configurazione delle opzioni dei metadati dell'istanza per le nuove istanze.

Fase 3: installare il software EFA

Installa il EFA-enabled kernel, i driver EFA, Libfabric e lo stack Open MPI necessari per supportare EFA sull'istanza temporanea.

Le fasi variano a seconda che si intenda utilizzare EFA con Open MPI, con Intel MPI o con Open MPI e Intel MPI..

> **Note**
>
> Alcuni sistemi operativi potrebbero non essere supportati con Intel MPI. Se utilizzi Intel MPI, fai riferimento alla documentazione Intel MPI per verificare il supporto per il sistema operativo in uso.

Per installare il software EFA

1. Connettersi all'istanza avviata. Per ulteriori informazioni, consulta Connessione a un'istanza Linux tramite SSH.
2. Per verificare che tutti i pacchetti software siano aggiornati, eseguire un aggiornamento rapido del software sull'istanza. Questo processo può richiedere alcuni minuti.

   - Amazon Linux 2023, RHEL, Rocky Linux 8/9 8/9

     ```
     $ sudo yum update -y
     ```

   - Ubuntu e Debian

     ```
     $ sudo apt-get update && sudo apt-get upgrade -y
     ```

   - SUSE Linux Enterprise

     ```
     $ sudo zypper update -y
     ```

3. Riavviare l'istanza e riconnettersi a essa.
4. Scarica i file di installazione del software. I file di installazione del software sono riuniti in un file (`.tar.gz`) tarball compresso. Per scaricare l'ultima versione stabile, utilizzare il comando seguente.

   È inoltre possibile ottenere l'ultima versione sostituendo il numero della versione con `latest` nel comando qui sopra.

   ```
   $ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.50.0.tar.gz
   ```

5. (Opzionale) Verifica l'autenticità e l'integrità del file tarball EFA (`.tar.gz`).

   È consigliabile eseguire questa operazione per verificare l'identità dell'autore del software e che il file non sia stato alterato o danneggiato dopo la pubblicazione. Se non desideri verificare il file tarball, ignora questo passaggio.

   > **Note**
   >
   > In alternativa, se preferisci verificare il file tarball utilizzando un checksum MD5 o SHA256, consulta Verifica del programma di installazione EFA utilizzando un checksum.

a. Scarica la chiave pubblica GPG e importala nel tuo keyring.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

Il comando dovrebbe restituire un valore di chiave. Prendere nota del valore della chiave poiché sarà necessario nella fase successiva.

b. Verifica l'impronta digitale della chiave GPG. Esegui questo comando e specifica la chiave valore creata nella fase precedente.

```
$ gpg --fingerprint key_value
```

Il comando dovrebbe restituire un'impronta digitale identica a `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Se l'impronta digitale non corrisponde, non eseguire lo script di installazione EFA e contatta Supporto.

c. Scarica il file di firma e verifica la firma del file tarball EFA.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.50.0.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.50.0.tar.gz.sig
```

Di seguito viene mostrato l'output di esempio.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Se il risultato include `Good signature` e se l'impronta digitale corrisponde a quella restituita nel passaggio precedente, procedi alla fase successiva. In caso contrario, non eseguire lo script di installazione EFA e contatta Supporto.

6. Estrarre i file dal file `.tar.gz` compresso e andare alla directory estratta.

```
$ tar -xf aws-efa-installer-1.50.0.tar.gz && cd aws-efa-installer
```

7. (Facoltativo) Verifica le firme dei singoli pacchetti durante l'installazione.

A partire da EFA installer 1.48.0, l'installatore include GPG-signed singoli pacchetti RPM e DEB. Per verificare l'autenticità e l'integrità di ogni singolo pacchetto durante l'installazione, usa il flag. `--check-signatures` Quando abiliti questo flag, il programma di installazione verifica prima tutte le firme dei pacchetti e procede con l'installazione solo se ogni pacchetto supera la verifica. Se un pacchetto non supera la verifica, il programma di installazione esce immediatamente senza installare nulla.

a. Scarica la chiave pubblica GPG.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key
```

b. Esporta il percorso chiave. Quindi, nel passaggio successivo, aggiungete `--check-signatures` al comando di installazione e usate `sudo -E` invece che `sudo` per preservare la variabile di ambiente.

```
$ export EFA_INSTALLER_KEY=$(pwd)/aws-efa-installer.key
```

RPM-based Sui sistemi (Amazon Linux, RHEL, Rocky Linux e SUSE), il programma di installazione verifica ogni RPM utilizzando. `rpm --checksig` DEB-based Sui sistemi (Ubuntu, Debian), l'installatore verifica ogni DEB utilizzando la verifica della firma GPG.

Se la verifica di un pacchetto fallisce, l'installazione si interrompe immediatamente, proteggendo il sistema da pacchetti danneggiati o dannosi.

> **Note**
>
> La `--check-signatures` bandiera è opzionale. Senza di esso, l'installatore non esegue la verifica della firma individuale.

8. Installare il software EFA. Eseguire una delle seguenti operazioni, a seconda del caso d'uso:

> **Note**
>
> Se avete completato il passaggio opzionale precedente per impostare la verifica della firma del pacchetto, aggiungetelo `--check-signatures` al comando di installazione e

usate `sudo -E` al posto di. `sudo` Ad esempio: `sudo -E ./efa_installer.sh -y --check-signatures`.

> **Note**
>
> EFA non supporta NVIDIA GPUDirect con SUSE Linux. Se utilizzi SUSE Linux, devi specificare anche l'opzione `--skip-kmod` per impedire l'installazione di kmod. Per impostazione predefinita, SUSE Linux non consente moduli kernel out-of-tree.

Open MPI and Intel MPI

Se intendi utilizzare EFA con Open MPI e Intel MPI, devi installare il software EFA con Libfabric e Open MPI e completare la Fase 5: installare Intel MPI.

Per installare il software EFA con Libfabric e Open MPI, eseguire il seguente comando.

> **Note**
>
> A partire da EFA 1.30.0, sia Open MPI 4.1 che Open MPI 5 sono installati per impostazione predefinita. Facoltativamente, è possibile specificare la versione di Open MPI che si desidera installare. Per installare solo Open MPI 4.1, includi. `--mpi=openmpi4` Per installare solo Open MPI 5, includere `--mpi=openmpi5`. Per installare entrambi, omettere l'opzione `--mpi`.

```
$ sudo ./efa_installer.sh -y
```

Libfabric è installato su `/opt/amazon/efa`. Open MPI 4.1 è installato su. `/opt/amazon/openmpi` Open MPI 5 è installato su `/opt/amazon/openmpi5`.

Open MPI only

Se intendi utilizzare EFA solo con Open MPI, devi installare il software EFA con Libfabric e Open MPI e puoi ignorare la Fase 5: installare Intel MPI. Per installare il software EFA con Libfabric e Open MPI, eseguire il seguente comando.

> **Note**
>
> A partire da EFA 1.30.0, sia Open MPI 4.1 che Open MPI 5 sono installati per impostazione predefinita. Facoltativamente, è possibile specificare la versione di Open MPI che si desidera installare. Per installare solo Open MPI 4.1, includi. `--mpi=openmpi4` Per installare solo Open MPI 5, includere `--mpi=openmpi5`. Per installare entrambi, omettere l'opzione `--mpi`.

```
$ sudo ./efa_installer.sh -y
```

Libfabric è installato su `/opt/amazon/efa`. Open MPI 4.1 è installato su. `/opt/amazon/openmpi` Open MPI 5 è installato su `/opt/amazon/openmpi5`.

Intel MPI only

Se si intende utilizzare solo EFA con Intel MPI, è possibile installare il software EFA senza Libfabric e Open MPI. In tal caso, Intel MPI utilizza Libfabric incorporato. Se si sceglie di eseguire questa operazione, è necessario completare la Fase 5: installare Intel MPI.

Per installare il software EFA senza Libfabric e Open MPI, eseguire il seguente comando.

```
$ sudo ./efa_installer.sh -y --minimal
```

9. Se il programma di installazione di EFA richiede il riavvio dell'istanza, eseguire questa operazione e riconnettersi all'istanza. In caso contrario, disconnettersi dall'istanza e quindi accedere di nuovo per completare l'installazione.
10. Elimina il tarball non compresso e il tarball stesso. Altrimenti, questi verranno inclusi nell' EFA-enabled AMI che crei, aumentandone le dimensioni.

Fase 4: (Facoltativo) Abilita Open MPI 5

> **Note**
>
> Esegui questa fase solo se intendi utilizzare Open MPI 5.

A partire da EFA 1.30.0, sia Open MPI 4.1 che Open MPI 5 sono installati per impostazione predefinita. In alternativa, puoi scegliere di installare solo Open MPI 4.1 o Open MPI 5.

Se scegli di installare Open MPI 5 nella Fase 3: installare il software EFA e desideri utilizzarlo, devi eseguire questa procedura per abilitarlo.

Abilitazione di Open MPI 5

1. Aggiungi Open MPI 5 alla variabile di ambiente PATH.

   ```
   $ module load openmpi5
   ```

2. Verifica che Open MPI 5 sia abilitato per l'uso.

   ```
   $ which mpicc
   ```

   Il comando dovrebbe restituire la directory di installazione di Open MPI 5: `/opt/amazon/openmpi5`.

3. (Facoltativo) Per garantire che Open MPI 5 venga aggiunto alla variabile di ambiente PATH a ogni avvio dell'istanza, esegui le seguenti operazioni:

   bash shell

   Aggiungi `module load openmpi5` a `/home/`*`username`*`/.bashrc` e `/home/`*`username`*`/.bash_profile`.

   csh and tcsh shells

   Aggiungere `module load openmpi5` a `/home/`*`username`*`/.cshrc`.

Se è necessario rimuovere Open MPI 5 dalla variabile di ambiente PATH, esegui il seguente comando e rimuovilo dagli script shell di avvio.

```
$ module unload openmpi5
```

Fase 5: (Facoltativo) Installa Intel MPI

> **Important**
>
> Esegui questa fase solo se intendi utilizzare Intel MPI. Se intendi utilizzare Open MPI, salta questa fase.

Intel MPI richiede un'installazione aggiuntiva e la configurazione di una variabile d'ambiente.

Prerequisito

Verificare che l'utente che esegue le fasi seguenti disponga delle autorizzazioni sudo.

Per installare Intel MPI

1. Per scaricare lo script di installazione Intel MPI, procedi come indicato di seguito
   a. Visita il sito Web Intel.
   b. Nella sezione Intel MPI Library (Libreria Intel MPI) della pagina Web, scegli il collegamento per il programma di installazione offline della Libreria Intel MPI per Linux.
2. Esegui lo script di installazione scaricato nel passaggio precedente.

   ```
   $ sudo bash installation_script_name.sh
   ```
3. Nel programma di installazione, scegli Accetta e installa.
4. Leggi il programma Intel Improvement, scegli l'opzione appropriata, quindi scegli Begin Installation (Inizia l'installazione).
5. Al termine dell'installazione, scegliere Chiudi.
6. Per impostazione predefinita, Intel MPI utilizza il proprio Libfabric incorporato (interno). Puoi tuttavia configurare Intel MPI per utilizzare il componente Libfabric fornito con il programma di installazione EFA. In genere, il programma di installazione EFA viene fornito con una versione successiva di Libfabric rispetto a Intel MPI. In alcuni casi, il componente Libfabric fornito con il programma di installazione EFA è anche più performante di quello di Intel MPI. Per configurare Intel MPI per l'utilizzo del componente Libfabric fornito con il programma di installazione EFA, esegui una delle operazioni seguenti, in base alla shell in uso.

bash shells

Aggiungi l'istruzione seguente a /home/*username*/.bashrc e /home/*username*/.bash_profile.

```
export I_MPI_OFI_LIBRARY_INTERNAL=0
```

csh and tcsh shells

Aggiungi l'istruzione seguente a /home/*username*/.cshrc.

```
setenv I_MPI_OFI_LIBRARY_INTERNAL 0
```

7. Aggiungi il comando di origine seguente allo script della shell per generare lo script `vars.sh` dalla directory di installazione e impostare l'ambiente del compilatore ad ogni avvio dell'istanza. Eseguire uno dei seguenti, a seconda della shell in uso.

   bash shells

   Aggiungi l'istruzione seguente a /home/*username*/.bashrc e /home/*username*/.bash_profile.

   ```
   source /opt/intel/oneapi/mpi/latest/env/vars.sh
   ```

   csh and tcsh shells

   Aggiungi l'istruzione seguente a /home/*username*/.cshrc.

   ```
   source /opt/intel/oneapi/mpi/latest/env/vars.csh
   ```

8. Per impostazione predefinita, se EFA non è disponibile a causa di una configurazione errata, Intel MPI utilizza per impostazione predefinita lo stack di TCP/IP rete, il che potrebbe comportare un rallentamento delle prestazioni delle applicazioni. Per evitare questo comportamento, imposta `I_MPI_OFI_PROVIDER` su `efa`. Se EFA non è disponibile, Intel MPI mostra l'errore seguente:

   ```
   Abort (XXXXXX) on node 0 (rank 0 in comm 0): Fatal error in PMPI_Init: OtherMPI
    error,
   MPIR_Init_thread (XXX).......:
   MPID_Init (XXXX).............:
   ```

```
MPIDI_OFI_mpi_init_hook (XXXX):
open_fabric (XXXX).............:
find_provider (XXXX)..........:
OFI fi_getinfo() failed (ofi_init.c:2684:find_provider:
```

Eseguire uno dei seguenti, a seconda della shell in uso.

bash shells

Aggiungi l'istruzione seguente a /home/*username*/.bashrc e /home/*username*/.bash_profile.

```
export I_MPI_OFI_PROVIDER=efa
```

csh and tcsh shells

Aggiungi l'istruzione seguente a /home/*username*/.cshrc.

```
setenv I_MPI_OFI_PROVIDER efa
```

9. Per impostazione predefinita, Intel MPI non stampa le informazioni di debug. Per controllare tali informazioni, puoi specificare livelli di verbosità diversi. I valori possibili (secondo la quantità di dettagli che forniscono) sono: `0` (impostazione predefinita), `1`, `2`, `3`, `4`, `5`. Il livello `1` e i livelli superiori stampano `libfabric version` e `libfabric provider`. Utilizza `libfabric version` per verificare se Intel MPI sta usando il componente Libfabric interno o quello fornito con il programma di installazione EFA. Se sta usando il componente Libfabric interno, la versione presenta il suffisso `impi`. Use `libfabric provider` to check with Intel MPI utilizza EFA o la rete. TCP/IP Se utilizza EFA, il valore è `efa`. Se è in uso TCP/IP, il valore è. `tcp;ofi_rxm`

   Per abilitare le informazioni di debug, esegui una delle operazioni seguenti, in base alla shell in uso.

   bash shells

   Aggiungi l'istruzione seguente a /home/*username*/.bashrc e /home/*username*/.bash_profile.

   ```
   export I_MPI_DEBUG=value
   ```

csh and tcsh shells

Aggiungi l'istruzione seguente a /home/*username*/.cshrc.

```
setenv I_MPI_DEBUG value
```

10. Per impostazione predefinita, Intel MPI utilizza la memoria condivisa del sistema operativo (shm) per le comunicazioni tra nodi e utilizza Libfabric (ofi) solo per le comunicazioni tra nodi. In generale, questa configurazione offre le prestazioni migliori. In alcuni casi, tuttavia, il fabric shm Intel MPI può causare il blocco di alcune applicazioni a tempo indeterminato.

    Per risolvere questo problema, puoi forzare Intel MPI a utilizzare Libfabric sia per le comunicazioni intranodo che per quelle internodo. A tal scopo, esegui una delle operazioni seguenti, in base alla shell in uso.

    bash shells

    Aggiungi l'istruzione seguente a /home/*username*/.bashrc e /home/*username*/.bash_profile.

    ```
    export I_MPI_FABRICS=ofi
    ```

    csh and tcsh shells

    Aggiungi l'istruzione seguente a /home/*username*/.cshrc.

    ```
    setenv I_MPI_FABRICS ofi
    ```

    > **Note**
    >
    > Il provider Libfabric di EFA utilizza la memoria condivisa del sistema operativo per le comunicazioni intranodo. Ciò significa che impostando I_MPI_FABRICS su ofi si ottengono prestazioni simili a quelle della configurazione shm:ofi predefinita.

11. Disconnettersi e quindi riconnettersi all'istanza.

Se non si desidera più utilizzare Intel MPI, rimuovere le variabili di ambiente dagli script shell di startup.

Fase 6: disabilitare la protezione Ptrace

Per migliorare le prestazioni dell'applicazione HPC, Libfabric utilizza la memoria locale dell'istanza per le comunicazioni tra processi quando i processi sono in esecuzione sulla stessa istanza.

La funzione di memoria condivisa utilizza Cross Memory Attach (CMA), che non è supportato con la protezione ptrace. Se si utilizza una distribuzione Linux con protezione ptrace abilitata per impostazione predefinita, come Ubuntu, è necessario disabilitarla. Se la tua distribuzione Linux non ha la protezione ptrace abilitata per impostazione predefinita, ignorare questo passaggio.

Per disabilitare la protezione ptrace

Scegliere una delle seguenti operazioni:

- Per disabilitare temporaneamente la protezione ptrace a scopo di test, esegui il comando seguente.

```
$ sudo sysctl -w kernel.yama.ptrace_scope=0
```

- Per disabilitare in modo permanente la protezione ptrace, aggiungere `kernel.yama.ptrace_scope = 0` a `/etc/sysctl.d/10-ptrace.conf` e riavviare l'istanza.

Fase 7. Conferma dell'installazione

Verifica della corretta installazione

1. Per verificare che MPI sia stato correttamente installato, esegui il comando seguente:

   ```
   $ which mpicc
   ```

   - Per Open MPI, il percorso restituito deve includere `/opt/amazon/`.
   - Per Intel MPI, il percorso restituito deve includere `/opt/intel/`. Se non ottieni l'output previsto, assicurati di aver fornito lo script `vars.sh` di Intel MPI.
2. Per confermare che i componenti software EFA e Libfabric siano stati installati correttamente, emetti il comando seguente.

```
$ fi_info -p efa -t FI_EP_RDM
```

Il comando deve restituire informazioni sulle interfacce EFA Libfabric. L'esempio seguente mostra l'output del comando.

```
provider: efa
    fabric: EFA-fe80::94:3dff:fe89:1b70
    domain: efa_0-rdm
    version: 2.0
    type: FI_EP_RDM
    protocol: FI_PROTO_EFA
```

Fase 8: installazione dell'applicazione HPC

Installa l'applicazione HPC sull'istanza temporanea. La procedura di installazione varia in base alla specifica applicazione HPC. Per ulteriori informazioni, consulta Gestire gli aggiornamenti del sistema operativo nella Guida per l'utente di Amazon Linux 2023.

> **Note**
>
> Fai riferimento alla documentazione dell'applicazione HPC per le istruzioni di installazione.

Fase 9: Creazione di un'AMI EFA-enabled

Dopo aver installato i componenti software richiesti, crei un'AMI che puoi riutilizzare per avviare le tue EFA-enabled istanze.

Per creare un'AMI dall'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza temporanea creata e seleziona Actions (Operazioni), Image (Immagine), Create Image (Crea immagine).
4. Per Create image (Crea immagine), effettua le seguenti operazioni:

    a. In Image name (Nome immagine), immettere un nome descrittivo per l'AMI.

b. (Facoltativo) In Image description (Descrizione immagine), inserire una breve descrizione dell'AMI.

c. Scegliere Create Image (Crea immagine).

5. Nel riquadro di navigazione scegliere AMIs (AMI).
6. Individua l'AMI che hai creato nell'elenco. Prima di procedere con la fase seguente, attendi che lo stato passi da `pending` a `available`.

Passaggio 10: avvia EFA-enabled le istanze in un gruppo di posizionamento del cluster

Avvia le tue EFA-enabled istanze in un gruppo di posizionamento del cluster utilizzando l' EFA-enabledAMI che hai creato nel passaggio 7 e il gruppo EFA-enabled di sicurezza che hai creato nel passaggio 1.

> **Note**
>
> - Non è un requisito assoluto avviare le EFA-enabled istanze in un gruppo di posizionamento del cluster. Tuttavia, consigliamo di eseguire le EFA-enabled istanze in un gruppo di posizionamento del cluster in quanto avvia le istanze in un gruppo a bassa latenza in una singola zona di disponibilità.
> - Per garantire che la capacità sia disponibile man mano che si ridimensionano le istanze del cluster, è possibile creare una prenotazione di capacità per il gruppo di posizionamento del cluster. Per ulteriori informazioni, consulta Utilizza Capacity Reservations con gruppi di collocamento.

Per avviare un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e quindi scegli Launch instances (Avvia istanze) per aprire la nuova procedura guidata di avvio dell'istanza.
3. (Opzionale) Nella sezione Name and tags (Nome e tag), fornisci un nome per l'istanza, ad esempio `EFA-instance`. Il nome viene assegnato all'istanza come tag di risorsa (`Name=`*`EFA-instance`*).
4. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), scegli My AMIs (Le mie AMI), quindi seleziona l'AMI creata nella fase precedente.

5. Nella sezione Instance type (Tipo di istanza), seleziona un tipo di istanza supportato.
6. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da utilizzare per l'istanza.
7. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica) e quindi esegui le operazioni qui descritte:

   a. Per Subnet (Sottorete) seleziona la subnet in cui avviare l'istanza.

   > **Important**
   >
   > È necessario selezionare una sottorete. Se non selezioni una sottorete, non puoi abilitare l'istanza per l'EFA.

   b. Per Firewall (security groups) (Firewall [gruppi di sicurezza]), scegli Select existing security group (Seleziona gruppo di sicurezza esistente) e quindi seleziona il gruppo di sicurezza creato nella fase precedente.

   c. Espandi la sezione Configurazione avanzata.

   Come Interfaccia di rete 1, seleziona Indice della scheda di rete = 0, Indice dispositivo = 0 e Tipo di interfaccia = EFA con ENA.

   (Facoltativo) Se utilizzi un tipo di istanza con più schede, ad esempio `p4d.24xlarge` o `p5.48xlarge`, per ogni interfaccia di rete aggiuntiva richiesta, scegli Aggiungi interfaccia di rete, per Indice scheda di rete seleziona il successivo indice non utilizzato, quindi seleziona Indice dispositivo = 1 e Tipo di interfaccia = EFA con ENA o. EFA-only
8. (Opzionale) Nella sezione Storage (Archiviazione), configura i volumi secondo necessità.
9. Nella sezione Advanced details (Dettagli avanzati), per Placement group name (Nome del gruppo di collocazione), seleziona il gruppo di collocazione cluster in cui avviare le istanze. Se occorre creare un nuovo gruppo di collocazione cluster, scegli Create new placement group (Crea nuovo gruppo di collocazione).
10. Nel pannello Riepilogo a destra, per Numero di istanze, inserisci il numero di EFA-enabled istanze che desideri avviare, quindi scegli Avvia istanza.

Fase 11: terminare l'istanza temporanea

A questo punto l'istanza avviata alla Fase 2 non è più necessaria. È possibile terminare l'istanza per evitare di incorrere in costi aggiuntivi.

Per terminare l'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza temporanea creata, quindi seleziona Operazioni, Stato istanza, Termina (elimina) istanza.
4. Quando viene richiesta la conferma, seleziona Termina (elimina).

Fase 12: abilitazione di SSH senza password

Per consentire l'esecuzione delle applicazioni in tutte le istanze del cluster, è necessario abilitare l'accesso SSH senza password dal nodo leader ai nodi membro. Il nodo principale è l'istanza da cui vengono eseguite le applicazioni. Le restanti istanze del cluster sono i nodi membro.

Per abilitare SSH senza password tra le istanze del cluster

1. Selezionare un'istanza nel cluster come nodo principale e connettersi a essa.
2. Disabilita `strictHostKeyChecking` e abilita `ForwardAgent` sul nodo principale. Aprire il file `~/.ssh/config` utilizzando qualsiasi editor di testo e aggiungere il seguente script.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Generare una coppia di chiavi RSA.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

   La coppia di chiavi viene creata nella directory `$HOME/.ssh/`.

4. Modifica le autorizzazioni della chiave privata sul nodo principale.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Aprire `~/.ssh/id_rsa.pub` utilizzando l'editor di testo preferito e copiare la chiave.
6. Per ogni nodo membro nel cluster, procedere nel modo seguente:

a. Collegarsi all'istanza.

b. Aprire `~/.ssh/authorized_keys` utilizzando qualsiasi editor di testo e aggiungere la chiave pubblica copiata in precedenza.

7. Per verificare che SSH senza password funzioni come previsto, connettersi al nodo leader ed eseguire il seguente comando.

```
$ ssh member_node_private_ip
```

La connessione al nodo membro non dovrebbe richiedere una chiave o una password.

Nozioni di base su EFA e NCCL per i carichi di lavoro ML su Amazon EC2

NVIDIA Collective Communications Library (NCCL) è una libreria di routine di comunicazione collettive standard per più GPU su un singolo nodo o su più nodi. Puoi utilizzare NCCL insieme a EFA, Libfabric e MPI per supportare vari carichi di lavoro di machine learning. Per ulteriori informazioni, consulta il sito Web NCCL.

Requisiti

- I tipi di istanza supportati includono i tipi di istanze della serie EFA-supported P e della serie G. Per ulteriori informazioni, consulta Istanze a calcolo accelerato Amazon EC2.
- AMI di base supportate: Amazon Linux 2023, Ubuntu 26.04, Ubuntu 24.04, Ubuntu 22.04, Debian 12 e RHEL 10.
- L'EFA supporta solo NCCL 2.4.2 e versioni successive.

Per ulteriori informazioni sull'esecuzione di carichi di lavoro di machine learning con EFA e NCCL utilizzando un AWS Deep Learning AMIs, consulta Using EFA on the DLAMI nella Developer Guide. AWS Deep Learning AMIs

Fasi

- Fase 1: Preparare un gruppo di sicurezza EFA-enabled
- Fase 2: avviare un'istanza temporanea
- Passaggio 3: installa i driver GPU NVIDIA, NVIDIA CUDA Toolkit e cuDNN
- Fase 4: installazione del GDRCopy
- Fase 5: installazione del software EFA

- Fase 6: installare NCCL
- Fase 7: installare i test NCCL
- Fase 8: testare la configurazione EFA e NCCL
- Fase 9: installare applicazioni di machine learning
- Passaggio 10: creare un EFA e un'AMI NCCL-enabled
- Fase 11: terminare l'istanza temporanea
- Fase 12: Avvia l'EFA e NCCL-enabled le istanze in un gruppo di collocamento del cluster
- Fase 13: abilitare SSH senza password

Fase 1: Preparare un gruppo di sicurezza EFA-enabled

Un EFA richiede un gruppo di sicurezza in cui sia consentito tutto il traffico in entrata e in uscita dal gruppo stesso. La procedura seguente crea un gruppo di sicurezza che consente tutto il traffico in entrata e in uscita da e verso se stesso e che consente il traffico SSH in entrata da qualsiasi indirizzo IPv4 per la connettività SSH.

> **Important**
>
> - Questo gruppo di sicurezza è destinato esclusivamente a scopi di test. Per i tuoi ambienti di produzione, consigliamo di creare una regola SSH in entrata che consenta il traffico solo dall'indirizzo IP da cui ti connetti, ad esempio l'indirizzo IP del tuo computer o un intervallo di indirizzi IP nella tua rete locale.
> - Le regole autoreferenziali in entrata e in uscita (che consentono tutto il traffico da e verso il gruppo di sicurezza stesso) sono obbligatorie per il funzionamento dell'EFA. Senza queste regole, il traffico EFA tra le istanze verrà bloccato e la comunicazione NCCL fallirà.

Per altri scenari, consulta Regole del gruppo di sicurezza per diversi casi d'uso.

Per creare un gruppo di sicurezza EFA-enabled

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Security Groups (Gruppi di sicurezza) e quindi Create Security Group (Crea gruppo di sicurezza).
3. Nella finestra Create Security Group (Crea gruppo di sicurezza) effettuare le operazioni seguenti:

a. In Nome gruppo di sicurezza, immettere un nome descrittivo per il gruppo di sicurezza, ad esempio `EFA-enabled security group`.

b. (Facoltativo) In Description (Descrizione), inserire una breve descrizione del gruppo di sicurezza.

c. Per VPC, seleziona il VPC in cui intendi avviare le tue EFA-enabled istanze.

d. Scegliere Create Security Group (Crea gruppo di sicurezza).

4. Seleziona il gruppo di sicurezza creato e nella scheda Details (Dettagli) copia il valore Security group ID (ID gruppo di sicurezza).

5. Dopo aver selezionato il gruppo di sicurezza, scegli Actions (Operazioni), Edit inbound rules (Modifica le regole in entrata) ed esegui le operazioni di seguito:

   a. Scegliere Add rule (Aggiungi regola).

   b. In Type (Tipo), selezionare All traffic (Tutto il traffico).

   c. Per Source type (Tipo di origine), scegli Custom (Personalizzata) e incolla nel campo l'ID del gruppo di sicurezza copiato in precedenza.

   d. Scegli Aggiungi regola.

   e. Per Type (Tipo) scegli SSH.

   f. Per Source (origine), scegli Anywhere-IPv4.

   g. Scegliere Salva regole.

6. Dopo aver selezionato il gruppo di sicurezza, scegli Actions (Operazioni), Edit outbound rules (Modifica le regole in uscita) ed esegui le operazioni di seguito:

   a. Scegliere Add rule (Aggiungi regola).

   b. In Type (Tipo), selezionare All traffic (Tutto il traffico).

   c. Per Destination type (Tipo di destinazione), scegli Custom (Personalizzata) e incolla nel campo l'ID del gruppo di sicurezza copiato in precedenza.

   d. Scegliere Salva regole.

Fase 2: avviare un'istanza temporanea

Avvia un'istanza temporanea da utilizzare per installare e configurare i componenti software EFA. Utilizzi questa istanza per creare un' EFA-enabled AMI da cui avviare le tue istanze. EFA-enabled

Per avviare un'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e quindi scegli Launch instances (Avvia istanze) per aprire la nuova procedura guidata di avvio dell'istanza.
3. (Opzionale) Nella sezione Name and tags (Nome e tag), fornisci un nome per l'istanza, ad esempio `EFA-instance`. Il nome viene assegnato all'istanza come tag di risorsa (`Name=EFA-instance`).
4. Nella sezione Immagini di applicazioni e sistema operativo, seleziona un'AMI per uno dei sistemi operativi supportati.
5. Nella sezione Tipo di istanza, seleziona un tipo di istanza supportato.
6. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da utilizzare per l'istanza.
7. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica) e quindi esegui le operazioni qui descritte:

   a. Per Subnet (Sottorete) seleziona la subnet in cui avviare l'istanza.

   > **Important**
   >
   > È necessario selezionare una sottorete. Se non selezioni una sottorete, non puoi abilitare l'istanza per l'EFA.

   b. Per Firewall (security groups) (Firewall [gruppi di sicurezza]), scegli Select existing security group (Seleziona gruppo di sicurezza esistente) e quindi seleziona il gruppo di sicurezza creato nella fase precedente.

   c. Espandi la sezione Configurazione avanzata.

      Come Interfaccia di rete 1, seleziona Indice della scheda di rete = 0, Indice dispositivo = 0 e Tipo di interfaccia = EFA con ENA.

      (Facoltativo) Se utilizzi un tipo di istanza con più schede, per ogni interfaccia di rete aggiuntiva richiesta, scegli Aggiungi interfaccia di rete, per Indice scheda di rete seleziona il successivo indice non utilizzato, quindi seleziona Indice dispositivo = 1 e Tipo di interfaccia = EFA con ENA o. EFA-only
8. Nella sezione Storage (Archiviazione), configura i volumi secondo necessità.

> **Note**
>
> È necessario fornire ulteriori 10-20 GiB di spazio di archiviazione per NVIDIA CUDA Toolkit. Se non fornisci spazio di archiviazione sufficiente, riceverai un `insufficient disk space` messaggio di errore quando tenti di installare i driver NVIDIA e il toolkit CUDA.

9. Nel pannello Summary (Riepilogo) a destra, scegli Launch instance (Avvia istanza).

Passaggio 3: installa i driver GPU NVIDIA, NVIDIA CUDA Toolkit e cuDNN

Amazon Linux 2023

Per installare i driver GPU NVIDIA, NVIDIA CUDA Toolkit e cuDNN

1. Per verificare che tutti i pacchetti software siano aggiornati, eseguire un aggiornamento rapido del software sull'istanza.

```
$ sudo dnf upgrade -y && sudo reboot
```

   Dopo il riavvio, riconnettersi all'istanza.

2. Installa le utilità necessarie per installare i driver GPU NVIDIA e il NVIDIA CUDA Toolkit.

```
$ sudo dnf groupinstall 'Development Tools' -y && sudo dnf install -y dkms
 kernel-devel-$(uname -r) kernel-headers-$(uname -r)
```

3. Disabilitare i driver open source `nouveau`.

   a. Installare le utility richieste e il pacchetto delle intestazioni kernel per la versione del kernel attualmente in esecuzione.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -
r)
```

   b. Aggiungi al file deny list`nouveau`. `/etc/modprobe.d/blacklist.conf`

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
```

```
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

c. Aggiungi `GRUB_CMDLINE_LINUX="rdblacklist=nouveau"` al `grub` file e ricostruisci la configurazione di GRUB.

```
$ echo 'GRUB_CMDLINE_LINUX="rdblacklist=nouveau"' | sudo tee -a /etc/
default/grub \
&& sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Riavviare l'istanza e riconnettersi a essa.
5. Aggiungere il repository di rete CUDA.

```
$ sudo yum-config-manager --add-repo https://developer.download.nvidia.com/
compute/cuda/repos/rhel8/x86_64/cuda-rhel8.repo
```

6. Scarica e installa il driver GPU NVIDIA.

```
$ wget https://us.download.nvidia.com/tesla/580.167.08/NVIDIA-Linux-
x86_64-580.167.08.run \
&& sudo sh NVIDIA-Linux-x86_64-580.167.08.run -m kernel-open --no-drm --disable-
nouveau --dkms --silent
```

7. Installa NVIDIA CUDA Toolkit e cuDNN.

```
$ sudo dnf install -y cuda-toolkit-13-0 libcudnn9-cuda-13 libcudnn9-devel-
cuda-13
```

8. Riavviare l'istanza e riconnettersi a essa.
9. (Istanze con NvSwitch, ad esempio istanze P-series multi-GPU) Installa e avvia NVIDIA Fabric Manager. G-series le istanze non utilizzano NVSwitch e non richiedono Fabric Manager.

```
$ sudo dnf install -y https://developer.download.nvidia.com/compute/cuda/repos/
rhel8/x86_64/nvidia-fabricmanager-580.167.08-1.el8.x86_64.rpm \
&& sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-
fabricmanager
```

10. Assicurarsi che i percorsi CUDA siano impostati ogni volta che viene avviata l'istanza.

    - Per le shell bash, aggiungere le seguenti istruzioni a /home/*username*/.bashrc e /home/*username*/.bash_profile.

      ```
      export PATH=/usr/local/cuda/bin:$PATH
      export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
      lib64:$LD_LIBRARY_PATH
      ```

    - Per le shell tcsh, aggiungere le seguenti istruzioni a /home/*username*/.cshrc.

      ```
      setenv PATH=/usr/local/cuda/bin:$PATH
      setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
      lib64:$LD_LIBRARY_PATH
      ```

11. Per confermare che i driver della GPU NVIDIA siano funzionanti, esegui il seguente comando.

    ```
    $ nvidia-smi -q | head
    ```

    Il comando dovrebbe restituire informazioni sulle GPU NVIDIA, sui driver delle GPU NVIDIA e sul NVIDIA CUDA Toolkit.

Ubuntu 26.04, Ubuntu 24.04, and Ubuntu 22.04

Per installare i driver GPU NVIDIA, NVIDIA CUDA Toolkit e cuDNN

1. Per verificare che tutti i pacchetti software siano aggiornati, eseguire un aggiornamento rapido del software sull'istanza.

   ```
   $ sudo apt-get update && sudo apt-get upgrade -y
   ```

2. Installa le utilità necessarie per installare i driver GPU NVIDIA e il NVIDIA CUDA Toolkit.

   ```
   $ sudo apt-get update && sudo apt-get install build-essential -y
   ```

3. Per utilizzare il driver GPU NVIDIA, devi prima disabilitare i driver open source. nouveau

   a. Installare le utility richieste e il pacchetto delle intestazioni kernel per la versione del kernel attualmente in esecuzione.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

b. Aggiungi nouveau al file della lista `/etc/modprobe.d/blacklist.conf` negata.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

c. Aprire il file `/etc/default/grub` utilizzando qualsiasi editor di testo e aggiungere il seguente script.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

d. Ricostruisci la configurazione di GRUB.

```
$ sudo update-grub
```

4. Riavviare l'istanza e riconnettersi a essa.
5. Aggiungi il repository CUDA e installa i driver GPU NVIDIA, NVIDIA CUDA Toolkit e cuDNN.

   - Ubuntu 26.04

```
$ wget https://developer.download.nvidia.com/compute/cuda/repos/ubuntu2604/
x86_64/cuda-keyring_1.1-1_all.deb \
&& sudo dpkg -i cuda-keyring_1.1-1_all.deb \
&& sudo add-apt-repository -y 'deb [trusted=yes] https://
developer.download.nvidia.com/compute/cuda/repos/ubuntu2604/x86_64 /' \
&& sudo apt-get update
```

```
$ sudo apt-get install -y nvidia-open cuda-toolkit-13-3 libcudnn9-cuda-13
 libcudnn9-dev-cuda-13
```

   - Ubuntu 24.04

```
$ wget https://developer.download.nvidia.com/compute/cuda/repos/ubuntu2404/
x86_64/cuda-keyring_1.1-1_all.deb \
```

```
&& sudo dpkg -i cuda-keyring_1.1-1_all.deb \
&& sudo add-apt-repository -y 'deb [trusted=yes] https://
developer.download.nvidia.com/compute/cuda/repos/ubuntu2404/x86_64 /' \
&& sudo apt-get update
```

```
$ sudo apt-get install -y nvidia-open-580 cuda-toolkit-13-0 libcudnn9-cuda-13
 libcudnn9-dev-cuda-13
```

- Ubuntu 22.04

```
$ wget https://developer.download.nvidia.com/compute/cuda/repos/ubuntu2204/
x86_64/cuda-keyring_1.1-1_all.deb \
&& sudo dpkg -i cuda-keyring_1.1-1_all.deb \
&& sudo DEBIAN_FRONTEND=noninteractive add-apt-repository -y "deb https://
developer.download.nvidia.com/compute/cuda/repos/ubuntu2204/x86_64/ /" \
&& sudo apt-get update
```

```
$ sudo apt-get install -y nvidia-open-580 cuda-toolkit-13-0 libcudnn9-cuda-13
 libcudnn9-dev-cuda-13
```

6. Riavviare l'istanza e riconnettersi a essa.
7. (Istanze con NvSwitch, ad esempio istanze P-series multi-GPU) Installa e avvia NVIDIA Fabric Manager. G-series le istanze non utilizzano NVSwitch e non richiedono Fabric Manager.

   - Ubuntu 26.04

   ```
   $ sudo apt-get install -y nvidia-fabricmanager \
   && sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-
   fabricmanager
   ```

   - Ubuntu 24.04 e Ubuntu 22.04

   ```
   $ sudo apt-get install -y nvidia-fabricmanager-580 \
   && sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-
   fabricmanager
   ```

8. Assicurarsi che i percorsi CUDA siano impostati ogni volta che viene avviata l'istanza.

   - Per le shell bash, aggiungere le seguenti istruzioni a `/home/`*`username`*`/.bashrc` e `/home/`*`username`*`/.bash_profile`.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

- Per le shell tcsh, aggiungere le seguenti istruzioni a /home/*username*/.cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

9. Per confermare che i driver della GPU NVIDIA funzionino, esegui il seguente comando.

```
$ nvidia-smi -q | head
```

Il comando dovrebbe restituire informazioni sulle GPU NVIDIA, sui driver delle GPU NVIDIA e sul NVIDIA CUDA Toolkit.

Debian 12

Per installare i driver GPU NVIDIA, NVIDIA CUDA Toolkit e cuDNN

1. Installa le utilità necessarie per installare i driver GPU NVIDIA e il NVIDIA CUDA Toolkit.

```
$ sudo apt-get install -y build-essential gcc make linux-headers-$(uname -r)
 dkms
```

2. Disabilitare i driver open source nouveau.

```
$ sudo sed -i 's/GRUB_CMDLINE_LINUX=""/
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"/' /etc/default/grub && sudo update-grub
```

3. Riavviare l'istanza e riconnettersi a essa.
4. Aggiungi il repository CUDA e installa i driver GPU NVIDIA, NVIDIA CUDA Toolkit e cuDNN.

```
$ wget https://developer.download.nvidia.com/compute/cuda/repos/debian12/x86_64/
cuda-keyring_1.1-1_all.deb \
&& sudo dpkg -i cuda-keyring_1.1-1_all.deb \
&& sudo DEBIAN_FRONTEND=noninteractive add-apt-repository -y "deb https://
developer.download.nvidia.com/compute/cuda/repos/debian12/x86_64/ /" \
```

```
&& sudo apt-get update
```

```
$ sudo apt-get install -y nvidia-open cuda-toolkit-13-0 libcudnn9-cuda-13
 libcudnn9-dev-cuda-13
```

5. Configura il modulo del kernel NVIDIA UVM.

```
$ uvm_ko=$(find /lib/modules/$(uname -r) -name 'nvidia*uvm*.ko*' 2>/dev/null
 | head -1) && if [ -n "$uvm_ko" ]; then real=$(basename "$uvm_ko"); real=
${real%.ko*}; echo "$real" | sudo tee /etc/modules-load.d/nvidia-uvm.conf; if
 [ "$real" != "nvidia-uvm" ]; then echo "alias nvidia-uvm $real" | sudo tee /
etc/modprobe.d/nvidia-uvm.conf; fi; sudo modprobe "$real" || true; fi && sudo
 modprobe nvidia
```

6. Riavviare l'istanza e riconnettersi a essa.
7. (Istanze con NvSwitch, ad esempio istanze P-series multi-GPU) Installa e avvia NVIDIA Fabric Manager. G-series le istanze non utilizzano NVSwitch e non richiedono Fabric Manager.

   a. Determina la versione del modulo del kernel NVIDIA.

   ```
   $ cat /proc/driver/nvidia/version | grep "Kernel Module"
   ```

   Di seguito è riportato un output di esempio.

   ```
   NVRM version: NVIDIA UNIX x86_64 Kernel Module  610.43.02  ...
   ```

   Nell'esempio precedente, è stata installata la versione principale `610` del modulo kernel.

   b. Installa NVIDIA Fabric Manager utilizzando la versione principale identificata nel passaggio precedente.

   ```
   $ sudo apt-get install -y nvidia-fabricmanager-major_version_number \
   && sudo systemctl enable nvidia-fabricmanager && sudo systemctl start
    nvidia-fabricmanager
   ```

8. Assicurarsi che i percorsi CUDA siano impostati ogni volta che viene avviata l'istanza.

   - Per le shell bash, aggiungere le seguenti istruzioni a `/home/username/.bashrc` e `/home/username/.bash_profile`.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

- Per le shell tcsh, aggiungere le seguenti istruzioni a /home/*username*/.cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

9. Per confermare che i driver della GPU NVIDIA siano funzionanti, esegui il seguente comando.

```
$ nvidia-smi -q | head
```

Il comando dovrebbe restituire informazioni sulle GPU NVIDIA, sui driver delle GPU NVIDIA e sul NVIDIA CUDA Toolkit.

RHEL 10

Per installare i driver GPU NVIDIA, NVIDIA CUDA Toolkit e cuDNN

1. Per verificare che tutti i pacchetti software siano aggiornati, eseguire un aggiornamento rapido del software sull'istanza.

```
$ sudo dnf upgrade -y && sudo reboot
```

Dopo il riavvio, riconnettersi all'istanza.

2. Installa le utilità necessarie per installare i driver GPU NVIDIA e il NVIDIA CUDA Toolkit.

```
$ sudo dnf groupinstall 'Development Tools' -y \
&& sudo dnf install -y dkms kernel-devel-$(uname -r) \
&& sudo dnf install -y https://dl.fedoraproject.org/pub/epel/epel-release-
latest-10.noarch.rpm
```

3. Disabilitare i driver open source nouveau.

a. Aggiungi al file deny listnouveau. /etc/modprobe.d/blacklist.conf

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

b. Aggiungi `GRUB_CMDLINE_LINUX="rdblacklist=nouveau"` al `grub` file e ricostruisci la configurazione di GRUB.

```
$ echo 'GRUB_CMDLINE_LINUX="rdblacklist=nouveau"' | sudo tee -a /etc/
default/grub \
&& sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Riavviare l'istanza e riconnettersi a essa.
5. Aggiungi il repository CUDA e installa i driver GPU NVIDIA, NVIDIA CUDA Toolkit e cuDNN.

```
$ sudo yum-config-manager --add-repo https://developer.download.nvidia.com/
compute/cuda/repos/rhel10/x86_64/cuda-rhel10.repo \
&& sudo dnf install -y nvidia-open-580.167.08 cuda-toolkit-13-0 libcudnn9-
cuda-13 libcudnn9-devel-cuda-13
```

6. Riavviare l'istanza e riconnettersi a essa.
7. (Istanze con NvSwitch, ad esempio istanze multi-GPU) Installa e avvia NVIDIA Fabric Manager. P-series G-series le istanze non utilizzano NVSwitch e non richiedono Fabric Manager.

```
$ sudo dnf install -y https://developer.download.nvidia.com/compute/cuda/repos/
rhel10/x86_64/nvidia-fabricmanager-580.167.08-1.x86_64.rpm \
&& sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-
fabricmanager
```

8. Assicurarsi che i percorsi CUDA siano impostati ogni volta che viene avviata l'istanza.

   - Per le shell bash, aggiungere le seguenti istruzioni a `/home/`*`username`*`/.bashrc` e `/home/`*`username`*`/.bash_profile`.

```
export PATH=/usr/local/cuda/bin:$PATH
```

```
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

- Per le shell tcsh, aggiungere le seguenti istruzioni a /home/*username*/.cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

9. Per confermare che i driver della GPU NVIDIA siano funzionanti, esegui il seguente comando.

```
$ nvidia-smi -q | head
```

Il comando dovrebbe restituire informazioni sulle GPU NVIDIA, sui driver delle GPU NVIDIA e sul NVIDIA CUDA Toolkit.

Fase 4: installazione del GDRCopy

Installa GDRCopy per migliorare le prestazioni di Libfabric. Per ulteriori informazioni su GDRCopy, consulta il repository GDRCopy.

Amazon Linux 2023

Installazione del GDRCopy

1. Installare le dipendenze richieste.

```
$ sudo yum -y install dkms rpm-build make check check-devel
```

2. Scarica ed estrai il pacchetto GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.5.2.tar.gz \
&& tar xf v2.5.2.tar.gz && cd gdrcopy-2.5.2/packages
```

3. Compila i pacchetti RPM di GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-rpm-packages.sh
```

4. Installa i pacchetti RPM di GDRCopy.

```
$ sudo rpm -Uvh gdrcopy-kmod-2.5.2*dkms*.rpm \
&& sudo rpm -Uvh gdrcopy-2.5.2*.rpm \
&& sudo rpm -Uvh gdrcopy-devel-2.5.2*.rpm
```

Ubuntu 26.04, Ubuntu 24.04, and Ubuntu 22.04

Installazione del GDRCopy

1. Installare le dipendenze richieste.

```
$ sudo apt-get install -y build-essential devscripts debhelper fakeroot pkg-
config dkms
```

> **Note**
>
> Su Ubuntu 22.04, installa anche le seguenti dipendenze aggiuntive:

```
$ sudo apt-get install -y check libsubunit-dev
```

2. Scarica ed estrai il pacchetto GDRCopy e crea i pacchetti.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.5.2.tar.gz \
&& tar xf v2.5.2.tar.gz \
&& cd gdrcopy-2.5.2/packages \
&& CUDA=/usr/local/cuda ./build-deb-packages.sh
```

3. Installa i pacchetti DEB di GDRCopy.

```
$ sudo dpkg -i gdrdrv-dkms_2.5.2-1_amd64.*.deb \
&& sudo dpkg -i libgdrapi_2.5.2-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy-tests_2.5.2-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy_2.5.2-1_amd64.*.deb
```

Debian 12

Installazione del GDRCopy

1. Installare le dipendenze richieste.

```
$ sudo apt-get install -y build-essential devscripts debhelper fakeroot pkg-
config dkms
```

2. Scarica ed estrai il pacchetto GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.5.2.tar.gz \
&& tar xf v2.5.2.tar.gz && cd gdrcopy-2.5.2/packages
```

3. Applica le patch della versione Debian e compila i pacchetti.

```
$ sed -i 's/(2.5.2)/(2.5.2-1)/g' debian-lib/changelog \
&& sed -i 's/(2.5.2)/(2.5.2-1)/g' debian-tests/changelog \
&& sed -i 's/(2.5.2)/(2.5.2-1)/g' dkms/debian/changelog \
&& sed -i 's/(2.5.2)/(2.5.2-1)/g' debian-meta/changelog \
&& sed -i 's/FULL_VERSION="${VERSION}"/FULL_VERSION="${VERSION}-
${DEBIAN_VERSION}"/g' build-deb-packages.sh
```

```
$ CUDA=/usr/local/cuda ./build-deb-packages.sh
```

4. Installa i pacchetti DEB di GDRCopy.

```
$ sudo dpkg -i gdrdrv-dkms_2.5.2*.deb \
&& sudo dpkg -i libgdrapi_2.5.2*.deb \
&& sudo dpkg -i gdrcopy-tests_2.5.2*.deb \
&& sudo dpkg -i gdrcopy_2.5.2*.deb
```

RHEL 10

Installazione del GDRCopy

1. Installare le dipendenze richieste.

```
$ sudo yum -y install dkms rpm-build make check check-devel
```

2. Scarica ed estrai il pacchetto GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.5.2.tar.gz \
&& tar xf v2.5.2.tar.gz && cd gdrcopy-2.5.2/packages
```

3. Compila i pacchetti RPM di GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-rpm-packages.sh
```

4. Installa i pacchetti RPM di GDRCopy.

```
$ sudo rpm -Uvh gdrcopy-kmod-2.5.2*dkms*.rpm \
&& sudo rpm -Uvh gdrcopy-2.5.2*.rpm \
&& sudo rpm -Uvh gdrcopy-devel-2.5.2*.rpm
```

Fase 5: installazione del software EFA

Installa il EFA-enabled kernel, i driver EFA, Libfabric, il plugin aws-ofi-nccl e lo stack Open MPI necessari per supportare l'EFA sulla tua istanza.

Per installare il software EFA

1. Connettersi all'istanza avviata. Per ulteriori informazioni, consulta Connessione a un'istanza Linux tramite SSH.
2. Scarica i file di installazione del software. I file di installazione del software sono costituiti da un file tarball () compresso. `.tar.gz` Per scaricare l'ultima versione stabile, utilizzare il comando seguente.

   ```
   $ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.50.0.tar.gz
   ```

   È inoltre possibile ottenere l'ultima versione sostituendo il numero della versione con `latest` nel comando qui sopra.
3. (Opzionale) Verifica l'autenticità e l'integrità del file tarball EFA (`.tar.gz`).

   È consigliabile eseguire questa operazione per verificare l'identità dell'autore del software e che il file non sia stato alterato o danneggiato dopo la pubblicazione. Se non desideri verificare il file tarball, ignora questo passaggio.

> **Note**
>
> In alternativa, se preferisci verificare il file tarball utilizzando un checksum MD5 o SHA256, consulta Verifica del programma di installazione EFA utilizzando un checksum.

a. Scarica la chiave pubblica GPG e importala nel tuo keyring.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

Il comando dovrebbe restituire un valore di chiave. Prendere nota del valore della chiave poiché sarà necessario nella fase successiva.

b. Verifica l'impronta digitale della chiave GPG. Esegui questo comando e specifica la chiave valore creata nella fase precedente.

```
$ gpg --fingerprint key_value
```

Il comando dovrebbe restituire un'impronta digitale identica a `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Se l'impronta digitale non corrisponde, non eseguire lo script di installazione EFA e contatta Supporto.

c. Scarica il file di firma e verifica la firma del file tarball EFA.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.50.0.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.50.0.tar.gz.sig
```

Di seguito viene mostrato l'output di esempio.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Se il risultato include `Good signature` e se l'impronta digitale corrisponde a quella restituita nel passaggio precedente, procedi alla fase successiva. In caso contrario, non eseguire lo script di installazione EFA e contatta Supporto.

4. Estrarre i file dal file `.tar.gz` compresso e andare alla directory estratta.

```
$ tar -xf aws-efa-installer-1.50.0.tar.gz && cd aws-efa-installer
```

5. (Facoltativo) Verificate le firme dei singoli pacchetti durante l'installazione.

A partire da EFA installer 1.48.0, l'installatore include GPG-signed singoli pacchetti RPM e DEB. Per verificare l'autenticità e l'integrità di ogni singolo pacchetto durante l'installazione, usa il flag. `--check-signatures` Quando abiliti questo flag, il programma di installazione verifica prima tutte le firme dei pacchetti e procede con l'installazione solo se ogni pacchetto supera la verifica. Se un pacchetto non supera la verifica, il programma di installazione esce immediatamente senza installare nulla.

a. Scarica la chiave pubblica GPG.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key
```

b. Esporta il percorso chiave. Quindi, nel passaggio successivo, aggiungete `--check-signatures` al comando di installazione e usate `sudo -E` invece che `sudo` per preservare la variabile di ambiente.

```
$ export EFA_INSTALLER_KEY=$(pwd)/aws-efa-installer.key
```

RPM-based Sui sistemi (Amazon Linux 2023, RHEL, Rocky Linux e SUSE), il programma di installazione verifica ogni RPM utilizzando. `rpm --checksig` DEB-based Sui sistemi (Ubuntu, Debian), l'installatore verifica ogni DEB utilizzando la verifica della firma GPG. Se la verifica di un pacchetto fallisce, l'installazione si interrompe immediatamente.

> **Note**
>
> Il `--check-signatures` contrassegno è opzionale. Senza di esso, l'installatore non esegue la verifica della firma individuale.

6. Eseguire lo script di installazione del software EFA.

> **Note**
>
> Se avete completato il passaggio opzionale precedente per impostare la verifica della firma del pacchetto, aggiungetelo `--check-signatures` al comando di installazione e usate `sudo -E` al posto di. `sudo` Ad esempio: `sudo -E ./efa_installer.sh -y --mpi=openmpi5 --check-signatures`.

> **Note**
>
> A partire da EFA 1.30.0, sia Open MPI 4.1 che Open MPI 5 sono installati per impostazione predefinita. A meno che tu non abbia bisogno di Open MPI 4.1, installa solo Open MPI 5. Il comando seguente installa solo Open MPI 5. Se desideri installare Open MPI 4.1 e Open MPI 5, rimuovi. `--mpi=openmpi5`

```
$ sudo ./efa_installer.sh -y --mpi=openmpi5
```

Libfabric è installato nella directory `/opt/amazon/efa`. Il plug-in aws-ofi-nccl è installato nella directory `/opt/amazon/ofi-nccl`. Open MPI è installato nella directory `/opt/amazon/openmpi`.

7. Se il programma di installazione di EFA richiede il riavvio dell'istanza, eseguire questa operazione e riconnettersi all'istanza. In caso contrario, disconnettersi dall'istanza e quindi accedere di nuovo per completare l'installazione.
8. Verificare che il software EFA sia stato installato correttamente.

```
$ fi_info -p efa -t FI_EP_RDM
```

Il comando deve restituire informazioni sulle interfacce EFA Libfabric.

Fase 6: installare NCCL

Installare NCCL. Per ulteriori informazioni su NCCL, consulta il repository NCCL.

Per installare NCCL

1. Passa alla directory `/opt`.

```
$ cd /opt
```

2. Clonare il repository NCCL ufficiale sull'istanza e navigare nel repository clonato locale.

```
$ sudo git clone https://github.com/NVIDIA/nccl.git -b v2.30.4-1 && cd nccl
```

3. Creare e installare NCCL e specificare la directory di installazione CUDA.

```
$ sudo make -j src.build CUDA_HOME=/usr/local/cuda-13
```

Fase 7: installare i test NCCL

Installare i test NCCL. I test NCCL consentono di confermare che NCCL sia installato correttamente e che funzioni come previsto. Per ulteriori informazioni sui test NCCL, consulta il repository nccl-tests.

Per installare i test NCCL

1. Passare alla home directory.

```
$ cd $HOME
```

2. Clonare il repository nccl-tests ufficiale sull'istanza e navigare nel repository clonato locale.

```
$ git clone https://github.com/NVIDIA/nccl-tests.git && cd nccl-tests
```

3. Aggiungere la directory Libfabric alla variabile `LD_LIBRARY_PATH`.

   - Amazon Linux 2023

   ```
   $ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
   ```

   - Ubuntu e Debian

   ```
   $ export LD_LIBRARY_PATH=/opt/amazon/efa/lib:$LD_LIBRARY_PATH
   ```

   - REGOLA 10

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
```

4. Installare i test NCCL e specificare le directory di installazione MPI, NCCL e CUDA.

```
$ make MPI=1 MPI_HOME=/opt/amazon/openmpi NCCL_HOME=/opt/nccl/build CUDA_HOME=/usr/
local/cuda-13
```

Fase 8: testare la configurazione EFA e NCCL

Eseguire un test per accertare che l'istanza temporanea sia configurata adeguatamente per EFA e NCCL.

Per testare la configurazione EFA ed NCCL

1. Creare un file host che specifichi gli host su cui eseguire i test. Il comando seguente crea un file di host denominato `my-hosts` che include un riferimento all'istanza stessa.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   meta-data/local-ipv4 >> my-hosts
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-
   hosts
   ```

2. Esegui il test NCCL. Il comando seguente presuppone che siano presenti 8 GPU per istanza. Regola i `-N` valori `-n` e in base al tipo di istanza.

   ```
   $ /opt/amazon/openmpi/bin/mpirun \
   -x FI_EFA_USE_DEVICE_RDMA=1 \
   -x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/lib:/
   opt/amazon/openmpi/lib:/opt/amazon/ofi-nccl/lib:$LD_LIBRARY_PATH \
   -x NCCL_DEBUG=INFO \
   --hostfile my-hosts -n 8 -N 8 \
   ```

```
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to none
 \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. È possibile confermare che EFA sia attivo come provider sottostante per NCCL quando viene stampato il log `NCCL_DEBUG`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

Le seguenti informazioni aggiuntive vengono visualizzate quando si utilizza un'istanza `p4d.24xlarge`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
 NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-
ofi-nccl/xml/p4d-24xl-topo.xml
```

Fase 9: installare applicazioni di machine learning

Installa le applicazioni di machine learning sull'istanza temporanea. La procedura di installazione varia in base alla specifica applicazione di machine learning. Per ulteriori informazioni sull'installazione del software sulla tua istanza Linux, consulta Gestire gli aggiornamenti del sistema operativo nella Guida per l'utente di Amazon Linux 2023.

> **Note**
>
> Per le istruzioni di installazione, consulta la documentazione dell'applicazione di machine learning.

Passaggio 10: creare un EFA e un'AMI NCCL-enabled

Dopo aver installato i componenti software richiesti, crei un'AMI che puoi riutilizzare per avviare le tue EFA-enabled istanze.

Per creare un'AMI dall'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).

3. Seleziona l'istanza temporanea creata e seleziona Actions (Operazioni), Image (Immagine), Create Image (Crea immagine).
4. Per Create image (Crea immagine), effettua le seguenti operazioni:
   a. In Image name (Nome immagine), immettere un nome descrittivo per l'AMI.
   b. (Facoltativo) In Image description (Descrizione immagine), inserire una breve descrizione dell'AMI.
   c. Scegliere Create Image (Crea immagine).
5. Nel riquadro di navigazione scegliere AMIs (AMI).
6. Individua l'AMI che hai creato nell'elenco. Prima di procedere con la fase seguente, attendere che lo stato passi da `pending` a `available`.

Fase 11: terminare l'istanza temporanea

A questo punto l'istanza temporanea avviata non è più necessaria. È possibile terminare l'istanza per evitare di incorrere in costi aggiuntivi.

Per terminare l'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza temporanea creata, quindi scegliere Actions (Operazioni), Instance state (Stato istanza), Terminate instance (Termina istanza).
4. Quando viene richiesta la conferma, seleziona Termina.

Fase 12: Avvia l'EFA e NCCL-enabled le istanze in un gruppo di collocamento del cluster

Avvia l'EFA e NCCL-enabled le istanze in un gruppo di posizionamento del cluster utilizzando l' EFA-enabledAMI e il gruppo di EFA-enabled sicurezza che hai creato in precedenza.

> **Note**
>
> - Non è un requisito assoluto avviare le EFA-enabled istanze in un gruppo di collocamento del cluster. Tuttavia, consigliamo di eseguire le EFA-enabled istanze in un gruppo di

posizionamento del cluster in quanto avvia le istanze in un gruppo a bassa latenza in una singola zona di disponibilità.

- Per garantire che la capacità sia disponibile durante il dimensionamento delle istanze del cluster, è possibile creare una prenotazione della capacità per il gruppo di collocazione cluster. Per ulteriori informazioni, consulta Utilizza Capacity Reservations con gruppi di collocamento.

New console

Per avviare un'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e quindi scegli Launch instances (Avvia istanze) per aprire la nuova procedura guidata di avvio dell'istanza.
3. (Opzionale) Nella sezione Name and tags (Nome e tag), fornisci un nome per l'istanza, ad esempio `EFA-instance`. Il nome viene assegnato all'istanza come tag di risorsa (`Name=`*`EFA-instance`*).
4. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), scegli My AMIs (Le mie AMI), quindi seleziona l'AMI creata nella fase precedente.
5. Nella sezione Instance type (Tipo di istanza), seleziona `p3dn.24xlarge` o `p4d.24xlarge`.
6. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da utilizzare per l'istanza.
7. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica) e quindi esegui le operazioni qui descritte:

   a. Per Subnet (Sottorete) seleziona la subnet in cui avviare l'istanza. Se non selezioni una sottorete, non puoi abilitare l'istanza per l'EFA.

   b. Per Firewall (security groups) (Firewall [gruppi di sicurezza]), scegli Select existing security group (Seleziona gruppo di sicurezza esistente) e quindi seleziona il gruppo di sicurezza creato nella fase precedente.

   c. Espandi la sezione Configurazione avanzata.

      Come Interfaccia di rete 1, seleziona Indice della scheda di rete = 0, Indice dispositivo = 0 e Tipo di interfaccia = EFA con ENA.

(Facoltativo) Se utilizzi un tipo di istanza con più schede, ad esempio `p4d.24xlarge` orp`5.48xlarge`, per ogni interfaccia di rete aggiuntiva richiesta, scegli Aggiungi interfaccia di rete, per Indice delle schede di rete seleziona il successivo indice non utilizzato, quindi seleziona Indice dispositivo = 1 e Tipo di interfaccia = EFA con ENA o. EFA-only

8. (Opzionale) Nella sezione Storage (Archiviazione), configura i volumi secondo necessità.
9. Nella sezione Advanced details (Dettagli avanzati), per Placement group name (Nome del gruppo di collocazione), seleziona il gruppo di collocazione cluster in cui avviare l'istanza. Se occorre creare un nuovo gruppo di collocazione cluster, scegli Create new placement group (Crea nuovo gruppo di collocazione).
10. Nel pannello Riepilogo a destra, per Numero di istanze, inserisci il numero di EFA-enabled istanze che desideri avviare, quindi scegli Avvia istanza.

Old console

Per avviare l'EFA e le NCCL-enabled istanze in un gruppo di collocamento del cluster

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Launch Instance (Avvia istanza).
3. Nella pagina Choose an AMI (Scegli un'AMI), seleziona My AMIs (Le mie AMI), trova l'AMI creata in precedenza e quindi scegli Select (Seleziona).
4. Nella pagina Choose an Instance Type (Scegli il tipo di istanza), seleziona p3dn.24xlarge e scegli Next: Configure Instance Details (Fase successiva: configurazione dei dettagli dell'istanza).
5. Nella pagina Configure Instance Details (Configura i dettagli dell'istanza), procedere come segue:

   a. Per Numero di istanze, inserisci il numero di EFA e NCCL-enabled le istanze che desideri avviare.

   b. In Network (Rete) e Subnet (Sottorete), selezionare il VPC e la sottorete in cui avviare le istanze.

   c. In Placement group (Gruppo di posizionamento), selezionare la casella Add instance to placement group (Aggiungi istanza a gruppo di posizionamento).

d. In Placement group name (Nome del gruppo di posizionamento), selezionare Add to a new placement group (Aggiungi a un nuovo gruppo di posizionamento) e immettere un nome descrittivo per il gruppo di posizionamento. Quindi, in Placement group strategy (Strategia gruppo di posizionamento), selezionare Cluster.

e. In EFA, scegliere Enable (Abilita).

f. Nella sezione Network Interfaces (Interfacce di rete), per il dispositivo eth0 scegliere New network interface (Nuova interfaccia di rete). Facoltativamente, è possibile specificare un indirizzo IPv4 primario e uno o più indirizzi IPv4 secondari. Se l'istanza viene avviata in una sottorete alla quale è associato un blocco CIDR IPv6, è possibile specificare un indirizzo IPv6 primario e uno o più indirizzi IPv6 secondari.

g. Scegliere Next: Add Storage (Successivo: aggiungi storage).

6. Nella pagina Add archiviazione (Aggiungi archiviazione), specificare i volumi da collegare all'istanza, oltre a quelli specificati dall'AMI (ad esempio il volume del dispositivo di root). Quindi selezionare Next: Add Tags (Fase successiva: aggiungere tag).
7. Nella pagina Add Tags (Aggiungi tag) specificare i tag per l'istanza, ad esempio un nome intuitivo, quindi selezionare Next: Configure Security Group (Successivo: configurazione del gruppo di sicurezza).
8. Nella pagina Configure Security Group (Configura gruppo di sicurezza), scegliere Assign a security group (Assegna un gruppo di sicurezza), selezionare Select an existing security group (Seleziona un gruppo di sicurezza esistente) e quindi selezionare il gruppo di sicurezza creato in precedenza.
9. Scegliere Review and Launch (Analizza e avvia).
10. Nella pagina Review Instance Launch (Verifica avvio istanza) controllare le impostazioni e selezionare Launch (Avvia) per scegliere una coppia di chiavi e avviare l'istanza.

Fase 13: abilitare SSH senza password

> **Note**
>
> L'utente SSH predefinito varia in base al sistema operativo: `ubuntu` per Ubuntu, per Debian, `admin` `ec2-user` per Amazon Linux e RHEL.

Per consentire l'esecuzione delle applicazioni in tutte le istanze del cluster, è necessario abilitare l'accesso SSH senza password dal nodo leader ai nodi membro. Il nodo principale è l'istanza da cui vengono eseguite le applicazioni. Le restanti istanze del cluster sono i nodi membro.

Per abilitare SSH senza password tra le istanze del cluster

1. Selezionare un'istanza nel cluster come nodo principale e connettersi a essa.
2. Disabilita `strictHostKeyChecking` e abilita `ForwardAgent` sul nodo principale. Aprire il file `~/.ssh/config` utilizzando qualsiasi editor di testo e aggiungere il seguente script.

   ```
   Host *
       ForwardAgent yes
   Host *
       StrictHostKeyChecking no
   ```

3. Generare una coppia di chiavi RSA.

   ```
   $ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
   ```

   La coppia di chiavi viene creata nella directory `$HOME/.ssh/`.
4. Modifica le autorizzazioni della chiave privata sul nodo principale.

   ```
   $ chmod 600 ~/.ssh/id_rsa
   chmod 600 ~/.ssh/config
   ```

5. Aprire `~/.ssh/id_rsa.pub` utilizzando l'editor di testo preferito e copiare la chiave.
6. Per ogni nodo membro nel cluster, procedere nel modo seguente:

   a. Collegarsi all'istanza.

   b. Aprire `~/.ssh/authorized_keys` utilizzando qualsiasi editor di testo e aggiungere la chiave pubblica copiata in precedenza.
7. Per verificare che SSH senza password funzioni come previsto, connettersi al nodo leader ed eseguire il seguente comando.

   ```
   $ ssh member_node_private_ip
   ```

   La connessione al nodo membro non dovrebbe richiedere una chiave o una password.

Inizia a usare EFA e NIXL per i carichi di lavoro di inferenza su Amazon EC2

La libreria NVIDIA Inference Xfer (NIXL) è una libreria di comunicazione ad alto rendimento e bassa latenza progettata specificamente per carichi di lavoro di inferenza disaggregati. NIXL può essere utilizzato insieme a EFA e Libfabric per supportare il KV-cache trasferimento tra nodi di precompilazione e decodifica e consente uno spostamento efficiente tra vari livelli di storage. KV-cache Per ulteriori informazioni, consulta il sito web NIXL. https://github.com/ai-dynamo/nixl

Requisiti

- Sono supportate solo le AMI di base di Ubuntu 24.04 e Ubuntu 22.04.
- EFA supporta solo NIXL 1.0.0 e versioni successive.

Fase 1: Preparare un gruppo di sicurezza EFA-enabled

Un EFA richiede un gruppo di sicurezza in cui sia consentito tutto il traffico in entrata e in uscita dal gruppo stesso. La procedura seguente crea un gruppo di sicurezza che consente tutto il traffico in entrata e in uscita da e verso se stesso e che consente il traffico SSH in entrata da qualsiasi indirizzo IPv4 per la connettività SSH.

> **Important**
>
> Questo gruppo di sicurezza è destinato esclusivamente a scopi di test. Per i tuoi ambienti di produzione, consigliamo di creare una regola SSH in entrata che consenta il traffico solo dall'indirizzo IP da cui ti connetti, ad esempio l'indirizzo IP del tuo computer o un intervallo di indirizzi IP nella tua rete locale.

Per altri scenari, consulta Regole del gruppo di sicurezza per diversi casi d'uso.

Per creare un gruppo EFA-enabled di sicurezza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Security Groups (Gruppi di sicurezza) e quindi Create Security Group (Crea gruppo di sicurezza).
3. Nella finestra Create Security Group (Crea gruppo di sicurezza) effettuare le operazioni seguenti:

a. In Nome gruppo di sicurezza, immettere un nome descrittivo per il gruppo di sicurezza, ad esempio `EFA-enabled security group`.

b. (Facoltativo) In Description (Descrizione), inserire una breve descrizione del gruppo di sicurezza.

c. Per VPC, seleziona il VPC in cui intendi avviare le tue EFA-enabled istanze.

d. Scegliere Create Security Group (Crea gruppo di sicurezza).

4. Seleziona il gruppo di sicurezza creato e nella scheda Details (Dettagli) copia il valore Security group ID (ID gruppo di sicurezza).

5. Dopo aver selezionato il gruppo di sicurezza, scegli Actions (Operazioni), Edit inbound rules (Modifica le regole in entrata) ed esegui le operazioni di seguito:

   a. Scegliere Add rule (Aggiungi regola).

   b. In Type (Tipo), selezionare All traffic (Tutto il traffico).

   c. Per Source type (Tipo di origine), scegli Custom (Personalizzata) e incolla nel campo l'ID del gruppo di sicurezza copiato in precedenza.

   d. Scegli Aggiungi regola.

   e. Per Type (Tipo) scegli SSH.

   f. Per Source (origine), scegli Anywhere-IPv4.

   g. Scegliere Salva regole.

6. Dopo aver selezionato il gruppo di sicurezza, scegli Actions (Operazioni), Edit outbound rules (Modifica le regole in uscita) ed esegui le operazioni di seguito:

   a. Scegliere Add rule (Aggiungi regola).

   b. In Type (Tipo), selezionare All traffic (Tutto il traffico).

   c. Per Destination type (Tipo di destinazione), scegli Custom (Personalizzata) e incolla nel campo l'ID del gruppo di sicurezza copiato in precedenza.

   d. Scegliere Salva regole.

> **Important**
>
> Le regole autoreferenziali in entrata e in uscita (che consentono tutto il traffico da e verso il gruppo di sicurezza stesso) sono obbligatorie per il funzionamento dell'EFA. Senza queste regole, il traffico EFA tra le istanze verrà bloccato.

Fase 2: avviare un'istanza temporanea

Avvia un'istanza temporanea da utilizzare per installare e configurare i componenti software EFA. Utilizzi questa istanza per creare un' EFA-enabled AMI da cui avviare le tue EFA-enabled istanze.

Per avviare un'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e quindi scegli Launch instances (Avvia istanze) per aprire la nuova procedura guidata di avvio dell'istanza.
3. (Opzionale) Nella sezione Name and tags (Nome e tag), fornisci un nome per l'istanza, ad esempio `EFA-instance`. Il nome viene assegnato all'istanza come tag di risorsa (`Name=EFA-instance`).
4. Nella sezione Immagini di applicazioni e sistema operativo, seleziona un'AMI per uno dei sistemi operativi supportati. Puoi anche selezionare un DLAMI supportato che si trova nella pagina delle note di rilascio del DLAMI.
5. Nella sezione Tipo di istanza, seleziona un tipo di istanza supportato.
6. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da utilizzare per l'istanza.
7. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica) e quindi esegui le operazioni qui descritte:

   a. Per Subnet (Sottorete) seleziona la subnet in cui avviare l'istanza. Se non selezioni una sottorete, non puoi abilitare l'istanza per l'EFA.

   b. Per Firewall (security groups) (Firewall [gruppi di sicurezza]), scegli Select existing security group (Seleziona gruppo di sicurezza esistente) e quindi seleziona il gruppo di sicurezza creato nella fase precedente.

   c. Espandi la sezione Configurazione avanzata.

      Come Interfaccia di rete 1, seleziona Indice della scheda di rete = 0, Indice dispositivo = 0 e Tipo di interfaccia = EFA con ENA.

(Facoltativo) Se utilizzi un tipo di istanza multischeda, ad esempio `p4d.24xlarge` o`p5.48xlarge`, per ogni interfaccia di rete aggiuntiva richiesta, scegli Aggiungi interfaccia di rete, per Indice delle schede di rete seleziona il successivo indice non utilizzato, quindi seleziona Indice dispositivo = 1 e Tipo di interfaccia = EFA con ENA o. EFA-only

8. Nella sezione Storage (Archiviazione), configura i volumi secondo necessità.

> **Note**
>
> Devi effettuare un provisioning aggiuntivo di 10-20 GiB di spazio di archiviazione per Nvidia CUDA Toolkit. Se non effettui il provisioning di uno spazio di archiviazione sufficiente, riceverai un errore `insufficient disk space` durante il tentativo di installare i driver Nvidia e il toolkit CUDA.

9. Nel pannello Summary (Riepilogo) a destra, scegli Launch instance (Avvia istanza).

> **Important**
>
> Salta il passaggio 3 se la tua AMI include già i driver GPU Nvidia, il toolkit CUDA e cuDNN o se stai utilizzando un'istanza non GPU.

Fase 3: installare driver GPU Nvidia, il kit di strumenti Nvidia CUDA e cuDNN

Per installare driver GPU Nvidia, il kit di strumenti Nvidia CUDA e cuDNN

1. Per verificare che tutti i pacchetti software siano aggiornati, eseguire un aggiornamento rapido del software sull'istanza.

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

2. Installare le utilità che sono richieste per installare i driver GPU Nvidia e il toolkit CUDA Nvidia.

```
$ sudo apt-get install build-essential -y
```

3. Per utilizzare il driver GPU Nvidia, è necessario prima disabilitare i driver open source `nouveau`.

   a. Installare le utility richieste e il pacchetto delle intestazioni kernel per la versione del kernel attualmente in esecuzione.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

b. Aggiungere nouveau al file dell'elenco dei `/etc/modprobe.d/blacklist.conf` negati.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

c. Aprire il file `/etc/default/grub` utilizzando qualsiasi editor di testo e aggiungere il seguente script.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

d. Ricompilare il file di configurazione di Grub.

```
$ sudo update-grub
```

4. Riavviare l'istanza e riconnettersi a essa.
5. Aggiungere il repository CUDA e installare i driver GPU Nvidia, il toolkit NVIDIA CUDA e cuDNN.

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/
compute/machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/repos/
ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-dkms-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535 cuda-
toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

6. Riavviare l'istanza e riconnettersi a essa.
7. (Solo `p4d.24xlarge` e `p5.48xlarge`) Installare Nvidia Fabric Manager.

   a. È necessario installare la versione di Nvidia Fabric Manager che corrisponde alla versione del modulo del kernel Nvidia installata al passaggio precedente.

      Eseguire questo comando per determinare la versione del modulo del kernel Nvidia.

      ```
      $ cat /proc/driver/nvidia/version | grep "Kernel Module"
      ```

      Di seguito è riportato un output di esempio.

      ```
      NVRM version: NVIDIA UNIX x86_64 Kernel Module  450.42.01  Tue Jun 15 21:26:37
       UTC 2021
      ```

      Nell'esempio precedente, è stata installata la versione principale `450` del modulo del kernel. Ciò significa che è necessario installare la versione `450` di Nvidia Fabric Manager.

   b. Installare Nvidia Fabric Manager. Eseguire questo comando e specificare la versione principale identificata nella fase precedente.

      ```
      $ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
      fabricmanager-major_version_number
      ```

      Ad esempio, se è stata installata la versione principale `450` del modulo del kernel, utilizzare il seguente comando per installare la versione corrispondente di Nvidia Fabric Manager.

      ```
      $ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
      fabricmanager-450
      ```

   c. Avviare il servizio e assicurarsi che venga avviato automaticamente all'avvio dell'istanza. Nvidia Fabric Manager è necessario per la gestione degli switch NV.

      ```
      $ sudo systemctl start nvidia-fabricmanager && sudo systemctl enable nvidia-
      fabricmanager
      ```

8. Assicurarsi che i percorsi CUDA siano impostati ogni volta che viene avviata l'istanza.

   - Per le shell bash, aggiungere le seguenti istruzioni a `/home/username/.bashrc` e `/home/username/.bash_profile`.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/lib64:
$LD_LIBRARY_PATH
```

- Per le shell tcsh, aggiungere le seguenti istruzioni a /home/*username*/.cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/lib64:
$LD_LIBRARY_PATH
```

9. Per confermare che i driver GPU di Nvidia GPU siano funzionanti, eseguire questo comando.

```
$ nvidia-smi -q | head
```

Il comando deve restituire le informazioni sulle GPU Nvidia, sui driver GPU Nvidia e su Nvidia CUDA toolkit.

> **Important**
>
> Salta il passaggio 4 se la tua AMI include già GDRCopy o se stai usando un'istanza non GPU.

Fase 4: installazione del GDRCopy

Installa GDRCopy per migliorare le prestazioni di Libfabric sulle piattaforme. GPU-based Per ulteriori informazioni su GDRCopy, consulta il repository GDRCopy.

Installazione del GDRCopy

1. Installare le dipendenze richieste.

```
$ sudo apt -y install build-essential devscripts debhelper check libsubunit-dev
 fakeroot pkg-config dkms
```

2. Scarica ed estrai il pacchetto GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz \
```

```
&& cd gdrcopy-2.4/packages
```

3. Compila i pacchetti DEB di GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-deb-packages.sh
```

4. Installa i pacchetti DEB di GDRCopy.

```
$ sudo dpkg -i gdrdrv-dkms_2.4-1_amd64.*.deb \
&& sudo dpkg -i libgdrapi_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy-tests_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy_2.4-1_amd64.*.deb
```

> **Important**
>
> Salta il passaggio 5 se la tua AMI include già l'ultimo programma di installazione EFA.

Fase 5: installazione del software EFA

Installa il EFA-enabled kernel, i driver EFA e lo stack Libfabric necessari per supportare EFA sulla tua istanza.

Per installare il software EFA

1. Connettersi all'istanza avviata. Per ulteriori informazioni, consulta Connessione a un'istanza Linux tramite SSH.
2. Scarica i file di installazione del software. I file di installazione del software sono riuniti in un file (`.tar.gz`) tarball compresso. Per scaricare l'ultima versione stabile, utilizzare il comando seguente.

```
$ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.50.0.tar.gz
```

3. Estrai i file dal `.tar.gz` file compresso, elimina il tarball e naviga nella directory estratta.

```
$ tar -xf aws-efa-installer-1.50.0.tar.gz && rm -rf aws-efa-installer-1.50.0.tar.gz
 && cd aws-efa-installer
```

4. (Facoltativo) Verificate le firme dei singoli pacchetti durante l'installazione.

A partire da EFA installer 1.48.0, l'installatore include GPG-signed singoli pacchetti RPM e DEB. Per verificare l'autenticità e l'integrità di ogni singolo pacchetto durante l'installazione, usa il flag. `--check-signatures` Quando abiliti questo flag, il programma di installazione verifica prima tutte le firme dei pacchetti e procede con l'installazione solo se ogni pacchetto supera la verifica. Se un pacchetto non supera la verifica, il programma di installazione esce immediatamente senza installare nulla.

a. Scarica la chiave pubblica GPG.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key
```

b. Esporta il percorso chiave. Quindi, nel passaggio successivo, aggiungete `--check-signatures` al comando di installazione e usate `sudo -E` invece che `sudo` per preservare la variabile di ambiente.

```
$ export EFA_INSTALLER_KEY=$(pwd)/aws-efa-installer.key
```

RPM-based Sui sistemi (Amazon Linux, RHEL, Rocky Linux e SUSE), il programma di installazione verifica ogni RPM utilizzando. `rpm --checksig` DEB-based Sui sistemi (Ubuntu, Debian), l'installatore verifica ogni DEB utilizzando la verifica della firma GPG.

Se la verifica di un pacchetto fallisce, l'installazione si interrompe immediatamente, proteggendo il sistema da pacchetti danneggiati o dannosi.

> **Note**
>
> La `--check-signatures` bandiera è opzionale. Senza di esso, l'installatore non esegue la verifica della firma individuale.

5. Eseguire lo script di installazione del software EFA.

> **Note**
>
> Se avete completato il passaggio opzionale precedente per impostare la verifica della firma del pacchetto, aggiungetelo `--check-signatures` al comando di installazione e

usate `sudo -E` al posto di. `sudo` Ad esempio: `sudo -E ./efa_installer.sh -y --check-signatures`.

```
$ sudo ./efa_installer.sh -y
```

Libfabric è installato nella directory `/opt/amazon/efa`.

6. Se il programma di installazione di EFA richiede il riavvio dell'istanza, eseguire questa operazione e riconnettersi all'istanza. In caso contrario, disconnettersi dall'istanza e quindi accedere di nuovo per completare l'installazione.
7. Verificare la corretta installazione dei componenti software EFA.

```
$ fi_info -p efa -t FI_EP_RDM
```

Il comando deve restituire informazioni sulle interfacce EFA Libfabric. L'esempio seguente mostra l'output del comando.

- `p3dn.24xlarge` con interfaccia di rete singola

```
provider: efa
fabric: EFA-fe80::94:3dff:fe89:1b70
domain: efa_0-rdm
version: 2.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

- `p4d.24xlarge` e `p5.48xlarge` con più interfacce di rete

```
provider: efa
fabric: EFA-fe80::c6e:8fff:fef6:e7ff
domain: efa_0-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c34:3eff:feb2:3c35
domain: efa_1-rdm
version: 111.0
type: FI_EP_RDM
```

```
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c0f:7bff:fe68:a775
domain: efa_2-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::ca7:b0ff:fea6:5e99
domain: efa_3-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

Passaggio 6: installare NIXL

Installa NIXL. Per ulteriori informazioni su NIXL, consulta il repository NIXL.

Pre-built distributions

Per installare NIXL usando PyPI

1. Installare le dipendenze richieste.

```
$ sudo apt install pip
```

2. Installa NIXL.

```
$ pip install nixl
```

Build from source

Per compilare e installare NIXL dal codice sorgente

1. Installare le dipendenze richieste.

```
$ sudo apt install cmake pkg-config meson pybind11-dev libaio-dev nvidia-cuda-
toolkit pip libhwloc-dev \
&& pip install meson ninja pybind11
```

2. Passare alla home directory.

```
$ cd $HOME
```

3. Clona il repository NIXL ufficiale sull'istanza e accedi al repository clonato locale.

```
$ sudo git clone https://github.com/ai-dynamo/nixl.git && cd nixl
```

4. Crea e installa NIXL e specifica il percorso della directory di installazione di Libfabric.

```
$ sudo meson setup . nixl --prefix=/usr/local/nixl -Dlibfabric_path=/opt/amazon/
efa
$ cd nixl && sudo ninja && sudo ninja install
```

Passo 7: Installa NIXL Benchmark e testa la tua configurazione EFA e NIXL

Installa NIXL Benchmark ed esegui un test per assicurarti che l'istanza temporanea sia configurata correttamente per EFA e NIXL. Il benchmark NIXL consente di confermare che NIXL sia installato correttamente e che funzioni come previsto. Per ulteriori informazioni, consulta il repository nixlbench.

NIXL Benchmark (nixlbench) richiede l'ETCD per il coordinamento tra client e server. Per utilizzare ETCD con NIXL sono necessari ETCD Server and Client e l'API ETCD CPP.

Build from Docker

Per installare e testare NIXL Benchmark utilizzando Docker

1. Clona il repository NIXL ufficiale sull'istanza e vai alla directory di build di nixlbench.

```
$ git clone https://github.com/ai-dynamo/nixl.git
$ cd nixl/benchmark/nixlbench/contrib
```

2. Compila il container.

```
$ ./build.sh
```

Per ulteriori informazioni sulle opzioni di compilazione di Docker, consulta il repository nixlbench. https://github.com/ai-dynamo/nixl/tree/main/benchmark/nixlbench

3. Installazione di Docker.

```
$ sudo apt install docker.io -y
```

4. Avviate il server ETCD per il coordinamento.

```
$ docker run -d --name etcd-server \
    -p 2379:2379 -p 2380:2380 \
    quay.io/coreos/etcd:v3.5.18 \
    /usr/local/bin/etcd \
    --data-dir=/etcd-data \
    --listen-client-urls=http://0.0.0.0:2379 \
    --advertise-client-urls=http://0.0.0.0:2379 \
    --listen-peer-urls=http://0.0.0.0:2380 \
    --initial-advertise-peer-urls=http://0.0.0.0:2380 \
    --initial-cluster=default=http://0.0.0.0:2380
```

5. Verificare che il server ETCD sia in esecuzione.

```
$ curl -L http://localhost:2379/health
```

Output previsto:

```
{"health":"true"}
```

6. Aprire due terminali per l'istanza. Su entrambi i terminali, esegui il seguente comando per verificare l'installazione. Il comando utilizza il server ETCD sulla stessa istanza, utilizza Libfabric come backend e funziona utilizzando la memoria GPU.

```
$ docker run -it --gpus all --network host nixlbench:latest \
    nixlbench --etcd_endpoints http://localhost:2379 \
    --backend LIBFABRIC \
    --initiator_seg_type VRAM \
    --target_seg_type VRAM
```

> **Note**
>
> Usa il valore `DRAM` invece che per le istanze non GPU. `VRAM`

Build from source

> **Important**
>
> Segui questa scheda solo se hai scelto Crea dal codice sorgente nel passaggio 6.

Per installare NIXL Benchmark

1. Installa le dipendenze di sistema richieste.

```
$ sudo apt install libgflags-dev
```

2. Installare il server e il client ETCD.

```
$ sudo apt install -y etcd-server etcd-client
```

3. Installa l'API CPP ETCD.

   a. Installa le dipendenze richieste per l'API CPP ETCD.

```
$ sudo apt install libboost-all-dev libssl-dev libgrpc-dev libgrpc++-dev
 libprotobuf-dev protobuf-compiler-grpc libcpprest-dev
```

   b. Clona e installa l'API CPP ETCD.

```
$ cd $HOME
$ git clone https://github.com/etcd-cpp-apiv3/etcd-cpp-apiv3.git
$ cd etcd-cpp-apiv3
$ mkdir build && cd build
$ cmake ..
$ sudo make -j$(nproc) && sudo make install
```

4. Compila e installa nixlbench.

```
$ sudo meson setup . $HOME/nixl/benchmark/nixlbench -Dnixl_path=/usr/local/nixl/
$ sudo ninja && sudo ninja install
```

Per testare la tua configurazione EFA e NIXL

1. Avviare il server ETCD sull'istanza.

```
$ etcd --listen-client-urls "http://0.0.0.0:2379" \
    --advertise-client-urls "http://localhost:2379" &
```

2. Verificare che il server ETCD sia in esecuzione.

```
$ curl -L http://localhost:2379/health
```

Output previsto:

```
{"health":"true"}
```

3. Aprire due terminali per l'istanza. Su entrambi i terminali, completa i seguenti passaggi per eseguire nixlbench.

a. Vai alla directory in cui è installato nixlbench.

```
$ cd /usr/local/nixlbench/bin/
```

b. Esegui il test e specifica il backend, l'indirizzo del server ETCD e il tipo di segmento dell'iniziatore. Il comando seguente utilizza il server ETCD sulla stessa istanza, utilizza Libfabric come backend e funziona utilizzando la memoria GPU. Le variabili di ambiente configurano quanto segue:

- `NIXL_LOG_LEVEL=INFO`— Abilita un output di debug dettagliato. È inoltre possibile specificare di `WARN` ricevere solo messaggi di errore.
- `LD_LIBRARY_PATH`— Imposta il percorso per la libreria NIXL.

Per ulteriori informazioni sugli argomenti del benchmark NIXL, consulta il README di NIXLBench nel repository ufficiale di nixlbench.

```
$ export NIXL_LOG_LEVEL=INFO
$ export LD_LIBRARY_PATH=/usr/local/nixl/lib/$(gcc -dumpmachine):
$LD_LIBRARY_PATH

$ nixlbench --etcd-endpoints 'http://localhost:2379' \
    --backend 'LIBFABRIC' \
    --initiator_seg_type 'VRAM' \
    --target_seg_type 'VRAM'
```

> **Note**
>
> Usa il `VRAM` valore invece che per le istanze non GPU. `DRAM`

Passaggio 8: installa le tue applicazioni di machine learning

Installa le applicazioni di machine learning sull'istanza temporanea. La procedura di installazione varia in base alla specifica applicazione di machine learning.

> **Note**
>
> Consulta la documentazione dell'applicazione di machine learning per le istruzioni di installazione.

Fase 9: Creare un EFA e un AMI NIXL-enabled

Dopo aver installato i componenti software richiesti, crei un'AMI che puoi riutilizzare per avviare le tue EFA-enabled istanze.

Per creare un'AMI dall'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza temporanea creata e seleziona Actions (Operazioni), Image (Immagine), Create Image (Crea immagine).
4. Per Create image (Crea immagine), effettua le seguenti operazioni:
   a. In Image name (Nome immagine), immettere un nome descrittivo per l'AMI.
   b. (Facoltativo) In Image description (Descrizione immagine), inserire una breve descrizione dell'AMI.
   c. Scegliere Create Image (Crea immagine).
5. Nel riquadro di navigazione scegliere AMIs (AMI).
6. Individua l'AMI che hai creato nell'elenco. Prima di procedere con la fase seguente, attendi che lo stato passi da `pending` a `available`.

Fase 10: terminazione dell'istanza temporanea

A questo punto l'istanza temporanea avviata non è più necessaria. È possibile terminare l'istanza per evitare di incorrere in costi aggiuntivi.

Per terminare l'istanza temporanea

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza temporanea creata, quindi scegliere Actions (Operazioni), Instance state (Stato istanza), Terminate instance (Termina istanza).
4. Quando viene richiesta la conferma, seleziona Termina.

Passaggio 11: avvia EFA e istanze NIXL-enabled

Avvia l'EFA e NIXL-enabled le istanze utilizzando l' EFA-enabled AMI che hai creato nel passaggio 9 e il gruppo di EFA-enabled sicurezza che hai creato nel passaggio 1.

Per avviare l'EFA e le istanze NIXL-enabled

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e quindi scegli Launch instances (Avvia istanze) per aprire la nuova procedura guidata di avvio dell'istanza.
3. (Opzionale) Nella sezione Name and tags (Nome e tag), fornisci un nome per l'istanza, ad esempio `EFA-instance`. Il nome viene assegnato all'istanza come tag di risorsa (`Name=`*`EFA-instance`*).
4. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), scegli My AMIs (Le mie AMI), quindi seleziona l'AMI creata nella fase precedente.
5. Nella sezione Tipo di istanza, seleziona un tipo di istanza supportato.
6. Nella sezione Key pair (Coppia di chiavi), seleziona la coppia di chiavi da utilizzare per l'istanza.
7. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica) e quindi esegui le operazioni qui descritte:

    a. Per Subnet (Sottorete) seleziona la subnet in cui avviare l'istanza. Se non selezioni una sottorete, non puoi abilitare l'istanza per l'EFA.

    b. Per Firewall (gruppi di sicurezza), scegli Seleziona gruppo di sicurezza esistente, quindi seleziona il gruppo di sicurezza che hai creato nel passaggio 1.

c. Espandi la sezione Configurazione avanzata.

   Come Interfaccia di rete 1, seleziona Indice della scheda di rete = 0, Indice dispositivo = 0 e Tipo di interfaccia = EFA con ENA.

   (Facoltativo) Se utilizzi un tipo di istanza con più schede, ad esempio `p4d.24xlarge` o `p5.48xlarge`, per ogni interfaccia di rete aggiuntiva richiesta, scegli Aggiungi interfaccia di rete, per Indice delle schede di rete seleziona il successivo indice non utilizzato, quindi seleziona Indice dispositivo = 1 e Tipo di interfaccia = EFA con ENA o. EFA-only

8. (Opzionale) Nella sezione Storage (Archiviazione), configura i volumi secondo necessità.
9. Nel pannello Riepilogo a destra, per Numero di istanze, inserisci il numero di EFA-enabled istanze che desideri avviare, quindi scegli Avvia istanza.

Fase 12: abilitazione di SSH senza password

Per consentire l'esecuzione delle applicazioni in tutte le istanze del cluster, è necessario abilitare l'accesso SSH senza password dal nodo leader ai nodi membro. Il nodo principale è l'istanza da cui vengono eseguite le applicazioni. Le restanti istanze del cluster sono i nodi membro.

Per abilitare SSH senza password tra le istanze del cluster

1. Selezionare un'istanza nel cluster come nodo principale e connettersi a essa.
2. Disabilita `strictHostKeyChecking` e abilita `ForwardAgent` sul nodo principale. Aprire il file `~/.ssh/config` utilizzando qualsiasi editor di testo e aggiungere il seguente script.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Generare una coppia di chiavi RSA.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

   La coppia di chiavi viene creata nella directory `$HOME/.ssh/`.

4. Modifica le autorizzazioni della chiave privata sul nodo principale.

```
$ chmod 600 ~/.ssh/id_rsa
```

```
chmod 600 ~/.ssh/config
```

5. Aprire `~/.ssh/id_rsa.pub` utilizzando l'editor di testo preferito e copiare la chiave.
6. Per ogni nodo membro nel cluster, procedere nel modo seguente:
   a. Collegarsi all'istanza.
   b. Aprire `~/.ssh/authorized_keys` utilizzando qualsiasi editor di testo e aggiungere la chiave pubblica copiata in precedenza.
7. Per verificare che SSH senza password funzioni come previsto, connettersi al nodo leader ed eseguire il seguente comando.

   ```
   $ ssh member_node_private_ip
   ```

   La connessione al nodo membro non dovrebbe richiedere una chiave o una password.

> **Important**
>
> Segui il passaggio 13 solo se hai seguito il passaggio 7.

Passaggio 13: verifica la configurazione EFA e NIXL su più istanze

Esegui un test per assicurarti che le tue istanze siano configurate correttamente per EFA e NIXL.

Build from Docker

Per testare la configurazione EFA e NIXL su più istanze utilizzando Docker

1. Seleziona due host per eseguire il benchmark nixlbench. Utilizzate l'indirizzo IP del primo host come IP del server ETCD per lo scambio di metadati.
2. Avviare il server ETCD sull'host 1.

   ```
   $ docker run -d --name etcd-server \
       -p 2379:2379 -p 2380:2380 \
       quay.io/coreos/etcd:v3.5.18 \
       /usr/local/bin/etcd \
       --data-dir=/etcd-data \
       --listen-client-urls=http://0.0.0.0:2379 \
       --advertise-client-urls=http://0.0.0.0:2379 \
   ```

```
    --listen-peer-urls=http://0.0.0.0:2380 \
    --initial-advertise-peer-urls=http://0.0.0.0:2380 \
    --initial-cluster=default=http://0.0.0.0:2380
```

3. Verificare che il server ETCD sia in esecuzione.

```
$ curl -L http://localhost:2379/health
```

```
{"health":"true"}
```

4. Esegui il benchmark nixlbench sull'host 1.

```
$ docker run -it --gpus all --network host nixlbench:latest \
    nixlbench --etcd_endpoints http://localhost:2379 \
    --backend LIBFABRIC \
    --initiator_seg_type VRAM
```

5. Esegui il benchmark nixlbench sull'host 2.

```
$ docker run -it --gpus all --network host nixlbench:latest \
    nixlbench --etcd_endpoints http://ETCD_SERVER_IP:2379 \
    --backend LIBFABRIC \
    --initiator_seg_type VRAM
```

Build from source

> **Important**
>
> Segui questa scheda solo se hai scelto Build from source nel passaggio 6.

Per testare la configurazione EFA e NIXL su più istanze

1. Seleziona due host per eseguire il benchmark nixlbench. Utilizzate l'indirizzo IP del primo host come IP del server ETCD per lo scambio di metadati.
2. Avviare il server ETCD sull'host 1.

```
$ etcd --listen-client-urls "http://0.0.0.0:2379" \
    --advertise-client-urls "http://localhost:2379" &
```

3. Verificare che il server ETCD sia in esecuzione.

```
$ curl -L http://localhost:2379/health
```

```
{"health":"true"}
```

4. Esegui il benchmark nixlbench sull'host 1.

```
$ export NIXL_LOG_LEVEL=INFO
$ export LD_LIBRARY_PATH=$HOME/nixl/lib/x86_64-linux-gnu:$LD_LIBRARY_PATH

$ nixlbench \
    --etcd-endpoints http://localhost:2379 \
    --backend LIBFABRIC \
    --initiator_seg_type VRAM
```

5. Esegui il benchmark nixlbench sull'host 2.

```
$ export NIXL_LOG_LEVEL=INFO
$ export LD_LIBRARY_PATH=$HOME/nixl/lib/x86_64-linux-gnu:$LD_LIBRARY_PATH

$ nixlbench \
    --etcd-endpoints http://ETCD_SERVER_IP:2379 \
    --backend LIBFABRIC \
    --initiator_seg_type VRAM
```

Fase 14: Testare l'inferenza disaggregata utilizzata su vLLM (Facoltativo)

Dopo aver installato NIXL, è possibile utilizzare NIXL tramite framework di inferenza e service LLM come vLLM, SGlang e. TensorRT-LLM

Per soddisfare il carico di lavoro di inferenza utilizzando vLLM

1. Installa vLLM.

```
$ pip install vllm
```

2. Avvia il server vLLM con NIXL. I seguenti comandi di esempio creano un'istanza di precompilazione (producer) e una di decodifica (consumer) per la connessione handshake NIXL, il connettore KV, il ruolo KV e il backend di trasporto. Per esempi e script dettagliati,

consulta la Guida all'uso di NIXLConnector. https://github.com/vllm-project/vllm/blob/2d977a7a9ead3179fde9ed55d69393ef7b6cec47/docs/features/nixl_connector_usage.md

Per utilizzare NIXL con EFA, imposta le variabili di ambiente in base alla configurazione e al caso d'uso.

- Configurazione Producer (Prefiller)

```
$ vllm serve your-application \
    --port 8200 \
    --enforce-eager \
    --kv-transfer-config
 '{"kv_connector":"NixlConnector","kv_role":"kv_both","kv_buffer_device":"cuda","kv_conne
{"backends":["LIBFABRIC"]}}'
```

- Configurazione Consumer (Decoder)

```
$ vllm serve your-application \
    --port 8200 \
    --enforce-eager \
    --kv-transfer-config
 '{"kv_connector":"NixlConnector","kv_role":"kv_both","kv_buffer_device":"cuda","kv_conne
{"backends":["LIBFABRIC"]}}'
```

La configurazione di esempio precedente imposta quanto segue:

- `kv_role`to`kv_both`, che consente una funzionalità simmetrica in cui il connettore può fungere sia da produttore che da consumatore. Ciò offre flessibilità per configurazioni e scenari sperimentali in cui la distinzione dei ruoli non è predeterminata.
- `kv_buffer_device`to`cuda`, che consente di utilizzare la memoria GPU.
- Backend NIXL to`LIBFABRIC`, che consente al traffico NIXL di superare l'EFA.

Ottimizzare la larghezza di banda della rete sulle istanze Amazon EC2 con più schede di rete

Molti tipi di istanze che supportano EFA hanno anche più schede di rete. Per ulteriori informazioni, consulta Schede di rete. Se si intende utilizzare EFA con uno di questi tipi di istanza, consigliamo di seguire questa configurazione di base:

- Per l'interfaccia di rete principale (indice delle schede di rete0, indice dei dispositivi0), crea un'interfaccia ENA. Non è possibile utilizzare un'interfaccia EFA-only di rete come interfaccia di rete principale.
- Se l'indice della scheda di rete 0 supporta EFA, crea un'interfaccia di EFA-only rete per l'indice della scheda di rete0, l'indice 1 del dispositivo.
- Per ogni interfaccia di rete aggiuntiva, utilizzate il successivo indice delle schede di rete inutilizzate, l'indice dei dispositivi per l'interfaccia di EFA-only rete0, l'indice dei and/or dispositivi 1 per l'interfaccia di rete ENA a seconda del caso d'uso, ad esempio i requisiti di larghezza di banda ENA o lo spazio degli indirizzi IP. Per casi d'uso di esempio, consultare Configurazione EFA per le istanze P5 e P5e.

> **Note**
>
> Le istanze P5 richiedono una specifica configurazione delle interfacce di rete per garantire la massima larghezza di banda della rete. Per ulteriori informazioni, consulta Configurazione EFA per le istanze P5 e P5e.

I seguenti esempi mostrano come avviare un'istanza in base a questi suggerimenti.

Instance launch

Per specificare gli EFA durante l'avvio di un'istanza utilizzando la procedura guidata di avvio dell'istanza

1. Nella sezione Impostazioni di rete scegli Modifica.
2. Expand Configurazione di rete avanzata.
3. Per l'interfaccia di rete principale (indice delle schede di rete0, indice dei dispositivi0), creare un'interfaccia ENA. Non è possibile utilizzare un'interfaccia EFA-only di rete come interfaccia di rete principale.
4. Se l'indice della scheda di rete 0 supporta EFA, crea un'interfaccia di EFA-only rete per l'indice della scheda di rete0, l'indice 1 del dispositivo.
5. Per ogni interfaccia di rete aggiuntiva, utilizzate il successivo indice delle schede di rete inutilizzate, l'indice dei dispositivi per l'interfaccia di EFA-only rete0, l'indice dei and/or dispositivi 1 per l'interfaccia di rete ENA a seconda del caso d'uso, ad esempio i requisiti di

larghezza di banda ENA o lo spazio degli indirizzi IP. Per casi d'uso di esempio, consultare Configurazione EFA per le istanze P5 e P5e.

Per specificare gli EFA durante l'avvio dell'istanza, utilizzare run-instances command

Per `--network-interfaces`, specifica il numero di interfacce di rete necessario. Per l'interfaccia di rete principale, specifica `NetworkCardIndex=0`, `DeviceIndex=0` e `InterfaceType=interface`. Se l'indice della scheda di rete 0 supporta EFA, specificare, `NetworkCardIndex=0DeviceIndex=1`, e. `InterfaceType=efa-only` Per eventuali interfacce di rete aggiuntive, `NetworkCardIndex` specificare il successivo indice inutilizzato, `DeviceIndex=0` for, for`InterfaceType=efa-only`. and/or `DeviceIndex=1` `InterfaceType=interface`

Il seguente frammento di comando di esempio mostra una richiesta con 32 dispositivi EFA e un dispositivo ENA.

```
$ aws ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami-0abcdef1234567890 \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 \
"NetworkCardIndex=0,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=1,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=2,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=3,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=4,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=5,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=6,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=7,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
```

```
"NetworkCardIndex=8,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=9,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
only" \
"NetworkCardIndex=10,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=11,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=12,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=13,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=14,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=15,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=16,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=17,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=18,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=19,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=20,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=21,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=22,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=23,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=24,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=25,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=26,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=27,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=28,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=29,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
```

```
"NetworkCardIndex=30,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only" \
"NetworkCardIndex=31,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
only"
...
```

Launch templates

Per aggiungere gli EFA a un modello di avvio utilizzando la console Amazon EC2

1. Nella sezione Impostazioni di rete, espandi Configurazione di rete avanzata.
2. Per l'interfaccia di rete principale (indice delle schede di rete`0`, indice dei dispositivi`0`), creare un'interfaccia ENA. Non è possibile utilizzare un'interfaccia EFA-only di rete come interfaccia di rete principale.
3. Se l'indice della scheda di rete 0 supporta EFA, crea un'interfaccia di EFA-only rete per l'indice della scheda di rete`0`, l'indice 1 del dispositivo.
4. Per ogni interfaccia di rete aggiuntiva, utilizzate il successivo indice delle schede di rete inutilizzate, l'indice dei dispositivi per l'interfaccia di EFA-only rete`0`, l'indice dei and/or dispositivi 1 per l'interfaccia di rete ENA a seconda del caso d'uso, ad esempio i requisiti di larghezza di banda ENA o lo spazio degli indirizzi IP. Per casi d'uso di esempio, consultare Configurazione EFA per le istanze P5 e P5e.

Per aggiungere EFA a un modello di avvio utilizzando create-launch-template command

Per `NetworkInterfaces`, specifica il numero di interfacce di rete necessario. Per l'interfaccia di rete principale, specifica `NetworkCardIndex=0`, `DeviceIndex=0` e `InterfaceType=interface`. Se l'indice della scheda di rete 0 supporta EFA, specificare,, e. `NetworkCardIndex=0` `DeviceIndex=1` `InterfaceType=efa-only` Per eventuali interfacce di rete aggiuntive, `NetworkCardIndex` specificare il successivo indice inutilizzato, `DeviceIndex=0` for, for`InterfaceType=efa-only`. and/or `DeviceIndex=1` `InterfaceType=interface`

Il seguente frammento mostra un esempio con 3 delle 32 possibili interfacce di rete.

```
"NetworkInterfaces":[
{
  "NetworkCardIndex":0,
  "DeviceIndex":0,
  "InterfaceType": "interface",
```

```
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 0,
  "DeviceIndex": 1,
  "InterfaceType": "efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 1,
  "DeviceIndex": 0,
  "InterfaceType": "efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 2,
  "DeviceIndex": 0,
  "InterfaceType": "efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 3,
  "DeviceIndex": 0,
  "InterfaceType": "efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
```

```
  "DeleteOnTermination":true
}
...
```

Configurazione EFA per le istanze P5 e P5e

`p5.48xlarge`e `p5e.48xlarge` le istanze supportano 32 schede di rete e hanno una capacità totale di larghezza di banda di rete di 3.200 Gbps, di cui fino a 800 Gbps possono essere utilizzati per il traffico di rete IP. Poiché il traffico EFA e il traffico di rete IP condividono le stesse risorse sottostanti, la larghezza di banda utilizzata da un tipo di traffico ridurrà quella disponibile per l'altro. Ciò significa che è possibile distribuire la larghezza di banda della rete tra il traffico EFA e il traffico IP con qualsiasi combinazione, purché la larghezza di banda totale non superi i 3.200 Gb/s e la larghezza di banda IP non superi gli 800 Gb/s. Ad esempio, se utilizzi una larghezza di banda IP di 400 Gbps, puoi ottenere contemporaneamente un massimo di 2.800 Gbps di larghezza di banda EFA.

Caso d'uso 1: salvare indirizzi IP ed evitare potenziali problemi di IP Linux

Questa configurazione fornisce fino a 3.200 Gb/s di larghezza di banda della rete EFA e un massimo di 100 Gb/s di larghezza di banda della rete IP con un indirizzo IP privato. Questa configurazione aiuta anche ad evitare potenziali problemi di IP Linux, come l'auto-assegnazione non consentita di indirizzi IP privati e sfide di routing IP (problemi di mappatura di nome host e indirizzo IP e mancate corrispondenze dell'indirizzo IP di origine), che si verificano se un'istanza ha più interfacce di rete.

- Per l'interfaccia di rete principale (indice della scheda di rete 0, indice del dispositivo 0), utilizzare un'interfaccia ENA.
- Per l'indice della scheda di rete 0, l'indice del dispositivo 1, creare un'interfaccia EFA-only di rete.
- Per le restanti interfacce di rete (indici delle schede di rete 1-31, indice del dispositivo 0), utilizzare le interfacce di rete. EFA-only

Caso d'uso 2: larghezza di banda della rete EFA e IP massima

Questa configurazione fornisce fino a 3.200 Gb/s di larghezza di banda della rete EFA e un massimo di 800 Gb/s di larghezza di banda della rete IP con 8 indirizzi IP privati. Non è possibile assegnare automaticamente indirizzi IP pubblici con questa configurazione. Tuttavia, è possibile collegare un indirizzo IP elastico all'interfaccia di rete principale (indice di scheda di rete 0, indice di dispositivo 0) dopo l'avvio per la connettività Internet.

- Per l'interfaccia di rete principale (indice della scheda di rete 0, indice del dispositivo 0), utilizzare un'interfaccia di rete ENA.
- Per le altre interfacce, eseguire le seguenti operazioni:
  - Specificare le EFA-only interfacce di rete sull'indice della scheda di rete 0, indice del dispositivo 1, e per gli indici delle schede di rete 1, 2 e 3, utilizzare l'indice del dispositivo 0.
  - Specificate un'interfaccia di rete ENA e quattro interfacce di EFA-only rete in ciascuno dei seguenti sottoinsiemi di indice delle schede di rete e utilizzate l'indice del dispositivo 1 per l'interfaccia di rete ENA e l'indice del dispositivo 0 per le interfacce di rete: EFA-only
    - [4,5,6,7]
    - [8,9,10,11]
    - [12,13,14,15]
    - [16,17,18,19]
    - [20,21,22,23]
    - [24,25,26,27]
    - [28,29,30,31]

Il seguente esempio illustra questa configurazione:

```
$ aws --region $REGION ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami_id \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=0,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=1,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=2,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=3,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=4,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
```

```
"NetworkCardIndex=5,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=6,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=7,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=8,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=9,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=10,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=11,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=12,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=13,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=14,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=15,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=16,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=17,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=18,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=19,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=20,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=20,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=21,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=22,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
```

```
"NetworkCardIndex=23,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=24,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=24,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=25,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=26,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=27,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=28,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=28,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=29,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=30,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=31,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only"
...
```

configurazione EFA per un'istanza P6-B200

P6-B200 le istanze hanno una capacità totale di larghezza di banda di rete di 3.200 Gbps, di cui fino a 1600 Gbps possono essere utilizzati per ENA. Sono dotati di 8 GPU e 8 schede di rete, in cui ciascuna scheda di rete supporta una larghezza di banda EFA fino a 400 Gbps e una larghezza di banda ENA di 200 Gbps. Dal momento che il traffico EFA e il traffico ENA condividono le stesse risorse sottostanti, la larghezza di banda utilizzata da un tipo di traffico ridurrà quella disponibile per l'altro.

Caso d'uso 1: salvare gli indirizzi IP

Questa configurazione utilizza almeno un indirizzo IP privato per istanza e supporta fino a 3200 Gbps di larghezza di banda EFA e 200 Gbps di larghezza di banda ENA.

- Per l'interfaccia di rete principale (indice della scheda di rete 0, indice del dispositivo 0), utilizzare un'interfaccia ENA.
- Per l'indice della scheda di rete 0, l'indice del dispositivo 1, creare un'interfaccia EFA-only di rete.

- Per le restanti 7 schede di rete (indici delle schede di rete 1-7, indice del dispositivo 0), utilizzare EFA-only le interfacce di rete.

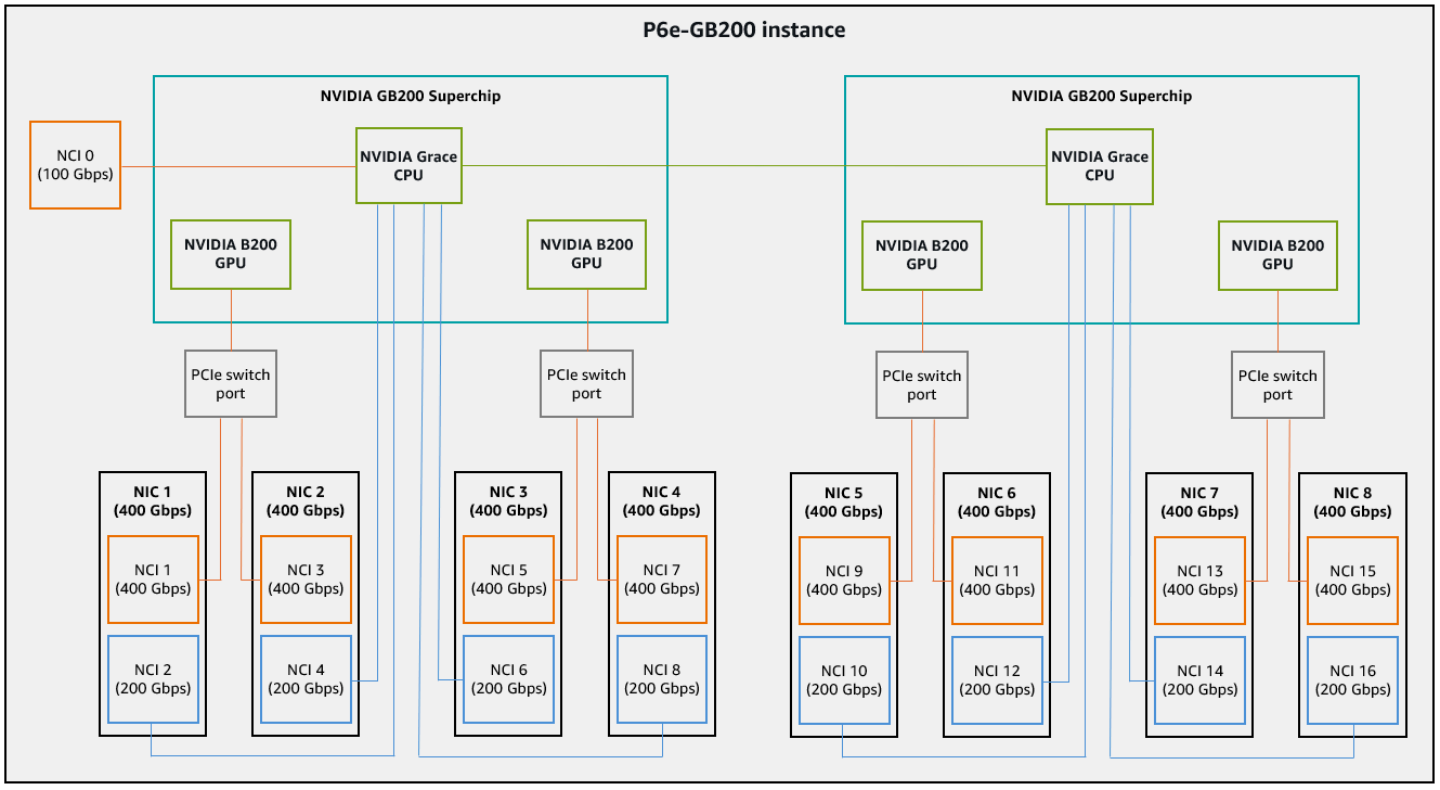
Caso d'uso 2: larghezza di banda di EFA e ENA massima

Questa configurazione utilizza almeno 8 indirizzi IP privati per istanza e supporta fino a 3200 Gbps di larghezza di banda EFA e 1600 Gbps di larghezza di banda ENA.

- Per l'interfaccia di rete principale (indice della scheda di rete 0, indice del dispositivo 0), utilizzare un'interfaccia ENA.
- Per l'indice della scheda di rete 0, l'indice del dispositivo 1, creare un'interfaccia EFA-only di rete.
- Per le restanti 7 schede di rete (indici delle schede di rete 1-7), creare un'interfaccia di EFA-only rete sull'indice del dispositivo 0 e un'interfaccia di rete ENA sull'indice del dispositivo 1.

Configurazione EFA per un'istanza P6e-GB200

P6e-GB200 le istanze possono essere configurate con un massimo di 17 schede di rete. L'immagine seguente mostra il layout fisico della scheda di interfaccia di rete (NIC) per P6e-GB200 le istanze, insieme alla mappatura degli indici delle schede di rete (NCI).



L'NCI primario (indice 0) supporta fino a 100 Gbps di larghezza di banda ENA. Gli NCI con i seguenti indici supportano le interfacce di EFA-only rete e la larghezza di banda EFA di 400 Gbps: [1, 3, 5, 7, 9, 11, 13, 15]. NCI con i seguenti indici supportano fino a 200 Gbps di larghezza di banda ENA o EFA: [2, 4, 6, 8, 10, 12, 14, 16].

NCI nei seguenti gruppi condividono una scheda NIC fisica sottostante sull'host:

- [1 e 2]
- [3 e 4]
- [5 e 6]
- [7 e 8]
- [9 e 10]
- [11 e 12]
- [13 e 14]
- [15 e 16]

Ciascun NIC fisico supporta fino a 400 Gbps di larghezza di banda. Poiché gli NCI di questi gruppi condividono la stessa scheda NIC fisica sottostante, la larghezza di banda utilizzata da uno ridurrà quella disponibile per l'altro. Ad esempio, se NCI 2 utilizza 200 Gbps di una larghezza di banda ENA, NCI 1 può utilizzare contemporaneamente un massimo di 200 Gbps di larghezza di banda EFA.

Ciascuna GPU sottostante sull'host può inviare traffico direttamente tramite le seguenti coppie di NCI:

- [1 e 3]
- [5 e 7]
- [9 e 11]
- [13 e 15]

Ciascuna GPU supporta fino a 400 Gbps di larghezza di banda EFA. Poiché le schede di rete di questi gruppi condividono la stessa GPU, la larghezza di banda utilizzata da uno ridurrà quella disponibile per l'altro. Ad esempio, se NCI 1 utilizza 200 Gbps di larghezza di banda EFA, NCI 3 può utilizzare contemporaneamente un massimo di 200 Gbps di larghezza di banda EFA. Pertanto, per ottenere le massime prestazioni EFA, consigliamo di eseguire una delle seguenti operazioni per ottenere una larghezza di banda EFA totale di 1.600 Gbps:

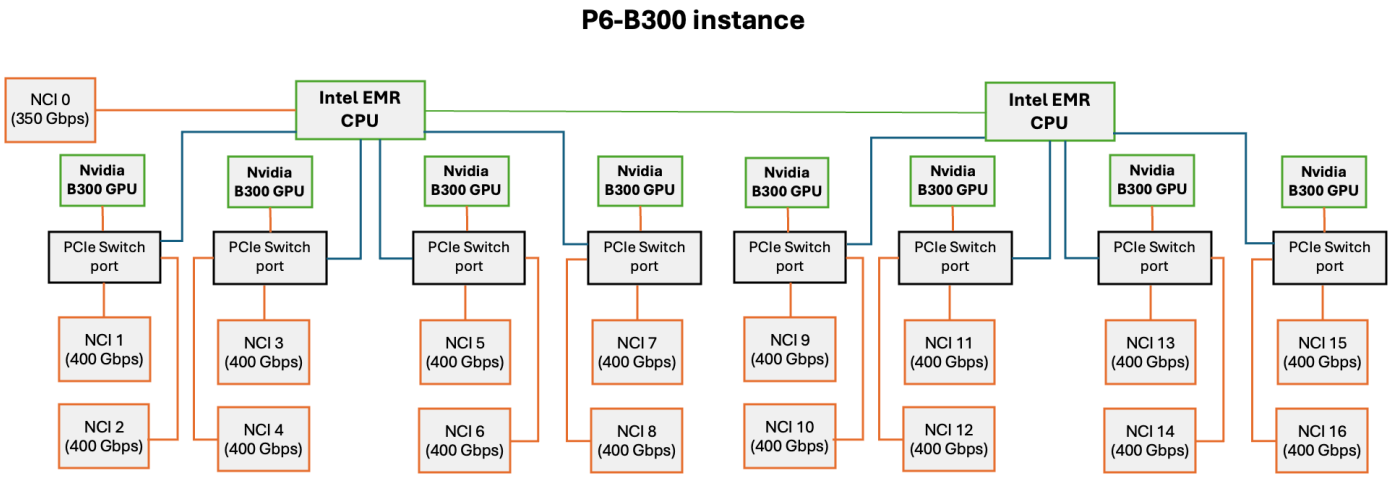
- Aggiungete un'interfaccia EFA-only di rete a un solo NCI in ogni gruppo per ottenere 400 Gbps per interfaccia di rete (4 interfacce di rete EFA x 400 Gbps).
- EFA-only Aggiungete un'interfaccia di rete a ciascun NCI di ciascun gruppo per ottenere 200 Gbps per interfaccia di rete (8 interfacce di rete EFA x 200 Gbps).

Ad esempio, la configurazione seguente fornisce fino a 1.600 Gbps di larghezza di banda EFA utilizzando una singola interfaccia di EFA-only rete in ciascun gruppo NCI e fino a 100 Gbps di larghezza di banda di rete ENA utilizzando solo l'NCI primario (indice 0).

- Per l’NCI primario (indice di scheda di rete 0, indice di dispositivo 0), utilizza un’interfaccia di rete ENA.
- Aggiungi interfacce di rete a quanto segue: EFA-only
  - NCI 1, indice del dispositivo 0
  - NCI 5, indice del dispositivo 0
  - NCI 9, indice del dispositivo 0
  - NCI 13, indice del dispositivo 0

Configurazione EFA per un'istanza P6-B300

P6-B300 le istanze hanno una capacità totale di larghezza di banda di rete fino a 6400 Gbps per il traffico EFA e fino a 3870 Gbps per il traffico ENA. Sono dotate di 8 GPU e 17 schede di rete, in cui la scheda di rete principale supporta solo un'interfaccia di rete ENA con una larghezza di banda fino a 350 Gbps. Le schede di rete secondarie supportano fino a 400 Gbps EFA e fino a 220 Gbps di larghezza di banda ENA. Dal momento che il traffico EFA e il traffico ENA condividono le stesse risorse sottostanti, la larghezza di banda utilizzata da un tipo di traffico ridurrà quella disponibile per l’altro.



Caso d'uso 1: salvare gli indirizzi IP

Questa configurazione utilizza almeno un indirizzo IP privato per istanza e supporta fino a 6400 Gbps di larghezza di banda EFA e fino a 350 Gbps di larghezza di banda ENA.

- Per l'interfaccia di rete principale (indice della scheda di rete 0, indice del dispositivo 0), utilizzare un'interfaccia di rete ENA.
- Per le restanti schede di rete (indici delle schede di rete 1-16, indice del dispositivo 0), utilizzare EFA-only le interfacce di rete.

```
--network-interfaces \
"NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=1,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=2,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=3,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=4,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=5,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=6,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=7,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
```

```
"NetworkCardIndex=8,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=9,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=10,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=11,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=12,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=13,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=14,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=15,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=16,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only"
```

Caso d'uso 2: larghezza di banda di EFA e ENA massima

Questa configurazione utilizza almeno 17 indirizzi IP privati per istanza e supporta fino a 6400 Gbps di larghezza di banda EFA e fino a 3870 Gbps di larghezza di banda ENA.

- Per l'interfaccia di rete principale (indice della scheda di rete 0, indice del dispositivo 0), utilizzare un'interfaccia di rete ENA.
- Per le restanti schede di rete, creare un' EFA-only interfaccia (indici delle schede di rete 1-16, indice del dispositivo 0) e un'interfaccia ENA (indici delle schede di rete 1-16, indice dei dispositivi 1).

```
--network-interfaces \
"NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=1,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=2,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=3,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=4,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
```

```
"NetworkCardIndex=5,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=6,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=7,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=8,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=9,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=10,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=11,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=12,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=13,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=14,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=15,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=16,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
```

```
"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
 \
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=in
```

Installare il software EFA in un contenitore

Questa sezione spiega come utilizzare il programma di installazione EFA in un ambiente containerizzato. Puoi installare il software EFA aggiungendo comandi a un Dockerfile o eseguendoli direttamente nella shell di un contenitore in esecuzione.

Per installare il software EFA in un contenitore usando i comandi della shell

1. Aggiornare i pacchetti del sistema operativo. Questo passaggio garantisce la disponibilità dei pacchetti più recenti.

   - Per i sistemi Debian-based operativi:

     ```
     apt-get update && apt-get upgrade -y
     ```

   - Per i sistemi RHEL-based operativi:

     ```
     yum update -y
     ```

2. Scarica il programma di installazione EFA. Ti consigliamo di utilizzare il programma di installazione EFA più recente. Per informazioni sulla versione più recente, vedere. Note sulla versione di Elastic Fabric Adapter

   ```
   mkdir /tmp/efa \
   && cd /tmp/efa \
   && curl -O https://efa-installer.amazonaws.com/aws-efa-installer-version.tar.gz
   ```

   (Facoltativo) Verifica la firma del pacchetto di installazione EFA.

```
wget https://efa-installer.amazonaws.com/aws-efa-installer.key \
&& gpg --import aws-efa-installer.key \
&& cat aws-efa-installer.key | gpg --fingerprint \
&& wget https://efa-installer.amazonaws.com/aws-efa-installer-version.tar.gz.sig \
&& gpg --verify ./aws-efa-installer-version.tar.gz.sig
```

3. Installare il software EFA. Il comando seguente utilizza questi argomenti:

   - `--skip-kmod`— Salta l'installazione del modulo del kernel. L'ambiente contenitore non può modificare i moduli del kernel.
   - `--skip-limit-conf`— Ignora la configurazione dei limiti. Non puoi ambientarlo `ulimit` all'interno di un contenitore. Configuralo invece come parte della creazione del contenitore.
   - `--no-verify`— Ignora il rilevamento dei dispositivi EFA. Utilizza il rilevamento del dispositivo`lspci`, che non funziona in un ambiente containerizzato.

```
tar -xf aws-efa-installer-version.tar.gz \
&& cd aws-efa-installer \
&& ./efa_installer.sh -y --skip-kmod --skip-limit-conf --no-verify
```

> **Note**
>
> Per i contenitori NGC, con la versione 1.49.0 o successiva del programma di installazione EFA è possibile utilizzare il `--enable-ngc` flag al posto dei tre flag precedenti. Questo flag gestisce automaticamente tutte le configurazioni specifiche del contenitore:
>
> ```
> ./efa_installer.sh -y --enable-ngc
> ```

4. Pulisci i file di installazione temporanei.

```
rm -rf /tmp/efa
```

Creare e collegare un Elastic Fabric Adapter a un'istanza Amazon EC2

È possibile creare un EFA e collegarlo a un'istanza Amazon EC2 proprio come qualsiasi altra interfaccia di rete elastica in Amazon EC2. Tuttavia, a differenza delle interfacce di rete elastica, gli EFA non possono essere collegati o scollegati da un'istanza nello stato `running`.

Considerazioni

- Puoi modificare un gruppo di sicurezza collegato a un EFA. Per abilitare la OS-bypass funzionalità, l'EFA deve essere membro di un gruppo di sicurezza che consenta tutto il traffico in entrata e in uscita da e verso il gruppo di sicurezza stesso. Per ulteriori informazioni, consulta Fase 1: Preparare un gruppo di sicurezza EFA-enabled.

  La procedura per modificare il gruppo di sicurezza associato a un EFA è uguale a quella usata per modificare il gruppo di sicurezza associato a un'ENI. Per ulteriori informazioni, consulta the section called “Modifica degli attributi dell'interfaccia di rete”.
- La procedura per assegnare un indirizzo IP elastico (IPv4) e IPv6 a un'interfaccia di rete EFA (EFA con ENA) è uguale a quella usata per assegnare un indirizzo IP a un'interfaccia di rete elastica. Per ulteriori informazioni, consulta Gestione degli indirizzi IP.

  Non è possibile assegnare un indirizzo IP a un'interfaccia di rete. EFA-only

Processi

- Creazione di un EFA
- Collegare un EFA a un'istanza arrestata
- Collegare un EFA all'avvio di un'istanza
- Aggiunta di un EFA a un modello di avvio

Creazione di un EFA

Puoi creare un EFA in una sottorete di un VPC. Non puoi spostare l'EFA in un'altra sottorete dopo averlo creato. Puoi solo collegarlo alle istanze terminate nella stessa zona di disponibilità.

Console

Per creare un'interfaccia di rete EFA (EFA con ENA o ENA-only)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel riquadro di navigazione, scegliere Network Interfaces (Interfacce di rete) e selezionare Create network interface (Crea interfaccia di rete).
3. In Description (Descrizione), immettere un nome descrittivo per l'EFA.
4. In Subnet (Sottorete), selezionare la sottorete in cui creare l'EFA.
5. Tipo di interfaccia, scegli una delle seguenti opzioni:

   - EFA con ENA: per creare un'interfaccia di rete che supporti sia i dispositivi ENA che EFA.
   - EFA-only— Per creare un'interfaccia di rete solo con un dispositivo EFA.
6. (Per EFA con solo ENA) Configura l'assegnazione dell'indirizzo IP e del prefisso per l'interfaccia di rete. Il tipo di indirizzi IP e prefissi che puoi assegnare "dipende" dalla sottorete selezionata. Per le IPv4-only sottoreti, è possibile assegnare solo indirizzi IP e prefissi IPv4. Per le IPv6-only sottoreti, è possibile assegnare solo indirizzi IP e prefissi IPv6. Per le sottoreti dual-stack, puoi assegnare indirizzi e prefissi IP IPv4 e IPv6.

   > **Note**
   >
   > Non è possibile assegnare indirizzi IP a un'interfaccia di rete. EFA-only

   a. Per l'indirizzo and/or IPv6 con indirizzo IPv4 privato, scegli di Auto-assign fare in modo che Amazon EC2 assegni automaticamente un indirizzo IP dalla sottorete selezionata oppure scegli Personalizzato per specificare manualmente l'indirizzo IP da assegnare.

   b. Se assegni un indirizzo IPv6, facoltativamente puoi abilitare Assegna IP IPv6 primario. Ciò assegna un indirizzo unicast globale IPv6 (GUA) primario all'interfaccia di rete. L'assegnazione di un indirizzo IPv6 primario consente di evitare l'interruzione del traffico verso istanze o ENI. Per ulteriori informazioni, consulta IPv6 addresses.

   c. Per la and/or delega del prefisso IPv4, scegli di Auto-assign fare in modo che Amazon EC2 assegni automaticamente un prefisso dal blocco CIDR della sottorete oppure scegli Personalizzato per specificare manualmente un prefisso dal blocco CIDR della sottorete. Se specifichi un prefisso, verifica che non sia già assegnato a un'altra risorsa. AWS Per ulteriori informazioni, consulta Delega del prefisso per Interfacce di rete Amazon EC2

   d. (Facoltativo) Configura le impostazioni del timeout di tracciamento della connessione inattiva. Per ulteriori informazioni, consulta Timeout di tracciamento delle connessioni inattive

- Timeout TCP stabilito: il periodo di timeout, in secondi, per le connessioni TCP inattive in uno stato stabilito. Minimo: 60 secondi. Massimo: 432.000 secondi (5 giorni). Valore predefinito: 432.000 secondi. Consigliato: meno di 432.000 secondi.
- Timeout UDP: il timeout, in secondi, per i flussi UDP inattivi che hanno registrato traffico solo in un'unica direzione o una singola transazione richiesta-risposta. Minimo: 30 secondi. Massimo 60 secondi. Valore predefinito: 30 secondi.
- Timeout del flusso UDP: il periodo di timeout, in secondi, per i flussi UDP inattivi classificati come flussi che hanno registrato più di una transazione richiesta-risposta. Minimo: 60 secondi. Massimo: 180 secondi (3 minuti). Valore predefinito: 180 secondi.

7. In Security groups (Gruppi di sicurezza), selezionare uno o più gruppi di sicurezza.
8. Seleziona Crea un'interfaccia di rete.

AWS CLI

Per creare un EFA

Utilizzare il comando create-network-interface. Per`--interface-type`, specificare `efa` un'interfaccia di rete EFA o un'interfaccia `efa-only` di rete. EFA-only

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --interface-type efa \
    --description "my efa"
```

PowerShell

Per creare un EFA

Utilizza il cmdlet New-EC2NetworkInterface. Per`-InterfaceType`, specificare `efa` per un'interfaccia di rete EFA o `efa-only` per un' EFA-only interfaccia di rete

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -InterfaceType efa `
    -Description "my efa"
```

Collegare un EFA a un'istanza arrestata

È possibile collegare un EFA a qualsiasi tipo di istanza supportato che sia in stato `stopped`. Non è possibile collegare un EFA a un'istanza in stato `running`. Per ulteriori informazioni sui tipi di istanza supportati, vedi Tipi di istanze supportati.

Collegare EFA a un'istanza nello stesso modo in cui si collega un'interfaccia di rete elastica a un'istanza. Per ulteriori informazioni, consulta Collega un'interfaccia di rete.

Collegare un EFA all'avvio di un'istanza

AWS CLI

Per collegare un EFA esistente all'avvio di un'istanza

Utilizza il comando run-instances con l'opzione `--network-interfaces`. Per l'interfaccia di rete principale, specificare un'interfaccia di rete EFA e `NetworkCardIndex=0`, `DeviceIndex=0`. Per collegare più interfacce di rete EFA, consulta Ottimizzare la larghezza di banda della rete.

```
--network-interfaces "NetworkCardIndex=0, \
    DeviceIndex=0, \
    NetworkInterfaceId=eni-1234567890abcdef0, \
    Groups=sg-1234567890abcdef0, \
    SubnetId=subnet-0abcdef1234567890"
```

Per collegare un nuovo EFA all'avvio di un'istanza

Utilizza il comando run-instances con l'opzione `--network-interfaces`. Per l'interfaccia di rete principale, utilizzare `NetworkCardIndex=0`, `DeviceIndex=0` e `InterfaceType=efa`. Se vengono collegate più interfacce di rete EFA, consultare Ottimizzare la larghezza di banda della rete.

```
--network-interfaces "NetworkCardIndex=0, \
    DeviceIndex=0, \
    InterfaceType=efa, \
    Groups=sg-1234567890abcdef0, \
    SubnetId=subnet-0abcdef1234567890"
```

PowerShell

Per collegare un EFA esistente all'avvio di un'istanza

Utilizzare il New-EC2Instance cmdlet con il `-NetworkInterfaces` parametro.

```
-NetworkInterface $networkInterface
```

Definisci l'interfaccia di rete come segue.

```
$networkInterface = New-Object
 Amazon.EC2.Model.InstanceNetworkInterfaceSpecification
$networkInterface.DeviceIndex = 0
$networkInterface.NetworkInterfaceId = "eni-1234567890abcdef0"
$networkInterface.Groups = @("sg-1234567890abcdef0")
$networkInterface.SubnetId = "subnet-0abcdef1234567890"
```

Per collegare un nuovo EFA all'avvio di un'istanza

Utilizzare il New-EC2Instance cmdlet con il parametro. `-NetworkInterfaces`

```
-NetworkInterface $networkInterface
```

Definisci l'interfaccia di rete come segue.

```
$networkInterface = New-Object
 Amazon.EC2.Model.InstanceNetworkInterfaceSpecification
$networkInterface.DeviceIndex = 0
$networkInterface.InterfaceType = "efa"
$networkInterface.Groups = @("sg-1234567890abcdef0")
$networkInterface.SubnetId = "subnet-0abcdef1234567890"
```

Aggiunta di un EFA a un modello di avvio

È possibile creare un modello di avvio che contenga le informazioni di configurazione necessarie per avviare EFA-enabled le istanze. È possibile specificare sia l'interfaccia EFA che quella EFA-only di rete nel modello di avvio. Per creare un modello di EFA-enabled lancio, create un nuovo modello di avvio e specificate un tipo di istanza supportato, la vostra EFA-enabled AMI e un gruppo EFA-enabled di sicurezza. Per `NetworkInterfaces`, specificare le interfacce di rete EFA da collegare. Per l'interfaccia di rete principale, utilizzare `NetworkCardIndex=0`, `DeviceIndex=0` e `InterfaceType=efa`. Se vengono collegate più interfacce di rete EFA, consultare Ottimizzare la larghezza di banda della rete sulle istanze Amazon EC2 con più schede di rete.

Puoi sfruttare i modelli di avvio per avviare EFA-enabled istanze con altri AWS servizi, come AWS Batch o. AWS ParallelCluster

Per ulteriori informazioni sulla creazione dei modelli di lancio, consulta Creare un modello di avvio Amazon EC2.

Scollegare ed eliminare un EFA da un'istanza Amazon EC2

È possibile scollegare un EFA da un'istanza Amazon EC2 ed eliminarlo proprio come si scollega ed elimina qualsiasi altra interfaccia di rete elastica in Amazon EC2.

Scollegare un EFA

Per scollegare un EFA da un'istanza, devi prima arrestare tale istanza. Non è possibile scollegare un EFA da un'istanza in esecuzione.

Scollegare EFA da un'istanza nello stesso modo in cui si scollega un'interfaccia di rete elastica dall'istanza. Per ulteriori informazioni, consulta Scollega un'interfaccia di rete.

Eliminazione di un EFA

Per eliminare un EFA devi prima scollegarlo dall'istanza. Non è possibile eliminare un EFA mentre è ancora collegato a un'istanza.

Eliminare EFAs nello stesso modo in cui si eliminano le interfacce di rete elastica. Per ulteriori informazioni, consulta Eliminazione di un'interfaccia di rete.

Monitorare un Elastic Fabric Adapter in Amazon EC2

Puoi utilizzare le seguenti funzionalità per monitorare le prestazioni dei tuoi Elastic Fabric Adapter.

Argomenti

- Parametri di driver EFA per un'istanza Amazon EC2
- Log di flusso Amazon VPC
- Amazon CloudWatch

Parametri di driver EFA per un'istanza Amazon EC2

Il driver Elastic Fabric Adapter (EFA) pubblica più metriche delle istanze a cui sono collegate interfacce EFA, in tempo reale. Puoi utilizzare queste metriche per risolvere i problemi relativi alle

prestazioni e alla rete delle applicazioni, scegliere la dimensione del cluster appropriata per un carico di lavoro, pianificare le attività di scalabilità in modo proattivo e confrontare le applicazioni per determinare se massimizzano le prestazioni EFA disponibili su un'istanza.

Argomenti

- Parametri di driver EFA disponibili
- Recuperare i parametri di driver EFA per l'istanza

Parametri di driver EFA disponibili

Il driver EFA pubblica i seguenti parametri all'istanza in tempo reale. Forniscono il numero complessivo di errori, eventi di connesione e pacchetti o byte inviati, ricevuti, ritrasmessi o abbandonati dai dispositivi EFA collegati dall'avvio dell'istanza o dall'ultimo ripristino del driver.

Metrica	Description	Tipi di istanze supportati
`tx_bytes`	Il numero di byte trasmessi. Unità: byte	Tutti i tipi di istanze che supportano EFA
`rx_bytes`	Il numero di byte ricevuti. Unità: byte	Tutti i tipi di istanze che supportano EFA
`tx_pkts`	Il numero di pacchetti trasmessi. Unità: numero	Tutti i tipi di istanze che supportano EFA
`rx_pkts`	Il numero di pacchetti ricevuti. Unità: numero	Tutti i tipi di istanze che supportano EFA
`rx_drops`	Il numero di pacchetti ricevuti e poi persi. Unità: numero	Tutti i tipi di istanze che supportano EFA

Metrica	Description	Tipi di istanze supportati
`send_bytes`	Il numero di byte inviati tramite operazioni di invio. Unità: byte	Tutti i tipi di istanze che supportano EFA
`recv_bytes`	Il numero di byte ricevuti da operazioni di invio. Unità: byte	Tutti i tipi di istanze che supportano EFA
`send_wrs`	Il numero di pacchetti inviati tramite operazioni di invio. Unità: numero	Tutti i tipi di istanze che supportano EFA
`recv_wrs`	Il numero di pacchetti ricevuti da operazioni di invio. Unità: numero	Tutti i tipi di istanze che supportano EFA
`rdma_write_wrs`	Il numero di operazioni di scrittura rdma completate. Unità: numero	Tutti i tipi di istanze che supportano EFA
`rdma_read_wrs`	Il numero di operazioni di lettura rdma completate. Unità: numero	Tutti i tipi di istanze che supportano EFA
`rdma_write_bytes`	Il numero di byte scritti da altre istanze tramite operazioni di scrittura rdma. Unità: byte	Tutti i tipi di istanze che supportano EFA

Metrica	Description	Tipi di istanze supportati
`rdma_read_bytes`	Il numero di byte ricevuti tramite operazioni di lettura rdma. Unità: byte	Tutti i tipi di istanze che supportano EFA
`rdma_write_wr_err`	Il numero di operazioni di scrittura rdma con errori locali o remoti. Unità: numero	Tutti i tipi di istanze che supportano EFA
`rdma_read_wr_err`	Il numero di operazioni di lettura rdma con errori locali o remoti. Unità: numero	Tutti i tipi di istanze che supportano EFA
`rdma_read_resp_bytes`	Il numero di byte inviati in risposta a operazioni di lettura rdma. Unità: byte	Tutti i tipi di istanze che supportano EFA
`rdma_write_recv_bytes`	Il numero di byte ricevuti da operazioni di scrittura rdma. Unità: byte	Tutti i tipi di istanze che supportano EFA
`retrans_bytes`	Il numero di byte EFA SRD ritrasmessi. Unità: numero	Tipi di istanza Nitro v4 e successive che supportano EFA
`retrans_pkts`	Il numero di pacchetti EFA SRD ritrasmessi. Unità: byte	Tipi di istanza Nitro v4 e successive che supportano EFA

Metrica	Description	Tipi di istanze supportati
`retrans_timeout_events`	Il numero di volte in cui il traffico EFA SRD è scaduto e ha determinato una modifica del percorso di rete. Unità: numero	Tipi di istanza Nitro v4 e successive che supportano EFA
`impaired_remote_conn_events`	Il numero di volte in cui le connessioni EFA SRD sono entrate in uno stato compromesso, con conseguente riduzione del limite di velocità di throughput. Unità: numero	Tipi di istanza Nitro v4 e successive che supportano EFA
`unresponsive_remote_events`	Il numero di volte in cui una connessione remota EFA SRD non ha risposto. Unità: numero	Tipi di istanza Nitro v4 e successive che supportano EFA

Per ulteriori informazioni sui tipi di istanza che supportano EFA, consulta Tipi di istanze supportati.

Recuperare i parametri di driver EFA per l'istanza

È possibile utilizzare lo strumento a riga di comando rdma-tool per recuperare i parametri di tutte le interfacce EFA collegate a un'istanza seguendo questa procedura:

```
$ rdma -p statistic show
link rdmap0s31/1
    tx_bytes 0
    tx_pkts 0
    rx_bytes 0
    rx_pkts 0
    rx_drops 0
    send_bytes 0
    send_wrs 0
    recv_bytes 0
```

```
    recv_wrs 0
    rdma_read_wrs 0
    rdma_read_bytes 0
    rdma_read_wr_err 0
    rdma_read_resp_bytes 0
    rdma_write_wrs 0
    rdma_write_bytes 0
    rdma_write_wr_err 0
    retrans_bytes 0
    retrans_pkts 0
    retrans_timeout_events 0
    unresponsive_remote_events 0
    impaired_remote_conn_events 0
```

In alternativa, è possibile recuperare i parametri per ogni interfaccia EFA collegata a un'istanza dai file sys utilizzando il comando riportato di seguito.

```
$ more /sys/class/infiniband/device_number/ports/port_number/hw_counters/* | cat
```

Ad esempio

```
$ more /sys/class/infiniband/rdmap0s31/ports/1/hw_counters/* | cat
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/lifespan
::::::::::::::
12
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_resp_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_wr_err
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_wrs
::::::::::::::
0
::::::::::::::
```

```
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_recv_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_wr_err
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_wrs
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/recv_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/recv_wrs
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rx_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rx_drops
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rx_pkts
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/send_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/send_wrs
::::::::::::::
0
::::::::::::::
```

```
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/tx_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/tx_pkts
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/retrans_bytes
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/retrans_pkts
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/retrans_timeout_events
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/unresponsive_remote_events
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/impaired_remote_conn_events
::::::::::::::
0
```

Log di flusso Amazon VPC

Puoi creare un log di flusso Amazon VPC per acquisire informazioni sul traffico da e per un EFA. I dati dei log di flusso possono essere pubblicati su Amazon CloudWatch Logs e Amazon S3. Dopo aver creato un log di flusso, puoi recuperare e visualizzarne i dati nella destinazione scelta. Per ulteriori informazioni, consulta l'argomento relativo ai Log di flusso VPC nella Guida per l'utente di Amazon VPC.

La procedura per creare un log di flusso per EFA è uguale a quella per crearlo per un'ENI. Per ulteriori informazioni, consulta Creazione di un log di flusso nella Guida per l'utente di Amazon VPC.

Nelle voci dei log di flusso, il traffico EFA è identificato da `srcAddress` e `destAddress`, entrambi formattati come indirizzi MAC, come mostrato nel seguente esempio.

```
version accountId  eniId        srcAddress        destAddress       sourcePort destPort
 protocol packets bytes start      end        action log-status
2       3794735123 eni-10000001 01:23:45:67:89:ab 05:23:45:67:89:ab -          -
 -        9       5689  1521232534 1524512343 ACCEPT OK
```

Amazon CloudWatch

Se utilizzi EFA in un cluster Amazon EKS, puoi monitorare i tuoi EFA utilizzando CloudWatch Container Insights. Amazon CloudWatch Container Insights supporta tutte le metriche dei driver EFA, ad eccezione di:,`retrans_bytes`,`retrans_pkts`, `retrans_timeout_events` e. `unresponsive_remote_events` `impaired_remote_conn_events`

Per ulteriori informazioni, consulta le metriche di Amazon EKS e Kubernetes Container Insights nella Amazon User Guide. CloudWatch

Verifica del programma di installazione EFA utilizzando un checksum

Facoltativamente, puoi verificare il tarball EFA (file `.tar.gz`) utilizzando un checksum MD5 o SHA256. È consigliabile eseguire questa operazione per verificare l'identità dell'autore del software e che l'applicazione non sia stata alterata o danneggiata dopo la pubblicazione.

Per verificare il tarball

Utilizzare l'utilità md5sum per il checksum MD5 o l'utilità sha256sum per il checksum SHA256 e specificare il nome del file tarball. È necessario eseguire il comando dalla directory in cui è stato salvato il file tarball.

- MD5

```
$ md5sum tarball_filename.tar.gz
```

- SHA256

```
$ sha256sum tarball_filename.tar.gz
```

I comandi devono restituire un valore di checksum nel formato seguente.

```
checksum_value tarball_filename.tar.gz
```

Confrontare il valore di checksum restituito dal comando con il valore di checksum fornito nella tabella seguente. Se i checksum corrispondono, allora è sicuro eseguire lo script di installazione. Se i checksum non corrispondono, non eseguire lo script di installazione e contattare Supporto.

Ad esempio, il comando seguente verifica il tarball EFA 1.9.4 utilizzando il checksum SHA256.

```
$  sha256sum aws-efa-installer-1.9.4.tar.gz
```

Output di esempio:

```
1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14 aws-efa-
installer-1.9.4.tar.gz
```

Nella tabella seguente sono elencati i checksum per le versioni recenti di EFA.

Versione	Checksum
EFA 1.50.0	MD5: e5a5178944b1f1112f3b2eb3b15ca5a7 SHA256: fa6dff8593d866866c13cb4640d9059835cd4efa427971f100ab40c97bef2841
EFA 1.49.0	MD5: bb10de6856e08a7e7e8a6b52bea6f681 SHA256: cf2e9281a2328a243c76f911a490faed43ca0fecfe4733c25e34b2e92a32c309
EFA 1.48.0	MD5: d30960f1876fb16ac8238193a26c6b29 SHA256: f3a8aadc2b94288694a9b9375bcad84a82f0f843e0eefafda7b158b2200549cc
EFA 1.4.70	MD5: c81d4caf24dabc04a6e4818590620f5f SHA256: 2df4201e046833c7dc8160907bee7f52b76ff80ed147376a2d0ed8a0dd66b2db

Versione	Checksum
EFA 1.46.0	MD5: a88bbd9b71624d7ca401b54bc2fc0c19 SHA256: 8302bd7849afb95c90 3a875d7dcb6f85b3d7629e9a8b6 7d020031cfc6f4d0ee1
EFA 1.45.1	MD5:91c3c87e16bbcaca1513252c38b771bb SHA256: 9aeb20c645135b6039 cc08986d8f14e63280f7839e882 a74df5e83627ffeaa17
EFA 1.45.0	MD5:800aeddfa9d9c5f139a7b8f7c4fec627 SHA256: 25ba26a0877fe33173 90dc126aad2f23e27fc461cf0b9 40004f032cb342fa539
EFA 1.44.0	MD5:d024f6bebe080db42745103b84ca7c43 SHA256: f129a5b44a49d593d2 47e55a59eb9bcb57121566e1c2e 42b832a4e794fa83d8a
EFA 1.43.3	MD5: 4dbc6eeecc516760253c10cbedb 6319d SHA256: 6c470ebce254c71653 47b5048895ac2996c8856727164 2297f4c597738300652
EFA 1.43.2	MD5: 7287b25a07c9747c0d4001e8fc5 f59b2 SHA256: de15c5bdbc83b952af bde876110830c604ad0796680e5 157c05f7c1979a41069

Versione	Checksum
EFA 1.43.1	MD5: `7cfafc8debaea51dd4966fa0b2bba673` SHA256:`54211eda0c193138ee8ed09b5fb41c41fc76fe0a77935fa4ec8d989466342740`
EFA 1.43.0	MD5: `f2b3dd7dc8670b541f7c23fd58e5e503` SHA256: `786df3458c499237be33bb8e50ffd4da7c18c20e254380ffc80fb90833d8cc73`
EFA 1.4.20	MD5: `94b2b1db09da1dde08ec049db1f24370` SHA256: `4114fe612905ee05083ae5cb391a00a012510f3abfecc642d86c9a5ae4be9008`
EFA 1.41.0	MD5: `086181c3ee3f8da512fc6e1c795e8936` SHA256: `3506354cdfbe31ff552fe75f5d0d9bb7efd29cf79bd99457347d29c751c38f9f`
EFA 1.40.0	MD5: `f3ec6f73fbeaccba082327507581157c` SHA256: `30491b0fe7c3470d4439594538855c981b05fa69862d74f8c05eb9b97912368a`

Versione	Checksum
EFA 1.39.0	MD5: c223d5954a85a7fbcd248c942b866e43 SHA256: 2cbc028c03064633bb990782b47c36156637769e2f48704417a9c700a7a32101
EFA 1.38.1	MD5: f112569e828ab65187777f794bab542c SHA256: 83923374afd388b1cfcf4b3a21a2b1ba7cf46a01a587f7b519b8386cb95e4f81
EFA 1.38.0	MD5: 43a2a446b33a2506f40853d55059f1ea SHA256: 4f436954f35ad53754b4d005fd8d0be63de3b4184de41a695b504bdce0fecb22
EFA 1.37.0	MD5: 6328070192bae920eca45797ad4c1db1 SHA256: 2584fc3c8bb99f29b3285e275747ff09d67c18e162c2a652e36c976b72154bfb
EFA 1.36.0	MD5: 1bec83180fbffb23452ab6469ca21dfa SHA256: de183f333cfb58aeb7908a67bf9106985ba3ccb7f8638b851d2a0d8dbfacaec4

Versione	Checksum
EFA 1.35.0	MD5: 252f03c978dca5f8e8d9f34e488b256e SHA256: 432b6ad4368ba0cd8b902729d14a908a97be7a3dcc5239422ea994a47f35a5e1
EFA 1.34.0	MD5: 5cd4b28d27a31677c16139b54c9acb45 SHA256: bd68839e741b0afd3ec2e37d50603803cfa7a279c120f0a736cc57c2ff2d7fdc
EFA 1.33.0	MD5: e2f61fccbcaa11e2ccfddd3660522276 SHA256: 0372877b87c6a7337bb7791d255e1053b907d030489fb2c3732ba70069185fce
EFA 1.32.0	MD5: db8d65cc028d8d08b5a9f2d88881c1b1 SHA256: 5f7233760be57f6fee6de8c09acbfbf59238de848e06048dc54d156ef578fc66
EFA 1.31.0	MD5: 856352f12bef2ccbadcd75e35aa52aaf SHA256: 943325bd37902a4300ac9e5715163537d56ecb4e7b87b37827c3e547aa1897bf

Versione	Checksum
EFA 1.30.0	MD5: 31f48e1a47fe93ede8ebd273fb747358 SHA256: 876ab9403e07a0c3c91a1a34685a52eced890ae052df94857f6081c5f6c78a0a
EFA 1.29.1	MD5: e1872ca815d752c1d7c2b5c175e52a16 SHA256: 178b263b8c25845b63dc93b25bcdff5870df5204ec509af26f43e8d283488744
EFA 1.29.0	MD5: 39d06a002154d94cd982ed348133f385 SHA256: 836655f87015547e733e7d9f7c760e4e24697f8bbc261bb5f3560abd4206bc36
EFA 1.28.0	MD5: 9dc13b7446665822605e66febe074035 SHA256: 2e625d2d6d3e073b5178e8e861891273d896b66d03cb1a32244fd56789f1c435
EFA 1.27.0	MD5: 98bfb515ea3e8d93f554020f3837fa15 SHA256: 1d49a97b0bf8d964d91652a79ac851f2550e33a5bf9d0cf86ec9357ff6579aa3

Versione	Checksum
EFA 1.26.1	MD5: 884e74671fdef4725501f7cd2d451d0c SHA256: c616994c924f54ebfabfab32b7fe8ac56947fae00a0ff453d975e298d174fc96
EFA 1.26.0	MD5: f8839f12ff2e3b9ba09ae8a82b30e663 SHA256: bc1abc1f76e97d204d3755d2a9ca307fc423e51c63141f798c2f15be3715aa11
EFA 1.25.1	MD5: 6d876b894547847a45bb8854d4431f18 SHA256: d2abc553d22b89a4ce92882052c1fa6de450d3a801fe005da718b7d4b9602b06
EFA 1,25.0	MD5: 1993836ca749596051da04694ea0d00c SHA256: 98b7b26ce031a2d6a93de2297cc71b03af647194866369ca53b60d82d45ad342
EFA 1.24.1	MD5: 211b249f39d53086f3cb0c07665f4e6f SHA256: 120cfeec233af0955623ac7133b674143329f9561a9a8193e473060f596aec62

Versione	Checksum
EFA 1.24.0	MD5: 7afe0187951e2dd2c9cc4b572e62f924 SHA256: 878623f819a0d9099d76ecd41cf4f569d4c3aac0c9bb7ba9536347c50b6bf88e
EFA 1.23.1	MD5: 22491e114b6ee7160a8290145dca0c28 SHA256: 5ca848d8e0ff4d1571cd443c36f8d27c8cdf2a0c97e9068ebf000c303fc40797
EFA 1.23.0	MD5: 38a6d7c1861f5038dba4e441ca7683ca SHA256: 555d497a60f22e3857fdeb3dfc53aa86d05926023c68c916d15d2dc3df6525bd
EFA 1.22.1	MD5: 600c0ad7cdbc06e8e846cb763f92901b SHA256: f90f3d5f59c031b9a964466b5401e86fd0429272408f6c207c3f9048254e9665
EFA 1.22.0	MD5: 8f100c93dc8ab519c2aeb5dab89e98f8 SHA256: f329e7d54a86a03ea51da6ea9a5b68fb354fbae4a57a02f9592e21fce431dc3a

Versione	Checksum
EFA 1.21.0	MD5: 959ccc3a4347461909ec02ed3ba7c372 SHA256: c64e6ca34ccfc3ebe8e82d08899ae8442b3ef552541cf5429c43d11a04333050
EFA 1.20.0	MD5: 7ebfbb8e85f1b94709df4ab3db47913b SHA256: aeefd2681ffd5c4c631d1502867db5b831621d6eb85b61fe3ec80df983d1dcf0
EFA 1.19.0	MD5: 2fd45324953347ec5518da7e3fefa0ec SHA256: 99b77821b9e72c8dea015cc92c96193e8db307deee05b91a58094cc331f16709
EFA 1.18.0	MD5: fc2571a72f5d3c7b7b576ce2de38d91e SHA256: acb18a0808aedb9a5e485f1469225b9ac97f21db9af78e4cd6939700debe1cb6
EFA 1.17.3	MD5: 0517df4a190356ab559235147174cafd SHA256: 5130998b0d2883bbae189b21ab215ecbc1b01ae0231659a9b4a17b0a33ebc6ca

Versione	Checksum
EFA 1.17.2	MD5: a329dedab53c4832df218a24449f4c9a SHA256: bca1fdde8b32b00346e175e597ffab32a09a08ee9ab136875fb38283cc4cd099
EFA 1.17.1	MD5: 733ae2cfc9d14b52017eaf0a2ab6b0ff SHA256: f29322640a88ae9279805993cb836276ea240623820848463ca686c8ce02136f
EFA 1.17.0	MD5: d430fc841563c11c3805c5f82a4746b1 SHA256: 75ab0cee4fb6bd38889dce313183f5d3a83bd233e0a6ef6205d8352821ea901d
EFA 1.16.0	MD5: 399548d3b0d2e812d74dd67937b696b4 SHA256: cecec36495a1bc6fdc82f97761a541e4fb6c9a3cbf3cfcb145acf25ea5dbd45b
EFA 1.15.2	MD5: 955fea580d5170b05823d51acde7ca21 SHA256: 84df4fbc1b3741b6c073176287789a601a589313accc8e6653434e8d4c20bd49

Versione	Checksum
EFA 1.15.1	MD5: c4610267039f72bbe4e35d7bf53519bc SHA256: be871781a1b9a15fca342a9d169219260069942a8bda7a8ad06d4baeb5e2efd7
EFA 1.15.0	MD5: 9861694e1cc00d884fadac07d22898be SHA256: b329862dd5729d2d098d0507fb486bf859d7c70ce18b61c302982234a3a5c88f
EFA 1.14.1	MD5: 50ba56397d359e57872fde1f74d4168a SHA256: c7b1b48e86fe4b3eaa4299d3600930919c4fe6d88cc6e2c7e4a408a3f16452c7
EFA 1.14.0	MD5: 40805e7fd842c36ececb9fd7f921b1ae SHA256: 662d62c12de85116df33780d40e0533ef7dad92709f4f613907475a7a1b60a97
EFA 1.13.0	MD5: c91d16556f4fd53becadbb345828221e SHA256: ad6705eb23a3fce44af3afc0f7643091595653a723ad0374084f4f2b715192e1

Versione	Checksum
EFA 1.12.3	MD5: 818aee81f097918cfaebd724eddea678 SHA256: 2c225321824788b8ca3fbc118207b944cdb096b847e1e0d1d853ef2f0d727172
EFA 1.12.2	MD5: 956bb1fc5ae0d6f0f87d2e481d49fccf SHA256: 083a868a2c212a5a4fcf3e4d732b685ce39cceb3ca7e5d50d0b74e7788d06259
EFA 1.12.1	MD5: f5bfe52779df435188b0a2874d0633ea SHA256: 5665795c2b4f09d5f3f767506d4d4c429695b36d4a17e5758b27f033aee58900
EFA 1.12.0	MD5: d6c6b49fafb39b770297e1cc44fe68a6 SHA256: 28256c57e9ecc0b0778b41c1f777a9982b4e8eae782343dfe1246079933dca59
EFA 1.11.2	MD5: 2376cf18d1353a4551e35c33d269c404 SHA256: a25786f98a3628f7f54f7f74ee2b39bc6734ea9374720507d37d3e8bf8ee1371

Versione	Checksum
EFA 1.11.1	MD5: `026b0d9a0a48780cc7406bd51997b1c0` SHA256: `6cb04baf5ffc58ddf319e956b5461289199c8dd805fe216f8f9ab8d102f6d02a`
EFA 1.11.0	MD5: `7d9058e010ad65bf2e14259214a36949` SHA256: `7891f6d45ae33e822189511c4ea1d14c9d54d000f6696f97be54e915ce2c9dfa`
EFA 1.10.1	MD5: `78521d3d668be22976f46c6fecc7b730` SHA256: `61564582de7320b21de319f532c3a677d26cc46785378eb3b95c636506b9bcb4`
EFA 1.10.0	MD5: `46f73f5a7afe41b4bb918c81888fefa9` SHA256: `136612f96f2a085a7d98296da0afb6fa807b38142e2fc0c548fa986c41186282`
EFA 1.9.5	MD5: `95edb8a209c18ba8d250409846eb6ef4` SHA256: `a4343308d7ea4dc943ccc21bcebed913e8868e59bfb2ac93599c61a7c87d7d25`

Versione	Checksum
EFA 1.9.4	MD5: `f26dd5c350422c1a985e35947fa5aa28` SHA256: `1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14`
EFA 1.9.3	MD5: `95755765a097802d3e6d5018d1a5d3d6` SHA256: `46ce732d6f3fcc9edf6a6e9f9df0ad136054328e24675567f7029edab90c68f1`
EFA 1.8.4	MD5: `85d594c41e831afc6c9305263140457e` SHA256: `0d974655a09b213d7859e658965e56dc4f23a0eee2dc44bb41b6d039cc5bab45`

Note sulla versione di Elastic Fabric Adapter

La tabella seguente descrive la cronologia delle versioni e il log delle modifiche per il software Elastic Fabric Adapter.

Versione	Modifiche	Data di rilascio
1.50.0	• Interrompi il supporto per Amazon Linux 2. L'ultima versione del programma di installazione EFA che supporta AL2 è la 1.49.0. • Aggiornamento a libfabric 2.6.0amzn1.0 •	21 agosto 2026

Versione	Modifiche	Data di rilascio
	Aggiornamento al driver EFA 3.3.0 • Aggiornamento a rdma-core 64.0 • Aggiornamento al AWS plugin OFI NCCL 1.21.1	

Versione	Modifiche	Data di rilascio

1.49.0	• Aggiornamento a libfabric 2.4.0amzn5.0
	• Aggiornamento al driver EFA 3.1.0
	• Aggiornamento a rdma-core 63.0
	• Aggiornamento al AWS plugin OFI NCCL 1.20.0
	• Interrompi il supporto per openSUSE Leap.
	• NGC installa aggiornamenti e correzioni di bug:
	  • Installa i pacchetti libfabric-aws- bin/dev mancanti quando viene utilizzato. `--build-ngc`
	  • Rimuovi il rilevamento automatico del caso d'uso di build-ngc e rimuovi l'opzione associata. `--disable-build-ngc`
	  • `--skip-rdma-core` non è più implicito quando viene specificato. `--build-ngc`
	  • Correzione di bug: quando si utilizza `--build-ngc` e non `--skip-rdma-core` è specificato, rdma-core viene ora installato come previsto.
	  • L'installazione completa è evitata in tutti i casi d'uso di NGC install.
	  • `--skip-mpi` e `--skip-rdma-core` sono ora scelte globali, non limitate al caso d'uso di NGC.
		27 giugno 2026

Versione	Modifiche	Data di rilascio
1.48.0	• Aggiornamento a libfabric 2.4.0amzn3.0 • Ottimizza il recupero degli indirizzi shm nelle operazioni RDM • Correggi i bug use-after-free nel completamento dei pacchetti DC, nel drenaggio CQ, nel test di unità AH e nella registrazione RM • Correggi le race condition nei blocchi efa_rdm_ep_get_peer e QP • Correggi gli array di descrittori non inizializzati che causano segfault con FI_EFA_ENABLE_SHM_TRANSFER=0 • Correggi le perdite di memoria in fi_info, err_buf, distruzione dei dispositivi EFA e test unitari • Aggiungi un controllo nullo per base_ep nel polling CQ per gestire i QP distrutti • Imposta qp->base_ep in efa_qp_create e restituisci un errore se efa_mr_reg_ibv_mr restituisce NULL • Sposta la tabella QP da dominio a dispositivo con blocco a livello di dispositivo • Aggiungi la generazione di QP all'ID della richiesta diretta del percorso dei dati e verifica il numero QP su CQE • Interrompi l'impostazione di qp->ibv_qp_ex->wr_id per Data Path Direct •	14 aprile 2026

Versione	Modifiche	Data di rilascio
	Rimuovi correttamente txe dall'elenco longcts_send al completamento della ricezione • Effettua il refactoring e pulisci efa_cq_handle_error • Converte i contatori di registrazione RM in operazioni atomiche • Migra il codice di registrazione shm MR e introduci la funzione mr regv interna • Disabilita la cache MR per impostazione predefinita in ASAN • Disabilita zcpy_rx solo quando p2p non è disponibile ma è richiesto FI_HMEM • Non tenete traccia del pool tx pkt per una build non di debug • Migliora la procedura wait_send e le funzioni simulate • Regola i livelli di log per efa-direct CQ err_data e efa_show_help • Definisci le macro di sanitizer e disabilita i memhook in ASAN • Aggiungi test unitari per abilitare il percorso degli errori e la gestione del completamento degli errori • Aggiornamento a libnccl-ofi 1.19.0 • Risolto un errore nella gestione degli handle dma-buf creati da e aggiunto il rilevamento del supporto dma-buf quando si utilizzava il runtime HSA su piattaforme ROCm/HSA RoCM	

Versione	Modifiche	Data di rilascio
	• Risolte le potenziali perdite di memoria • È stato risolto il problema della generazione della topologia NCCL per GB200 nei contenitori Docker in cui i nodi NUMA disconnessi dai nodi Package causavano una generazione errata della topologia • Riduzione dell'utilizzo di QP su NIC 0 durante l'inizial izzazione • Scelte migliorate degli algoritmi di sintonizzazione per i tipi di istanza e P6-B200 P6-B300 • Supporto per l'installazione di libnccl-ofi su contenitori NGC • Aggiungi RPM/DEB il supporto per la verifica della firma dei singoli pacchetti • Aggiungi il supporto per RHEL 10 • Aggiungere il plugin OFI NCCL su Debian 12 e RHEL 10	

Versione	Modifiche	Data di rilascio

1.47.0	• Aggiornamento a libfabric 2.4.0amzn1.0
	  • Refactor peer management: sposta endpoint→peer hashmap a livello AV
	  • Aggiungi il contatore di generazione delle entrate dei pacchetti per prevenire problemi ABA
	  • Implementa il blocco del supporto alla lettura CQ (fi_cq_sread) con oggetti wait
	  • Risolto il problema del double free nell'elaborazione dei pacchetti RTM /longread eager/mulreq
	  • Correggi i flag di accesso IBV per la registrazione MR in base alle funzionalità RDMA del dispositivo
	  • Disabilita FI_OPT_EFA_SENDRECV_IN_ORDER_ALIGNED_128_BYTES (restituisce -FI_EOPNOTSUPP)
	  • Ottimizza l'immissione dei pacchetti per adattarli a due righe di cache x86 (128 byte)
	  • Effettua sempre l'operazione efa_rdm_srx_start e visualizza la finestra recv in caso di errori RTM/RTA
	  • Scollega le voci dei pacchetti RX prima del rilascio durante la pulizia degli endpoint
	• Aggiornamento a libnccl-ofi 1.18.0
	  • P6-B300 supporto: aggiunte decisioni di sintonizzazione personalizzate per P6-B300
	  •
		29 gennaio 2026

Versione	Modifiche	Data di rilascio
	Miglioramento delle prestazioni di PAT on P6-B200 grazie alla riduzione del numero di canali per messaggi di dimensioni inferiori • Le impostazioni predefinite del protocollo sono state modificate, il protocollo RDMA su Trn1 e il protocollo SENDRECV su g7e.8xlarge • Selezione dinamica della piattaforma: funzionalità aggiunta per abilitare le ottimizzazioni in fase di esecuzione in base alla presenza di NIC. AWS AWS Ciò consente di utilizzar e un singolo plug-in binario per entrambe le piattaforme AWS e per quelle non.AWS AWS le ottimizzazioni possono ancora essere disabilitate in fase di compilazione. • Supporto fisso per i provider non FI_MR_VIRT_ADDR nel protocollo RDMA • Rapporti migliorati della velocità e della larghezza del collegamento NIC PCIe a NCCL • Modello di threading riprogettato per supportare applicazioni multithread senza richiedere un dominio Libfabric separato per ogni thread. • È stato corretto il supporto per i provider FI_MR_ENDPOINT (supporta solo il protocollo SENDRECV) ripulendo le risorse nell'ordine corretto • Aggiornamento a rdma-core 61.0 • Usa un CQ a thread singolo se è stato fornito Thread Domain • Verifica il numero QP sui processi CQE	

Versione	Modifiche	Data di rilascio

	• Aggiornamento al driver efa 3.0.0
	  • Migliora la gestione degli errori amministrativi
	  • Verifica la correttezza del numero QP al completamento del sondaggio
	  • Rimuovi il backport incondizionato della ricerca della dimensione della pagina migliore
	  • Stampa le stringhe errno per i puntatori di errore
	  • Semplifica il codice nei flussi di creazione di CQ
	  • Esegui il backport delle modifiche upstream nel CQ con il flusso di creazione umem
	  • Modifica la configurazione del DKMS per le nuove versioni del DKMS
	• Aggiornamento a Open MPI 5.0.9amzn1
	  • Bugfix: imposta il livello di threading del dominio in base al supporto dei thread MPI
	  • Bugfix: richiedi il flag FI_COMPLETION per garantire che vengano generati i completamenti per tutti gli eventi di trasferimento dei dati
	  • Condividi i domini tra BTL e MTL per ridurre il numero totale di domini creati per risolvere l'esaurimento delle risorse su sistemi con un numero elevato di core	

Versione	Modifiche	Data di rilascio

1.46.0	• Aggiungi il supporto per Debian 13
	• Aggiornamento a efa-nv-peermem 1.2.3
	  • Correggi gli errori di compilazione e gli avvisi con nuovi kernel e DKMS
	• Aggiornamento a libfabric 2.3.1amzn4.0 https://github.com/aws/libfabric/releases/tag/v2.3.1amzn4.0
	  • Abilita il percorso dati diretto per il percorso del protocollo efa-rdm
	  • Abilita il supporto RoCR HMEM
	  • Nuova opzione FI_OPT_EFA_USE_UNSOLICITED_WRITE_RECV per disabilitare la scrittura non richiesta
	  • Ottimizza i tempi di creazione della connessione
	• Aggiungere libnccl-ofi su RHEL 9, Rocky Linux 9 e Debian 13
		12 dicembre 2025

1.45.1	• Aggiornamento a libfabric 2.3.1amzn3.0 • Risolto il bug che troncava cq_data a 2 byte mentre il provider pubblicizzava il supporto per 4 byte	26 novembre 2025

Versione	Modifiche	Data di rilascio

1.45.0	• Aggiornamento a rdma-core 60.amzn0
	  • Estendi DV Query CQ per restituire il campanello
	• Aggiornamento a libfabric 2.3.1amzn2.0 https://github.com/aws/libfabric/releases/tag/v2.3.1amzn2.0
	  • Supporta la modalità FI_RX_CQ_DATA per efa-direct
	  • Ottimizza il post WQE nel percorso diretto del percorso dati
	  • Correggi le condizioni della gara in cntr progress
	  • Migliora la registrazione dei messaggi di avviso
	  • Gestisce correttamente il completamento dell'RMA per i peer rimossi
	  • Elimina le voci AH dall'AV implicito quando viene raggiunto il limite AH
	• Aggiornamento a libnccl-ofi 1.17.2
	  • Risolto un crash con NCCL v2.28.x quando l'inizializzazione di Libfabric falliva
	  • È stato aggiunto il supporto per la famiglia di istanze g7e
	  • È stato risolto un problema per cui NCCL poteva tentare erroneamente di utilizzare un percorso RDMA GPUDirect su piattaforme che supportano DMA-BUF
	  •
		17 novembre 2025

Versione	Modifiche	Data di rilascio
	È stato risolto il problema relativo all'ordine di spegnimento sulle NIC che richiedono la registrazione della memoria per endpoint (Cray Slingshot)	

Versione	Modifiche	Data di rilascio

1.44.0	• Aggiornamento a rdma-core 59.amzn0
	  • Aggiungi il supporto per associare QP e CQ ai domini di thread
	  • Aggiungi il supporto per allocare un dominio principale
	  • Aggiungi il supporto per allocare i domini dei thread
	  • Aggiungi verbi diretti per interrogare QP e CQ
	  • Aggiungi l'opzione per creare CQ con memoria esterna`
	  • Correggi il sondaggio CQ dopo la distruzione di QP
	• Aggiornamento a libfabric 2.3.1amzn1.0
	• Aggiornamento a Open MPI 5.0.8amzn1
	  • Miglioramenti delle funzionalità
	  • Correzioni di bug
	• Aggiornamento a libnccl-ofi 1.17.1
	  • Supporta NCCL v2.28.3-1 mantenendo al contempo la retrocompatibilità con NCCL v2.17.1 e successive.
	  • La creazione con platform-aws richiede Libfabric v1.22.0amzn4.0 o superiore. Testato con versioni fino a Libfabric v2.3.1amzn1.0.
	  • Correzioni per supportare la compatibilità tra CUDA12 e CUDA13.
		29 ottobre 2025

Versione	Modifiche	Data di rilascio

1,43,3	• Aggiornamento al driver efa 2.17.3
	  • Supporto del P2P con i driver NVIDIA 580
	  • Modifica la registrazione MR per 6.17 e sui kernel
		01 ottobre 2025

1,43,2	• Aggiornamento a libnccl-ofi 1.16.3
	  • Supporta NCCL v2.27.7-1 mantenendo al contempo la retrocompatibilità con NCCL v2.17.1 e successive.
	  • La creazione con platform-aws richiede Libfabric v1.22.0amzn4.0 o superiore. Testato con versioni fino a Libfabric 2.1.0amzn5.0.
	  • Abilitazione del dominio per thread per impostazione predefinita su tutti i tipi di istanze Amazon EC2 per migliorare le prestazioni per alcune applicazioni in cui NCCL crea più thread proxy
		15 agosto 2025

Versione	Modifiche	Data di rilascio

1,43,1	• Aggiornamento a libnccl-ofi 1.16.2
	  • Supporta NCCL v2.27.6-1 mantenendo al contempo la retrocompatibilità con NCCL v2.17.1 e successive.
	  • La creazione con platform-aws richiede Libfabric v1.22.0amzn4.0 o superiore. Testato con versioni fino a Libfabric 2.1.0amzn4.0.
	  • È stata aggiunta una nuova configurazione della piattaforma per supportare l'utilizzo del plugin OFI NCCL sul tipo di istanza Amazon EC2 p5.4xlarge
	• Aggiornamento a libfabric 2.1.0amzn5.0
		31 luglio 2025

Versione	Modifiche	Data di rilascio

1,43,0	• Aggiornamento a libnccl-ofi 1.16.1
	  • Supporta NCCL v2.27.6-1 mantenendo al contempo la retrocompatibilità con NCCL v2.17.1 e successive.
	  • La creazione con platform-aws richiede Libfabric v1.22.0amzn4.0 o superiore. Testato con versioni fino a Libfabric 2.1.0amzn3.
	  • Aggiorna il formato di velocità di collegamento PCI riportato nel file di topologia in modo che corrisponda al kernel 5.7+
	  • Aggiunto SKIP_NICS_WITHOUT_ACCEL_AT_SAME_PCI_LEVEL per saltare le nic libfabric che non dispongono di un acceleratore allo stesso livello pci
	• Aggiornamento al driver efa 2.17.2
	• Aggiornamento a efa-nv-peermem 1.2.2
	• Aggiornamento a libfabric 2.1.0amzn4.0
	• Aggiornamento a rdma-core 58.amzn0
	  • Risolvi il doppio utilizzo dell'indice delle richieste di lavoro
	  • Aggiungi la lunghezza WQE al tracepoint post_send
	• Abilita le ottimizzazioni per le piattaforme Graviton
	• Supporto obsoleto per Ubuntu 20.04
		25 luglio 2025

Versione	Modifiche	Data di rilascio

1.42.0	• Aggiornamento al driver efa 2.15.3
	• Aggiornamento a efa-nv-peermem 1.2.1
	• Aggiornamento a rdma-core 57.amzn1
	  • Risolvi il doppio utilizzo dell'indice delle richieste di lavoro
	• Aggiornamento a libfabric 2.1.0amzn3.0
	• Aggiornamento a libnccl-ofi 1.15.0
	  • Supporta NCCL 2.26.6-1 mantenendo la compatibilità con le versioni precedenti con NCCL v2.17.1 e successive.
	  • La creazione con platform-aws richiede Libfabric v1.22.0amzn4.0 o superiore. Testato con versioni fino a Libfabric 2.1.0amzn3.
	  • Custruzione del supporto per sistemi e piattaforme
	  • È stato aggiunto il supporto per la piattaforma Amazon EC2 P6-B200
	  • Modificato il nome della libreria di plugin predefinita in libnccl-net-ofi.so e, per impostazione predefinita, crea un collegamento simbolico da libnccl-net-ofi.so a libnccl-net.so per mantenere la compatibilità con le versioni precedenti. Ciò consente agli utenti di impostare NCCL_NET_PLUGIN=ofi per forzare NCCL a utilizzare il plugin OFI per la comunicazione. La specificazione di --disable-nccl-net-symlink da configurare salterà il collegamento simbolico, permettendo l'installazione di più plugin nello stesso container.
	  • Ottimizzazione e miglioramenti delle prestazioni
		6 giugno 2025

Versione	Modifiche	Data di rilascio
	• È stato aggiunto il supporto del tuner P6-B200 per AllReduce AllGather, e per le ReduceScatter regioni per bitmask 0x0 e 0x7 • Latenza predefinita aggiornata per P5en e piattaforme in base a risultati e analisi empirici P6-B200 • Aggiornamento per utilizzare l'API NCCL v10 con supporto dei parametri trafficClass per la prioritizzazione del traffico futuro • Base di codice del plugin migrata da C a C++ • È stato aggiunto il supporto per i lavori in cui il numero di NIC per GPU è diverso tra i sistemi. Per ulteriori informazi oni, consulta la documentazione della variabile di ambiente di runtime OFI_NCCL_FORCE_NUM_RAILS.	
1.41.0	• Aggiornamento a rdma-core 57.amzn0	16 maggio 2025
1.40.0	• Aggiornamento a libfabric 2.1.0amzn2.0 • Aggiornamento a rdma-core 56.0 • Aggiornamento a efa-config 1.18. • Supporto obsoleto per Debian 10 • Aggiornamento a libnccl-ofi 1.14.2 • Abilitazione del supporto CUDA in Libfabric su ARM per Ubuntu e Amazon Linux 2023 • Aggiunta di libnccl-ofi su ARM per Ubuntu e Amazon Linux 2023	2 maggio 2025
1.39.0	• Aggiornamento a libfabric 2.1.0 • Aggiornamento a Open MPI 5.0.6 • Aggiornamento a libnccl-ofi 1.14.1 • Aggiornamento al driver efa 2.15.0	16 aprile 2025

Versione	Modifiche	Data di rilascio
1,38,1	• Aggiornato a `Libfabric 1.22.0amzn5.0`	3 marzo 2025
1,38,0	• Add `libnccl-ofi 1.13.2-1`	08 gennaio 2025
1.37.0	• Aggiornamento ad `libfabric 1.22.0amzn4.0` • Aggiornamento ad `rdma-core 54.amzn0`	18 novembre 2024
1,36,0	• Aggiunta del supporto per Debian 12 • Distribuisci `efa_test.sh` come script di utilità a `/opt/amazon/efa/bin` • Aggiornamento al driver efa 2.13.0 • Aggiornamento ad `libfabric 1.22.0amzn3.0` • Aggiornamento ad `rdma-core 54.0` • Aggiornamento a open mpi 4.1.7	7 novembre 2024
1.35.0	• Aggiornamento a Open MPI 5.0.5 • Aggiornamento a PRRTE 3.0.6 e rinomina il pacchetto RPM in prrte-aws • Rinomina del pacchetto RPM di OpenPMIX in pmix-aws • Configurazione delle opzioni di costruzione per le build dpkg e RPM • Aggiornamento ad `Libfabric 1.22.0amzn2.0` • Aggiornamento al driver efa 2.12.1	14 ottobre 2024
1,34,0	• Abbandono del supporto per CentOS 7 e RHEL 7 • Acquisizione di `Libfabric 1.22.0amzn1.0` • Aggiornamento del pacchetto efa-config a 1.17	6 agosto 2024

Versione	Modifiche	Data di rilascio
1,33,0	• Aggiornamento al driver efa 2.10.0 • Aggiornamento ad `rdma-core 52.0` • Aggiornamento a PRRTE 3.0.5 • Aggiornamento a Open MPI 5.0.3 • Aggiunto il supporto per Ubuntu 24.04 LTS • Rimuozione della documentazione HTML di OpenPMIX, PRRTE e Open MPI. Gli utenti devono fare riferimento al sito Web ufficiale. • Abbandono del supporto per openSUSE 15.4 o precedenti	20 giugno 2024
1.32.0	• Aggiornamento al driver efa 2.8.0 • Aggiornamento al driver efa-nv-peermem 1.1.1 • Aggiornamento del pacchetto efa-config a 1.16 • Aggiornamento del pacchetto efa-profile a 1.7 • Aggiornamento ad `rdma-core 50.0` • Aggiornamento ad `libfabric 1.21.0amzn1.0` • Miglioramento di `efa_test.sh` con la selezione delle porte `fi_pingpong` • Installazione del nuovo rdma-core dal sistema quando necessario	18 aprile 2024
1,31,0	• Aggiornamento a OpenPMIx 4.2.8 • Aggiornamento a PRRTE 3.0.3 • Aggiornamento a Open MPI 5.0.2 e conversione dei componenti MCA in DSO. • Aggiornamento ad `Libfabric 1.20.1amzn1.0`	7 marzo 2024

Versione	Modifiche	Data di rilascio
1.30.0	• Inclusione di OpenPMix 4.2.7, installato in `/opt/amazon/pmix` per impostazione predefinita • Inclusione di PRRTE 3.0.2, installato in `/opt/amazon/prrte` per impostazione predefinita • Inclusione di Open MPI 5.0.0, installato in `/opt/amazon/openmpi5` per impostazione predefinita • Aggiornamento di efa-profile a 1.6	Dicembre 2023
1.29.1	• Acquisizione di `libfabric 1.19.0amzn4.0`	Dicembre 2023
1.29.0	• Acquisizione del driver del kernel efa 2.6.0 • Acquisizione di `libfabric 1.19.0amzn3.0`	Novembre 2023
1.28.0	• Aggiornamento di Open MPI a 4.1.6 • Acquisizione di `libfabric 1.19.0amzn2.0`	Ottobre 2023
1.27.0	• Aggiunta di `Libfabric 1.19.0amzn1.0` al programma di installazione • Abilitazione degli atomici incorporati in GCC per Open MPI 4	Settembre 2023
1,261	• `efa_test.sh` : correzione del bug dei tentativi infiniti	Settembre 2023
1.26.0	• Aggiunta del supporto per RHEL 9 • Correzione della build di debug su più distribuzioni • Acquisizione di `libfabric 1.18.2amzn1.0` • `efa_test.sh` : aggiunta di un tentativo per `fi_pingpong`	Settembre 2023
1.25.1	• Acquisizione di `libfabric 1.18.1amzn1.0` • Aggiornamento dei timeout negli script del programma di installazione EFA	Settembre 2023

Versione	Modifiche	Data di rilascio
1.25.0	• Aggiungi il supporto per Amazon Linux 2023 • Correzione di bug nel test post-installazione	Luglio 2023
1.24.1	• Aggiornamento di libfabric a 1.18.1 • Aggiornamento del driver efa a 2.5.0	Luglio 2023
1.24.0	• Acquisizione di `rdma-core 46.0` • Acquisizione di un driver efa 2.4.1 • Supporto di Debian 11	Giugno 2023
1.23.1	• Acquisizione di `libfabric 1.18.0amzn2.0`	Giugno 2023
1.23.0	• Aggiunta del supporto per Debian 10 • Abbandono del supporto per Ubuntu 18.04 LTS • Aggiornamento del pacchetto efa-config a 1.14 • Acquisizione di `libfabric 1.18.0amzn1.0`	Maggio 2023
1.22.1	• Aggiornamento di libfabric a 1.17.1	Marzo 2023
1.22.0	• Aggiornamento di Open MPI a 4.1.5 • Aggiornamento di libfabric a 1.17.0 • Aggiornamento del pacchetto efa-config a 1.13	Febbraio 2023
1.21.0	• Aggiunta del supporto per il sistema operativo Rocky Linux 9 • Acquisizione di un driver efa 2.1.1 • Acquisizione di `libfabric 1.16.1amzn3.0` • Aggiornamento del pacchetto efa-config a 1.12	Dicembre 2022
1.20.0	• Aggiunta del supporto per il sistema operativo Rocky Linux 8. • Acquisizione di un driver efa 2.1.0. • Acquisizione di `rdma-core 43.0`. • Acquisizione di `libfabric 1.16.1amzn1.0`	Novembre 2022

Versione	Modifiche	Data di rilascio
1.19.0	• Acquisizione di `libfabric 1.16.0` • Costruzione di Open MPI con `--enable-orterun-prefix-by-default`	ottobre 2022
1.18.0	• Aggiungi il supporto per Ubuntu22.04	Agosto 2022
1.17.3	• Aggiornamento di libfabric a `1.16.0~amzn4.0` . ~ indica che si tratta di una versione non definitiva di libfabric 1.16.0. • Estende il timeout del test di pingpong post-installazione a 20 secondi	Agosto 2022
1.17.2	• Aggiornamento di libfabric a `1.16.0~amzn3.0` . ~ indica che si tratta di una versione non definitiva di libfabric 1.16.0.	luglio 2022
1.17.1	• Aggiornamento di libfabric a `1.16.0~amzn2.0` . ~ indica che si tratta di una versione non definitiva di libfabric 1.16.0. • Disabilitazione del provider di rete sperimentale durante la costruzione di libfabric	luglio 2022
1.17.0	• Aggiornamento di `rdma-core` a v41.0 • Aggiornamento di Open MPI a 4.1.4 • Aggiornamento di libfabric a `1.16.0~amzn1.0` . ~ indica che si tratta di una versione non definitiva di libfabric 1.16.0.	luglio 2022
1.16.0	• Aggiornamento di libfabric a `1.15.1amzn1.0` , contiene la modifica del nome della libreria neuronale • Aggiornamento di efa-config a 1.10 • Esclusione dei provider opx e rxd nella build di libfabric	giugno 2022
1.15.2	• Aggiornamento di libfabric a 1.14.1	Maggio 2022
1.15.1	• Aggiornamento di libfabric a `1.14.0amzn1.0`	marzo 2022

Versione	Modifiche	Data di rilascio
1.15.0	• Risoluzione di un bug che causava il fallimento dell'installazione su Open SuSE 15.3 • Abbandono del supporto per Open SuSE 15.2 (poiché Open SuSE 15.2 ha raggiunto la fine del ciclo di vita) • Abbandono del supporto di CentOS 8 (quando CentOS 8 ha raggiunto la fine del ciclo di vita) • Aggiornamento di libfabric a 1.14.0 • Aggiornamento del driver del kernel efa a 1.16.0 • Aggiornamento di `rdma-core` a v39.0 • Aggiornamento di Open MPI alla versione 4.1.2.	Febbraio 2022
1.14.1	• Aggiornamento di libfabric a `1.13.2amzn1.0` .	ottobre 2021
1.14.0	• Acquisizione del driver del kernel efa 1.14.2. • Realizzazione di `-g, --enable-gdr` in `efa_installer.sh` come un'opzione no-op poiché l'ultimo driver del kernel efa abilita il supporto GDR per impostazione predefinita. • Acquisizione di `rdma-core v37.0`. • Acquisizione di `libfabric 1.13.2`. • Aggiungi l'elenco dei pacchetti e confrontalo RPM/DEB con l'elenco durante l'installazione per evitare l'installazione di pacchetti sconosciuti. • Aggiunta una pausa in uno script del programma di installazione per attendere che la regola udev sia applicata dopo il ricaricamento del driver EFA.	ottobre 2021

Versione	Modifiche	Data di rilascio
1.13.0	• Aggiornamento di `rdma-core` a v35.0. • Aggiornamento di `libfabric` a v1.13.0amzn1.0. • Aggiungi il supporto EFA per CentOS/RHEL 8 sulla piattaforma Gravition2. • Aggiunta della logica di confronto delle versioni nello script del programma di installazione per saltare l'installazione del pacchetto locale quando ce n'è uno installato nel sistema con una versione superiore.	Agosto 2021
1.12.3	• Aggiornamento del modulo kernel EFA a 1.13.0. • Aggiornamento del pacchetto efa-config alla versione 1.9. Miglioramento del calcolo della prenotazione di huge page per gestire huge page di dimensioni predefinite.	luglio 2021
1.12.2	• Aggiornamento del modulo kernel EFA a 1.12.3. • Costruzione di pacchetti debian Open MPI con `--with-libevent=external` e `--with-hwloc=external` . • Incrementazione dell'ID build Open MPI rpm a 2 per risolvere il problema di compatibilità con le versioni precedenti di HWLOC su CentOS 8. • Rimozione dell'installazione dei pacchetti kernel-devel e kernel-source su SLES15SP2 e openSUSE 15.2.	giugno 2021
1.12.1	• Aggiornamento di Libfabric alla versione 1.11.2amzon1.1. • Aggiornamento del modulo kernel EFA alla versione 1.12.1.	Maggio 2021

Versione	Modifiche	Data di rilascio
1.12.0	• Aggiornamento di Open MPI alla versione 4.1.1. • Aggiornamento di Libfabric alla versione 1.11.2amzn1.0. • Costruzione di rdma-core per Amazon Linux 2 utilizzando la stessa configurazione di packaging di AL2 rdma-core. • Non forzare `-Wl,--enable-new-dtags` durante la costruzione di RPM Open MPI. • Costruzione di Open MPI con librerie di sistema per hwloc e libevent. • Aggiornamento del modulo kernel EFA alla versione 1.12.0 • Aggiornamento del pacchetto efa-config alla versione 1.8. Miglioramento del calcolo della prenotazione di huge page per istanze di lunga durata. • Aggiornamento del pacchetto efa-profile alla versione 1.5. Rimozione del file di ottimizzazione dei collettivi open mpi che ha funzionato come soluzione alternativa per correggere il blocco di Open MPI 4.1.0 su P4d. • Aggiornamento di `rdma-core` a v32.1. • Abbandono del supporto per Amazon Linux 1 e Ubuntu 16.04.	Maggio 2021
1.11.2	• Risoluzione del blocco di Open MPI quando si utilizza Open MPI su P4d modificando l'algoritmo predefinito utilizzato per implementare MPI_BARRIER tramite un file di configurazione. • Disabilitazione dell'uso degli atomici incorporati in Open MPI su ARM tramite `--disable-builtin-atomics` per aggirare il problema del compilatore.	febbraio 2021

Versione	Modifiche	Data di rilascio
1.11.1	• Aggiornamento di Open MPI alla versione 4.1.0. • Aggiornamento del pacchetto efa-config alla versione 1.7. Miglioramento del calcolo del numero di prenotazioni di huge page. • Aggiornamento del pacchetto efa-profile alla versione 1.3. Rimuove il file di decisione dei collettivi non necessari ora che è usato Open MPI 4.1.0.	dicembre 2020
1.11.0	• Aggiunta del supporto per la piattaforma Gravition2. • Aggiornamento di `rdma-core` alla versione 31.2amzn. • Aggiornamento di Libfabric alla versione 1.11.1amzn1.0. • Aggiornamento di efa-config alla versione 1.6. • Aggiornamento di efa-profile alla versione 1.2.	dicembre 2020
1.10.1	• Aggiunta del supporto per CentOS/RHEL 8. • Aggiunta del supporto per Ubuntu 20.04. • Aggiunta del supporto per SUSE Linux Enterprise 15.	Novembre 2020
1.10.0	• Aggiunta del supporto GPUDirect RDMA per la piattaforma P4d. Usa l'opzione `--enable-gdr` installer per installare il modulo del GDR-aware kernel e lo spazio utente. • Aggiornamento del modulo kernel EFA alla versione 1.10.2. • Aggiornamento di `rdma-core` alla versione 31.amzn0. • Aggiornamento di Libfabric alla versione 1.11.1. • Aggiornamento di Open MPI alla versione 4.0.5. • Aggiornamento di efa-config alla versione 1.5. • Aggiornamento di efa-profile alla versione 1.1. Include il file decisionale dei collettivi Open MPI migliorato.	ottobre 2020
1.9.5	• Aggiornamento di efa-config alla versione 1.4. Corregge un bug nel file decisionale dei collettivi Open MPI.	settembre 2020

Versione	Modifiche	Data di rilascio
1.9.4	• Aggiornamento di Open MPI alla versione 4.0.3. • Aggiornamento di Libfabric alla versione 1.10.1amazon1.1. • Aggiornamento di `rdma-core` alla versione 28.amzn0.	luglio 2020
1.9.3	• Aggiornamento del modulo kernel EFA alla versione 1.6.0. • Aggiornamento di `rdma-core` alla versione 28.amzn0. • Aggiornamento di Libfabric alla versione 1.10.1amzn1.1. • Aggiornamento di efa-config alla versione 1.3. Aggiunge un file di ottimizzazione dei collettivi per Open MPI. • Salto dell'installazione di dms se è già installato. • Correzione della modalità di installazione `--skip-kmod` per farla funzionare davvero.	Giugno 2020
1.8.4	• Spostamento dei file di configurazione nei pacchetti efa-confi g ed efa-profile in modo che siano tracciati dal gestore dei pacchetti del sistema operativo. • Aggiornamento di Open MPI alla versione 4.0.3.	Aprile 2020
1.8.3	• Aggiornamento del modulo kernel EFA alla versione 1.5.1. • DKMS distribuito su alcune piattaforme anziché affidarsi agli archivi EPEL per una maggiore affidabilità dell'installazione. • Su RHEL 7, installazione degli RPM costruiti su CentOS 7 anziché gli RPM costruiti su Amazon Linux 2.	Febbraio 2020
1.8.2	• Ritorno di `rdma-core` alla versione 25 per via di una mancata corrispondenza nella denominazione dei dispositivi tra il modulo del kernel e `rdma-core` .	Gennaio 2020
1.8.1	• Aggiornamento di Libfabric alla versione 1.9.0amzn1.1.	Gennaio 2020

Versione	Modifiche	Data di rilascio
1.8.0	• Aggiornamento di `rdma-core` alla versione 27.0. • Aggiornamento del modulo kernel EFA alla versione 1.5.0. • Aggiornamento di Libfabric alla versione 1.9.0amzn1.0. • Aggiunta dell'opzione `--minimal` per installare solo il modulo del kernel EFA e `rdma-core` .	Dicembre 2019
1.7.1	• Aggiornamento di Libfabric alla versione 1.8.1amzn1.3.	Dicembre 2019
1.7.0	• Aggiunta del file del modulo Libfabric. • Aggiornamento di Libfabric alla versione 1.8.1amzn1.1.	Novembre 2019
1.6.2	• Aggiornamento di Open MPI alla versione 1.6.2.	Ottobre 2019
1.6.1	• Aggiornamento di Libfabric alla versione 1.8.1amzn1.0. • Aggiornamento di Open MPI alla versione 4.0.1. • Aggiornamento di `rdma-core` alla versione 26.0.	Ottobre 2019
1.5.4	• Aggiornamento del modulo kernel EFA alla versione 1.4.1.	Settembre 2019
1.5.3	• Aggiornamento del modulo kernel EFA alla versione 1.3.1. • Evitamento dell'installazione di pacchetti `kernel-devel` o `linux-headers` a meno che non si installi il driver del kernel.	Settembre 2019
1.5.1	• Configurazione delle huge page solo quando è presente un dispositivo EFA.	Agosto 2019
1.5.0	• Aggiornamento di Libfabric alla versione 1.8.0amzn1.1. • Aggiornamento di `rmda-core` alla versione 25.0.	Agosto 2019

Versione	Modifiche	Data di rilascio
1.4.1	• Aggiunta dei percorsi delle librerie Libfabric e Open MPI (`/opt/amazon/efa/lib64` e `/opt/amazon/efa/openmpi/lib`) a `/etc/ld.so.conf.d/efa.conf` per garantire che le librerie condivise Open MPI e Libfabric siano posizionate correttamente.	Luglio 2019
1.4.0	• Aggiornamento del modulo kernel EFA alla versione 1.3.0. • Aggiornamento di Libfabric alla versione 1.8.0amzn1.0 • Prima versione per supportare Intel MPI 2019 Update 4.	Luglio 2019

Topologia Amazon EC2

La topologia di Amazon EC2 offre una visualizzazione gerarchica della vicinanza relativa della capacità di calcolo. Puoi utilizzare queste informazioni per gestire l'infrastruttura di calcolo ad alte prestazioni (HPC), machine learning (ML) e intelligenza artificiale generativa su larga scala.

API disponibili

Amazon EC2 offre due API per comprendere la topologia di EC2:

- DescribeInstanceTopology
  - Mostra qual è la posizione delle istanze in esecuzione le une rispetto alle altre nella gerarchia di rete.
  - Aiuta a ottimizzare le posizioni in cui eseguire i carichi di lavoro sulle istanze esistenti.
- DescribeCapacityReservationTopology
  - Mostra dove la capacità riservata sarà posizionata rispetto ad altra capacità nella gerarchia di rete prima dell'avvio delle istanze.
  - Aiuta a pianificare la capacità offrendo informazioni sul posizionamento della capacità riservata prima dell'avvio delle istanze.

Vantaggi principali

La topologia di EC2 offre i seguenti vantaggi principali:

- Gestione della capacità: ottimizza l'utilizzo delle risorse.
- Pianificazione dei processi: prendi decisioni informate sul posizionamento dei carichi di lavoro.
- Classificazione dei nodi: comprendi la vicinanza relativa per ottimizzare le prestazioni delle istanze strettamente collegate.

Considerazioni

- Le visualizzazioni della topologia sono disponibili solamente per:
  - Le istanze nello stato `running`.
  - Le prenotazioni della capacità nello stato `pending` o `active`.
- Ogni vista della topologia è unica per. Account AWS
- Non Console di gestione AWS supporta la visualizzazione della topologia.
- Anche se le informazioni sulla topologia aiutano a comprendere il posizionamento dell'istanza, non puoi utilizzarle per avviare una nuova istanza fisicamente vicina a un'istanza esistente. Per influenzare il posizionamento delle istanze, puoi creare delle Prenotazioni della capacità in gruppi di posizionamento cluster.

Prezzi

La descrizione della topologia di EC2 non comporta costi aggiuntivi.

Indice

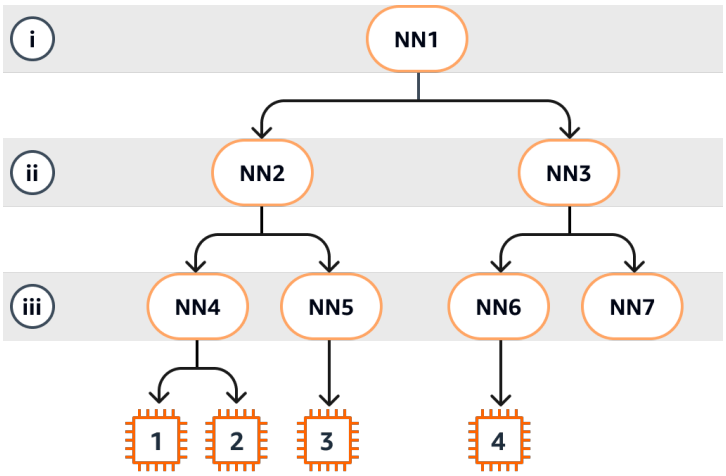
- Come funziona la topologia di Amazon EC2
- Prerequisiti per la topologia di Amazon EC2
- Esempi di topologia dell'istanza Amazon EC2

Come funziona la topologia di Amazon EC2

La AWS rete è organizzata in una gerarchia di livelli. Le istanze EC2 si connettono alla rete in corrispondenza o al di sotto del terzo livello, a seconda del tipo di istanza. La topologia di un'istanza è descritta da un insieme di nodi, con un nodo in ogni livello della rete. Il nodo impostato nella risposta DescribeInstanceTopology o DescribeCapacityReservationTopology API fornisce una vista dall'alto verso il basso della gerarchia di rete, con il nodo inferiore connesso a un'istanza.

> **Note**
>
> Alcuni tipi di istanza comprendono 4 nodi di rete in un set di nodi che rappresenta 4 livelli della rete, mentre altri includono 3 nodi di rete che rappresentano 3 livelli. Per conoscere i tipi di istanza supportati, consulta Tipi di istanza.
> A seconda del tipo di prenotazione della capacità, potresti visualizzare solo 1, 2 o 3 nodi di rete.

Il diagramma riportato di seguito offre una rappresentazione visiva che puoi utilizzare per comprendere la topologia di EC2. I nodi di rete sono identificati come NN1 — NN7. Le numerazioni i, ii e iii rappresentano i livelli di rete. I numeri 1, 2, 3 e 4 identificano le istanze EC2. Le istanze si connettono a un nodo nel livello inferiore, identificato da iii nel seguente diagramma. Più istanze possono connettersi allo stesso nodo.



In questo esempio:

- L'istanza 1 si connette al nodo di rete 4 (NN4) nel livello iii. NN4 si connette al nodo di rete 2 (NN2) nel livello ii e NN2 si connette al nodo di rete 1 (NN1) nel livello i, che è la parte superiore della gerarchia di rete in questo esempio. Il set di nodi di rete comprende NN1, NN2 e NN4, espressi gerarchicamente dai livelli superiori al livello inferiore.
- L'istanza 2 si connette anche al nodo di rete 4 (NN4). L'istanza 1 e l'istanza 2 condividono lo stesso set di nodi di rete: NN1, NN2 e NN4.
- L'istanza 3 si connette al nodo di rete 5 (NN5). NN5 si connette a NN2 e NN2 si connette a NN1. Il set di nodi di rete per l'istanza 3 è NN1, NN2 e NN5.
- L'istanza 4 si connette al nodo di rete 6 (NN6). Il set di nodi di rete è NN1, NN3 e NN6.

Se si considera la vicinanza delle istanze 1, 2 e 3, le istanze 1 e 2 sono più vicine tra loro perché si connettono allo stesso nodo di rete (NN4), mentre l'istanza 3 è più lontana perché si connette a un nodo di rete diverso (NN5).

Se si considera la prossimità di tutte le istanze in questo diagramma, le istanze 1, 2 e 3 sono più vicine tra loro rispetto all'istanza 4 perché condividono NN2 nel loro set di nodi di rete.

Come regola generale, se il nodo di rete connesso a due istanze qualsiasi è lo stesso, queste istanze sono fisicamente vicine l'una all'altra, come nel caso delle istanze 1 e 2. Inoltre, minore è il numero di salti tra i nodi di rete, più le istanze sono vicine tra loro. Ad esempio, le istanze 1 e 3 hanno meno passaggi verso un nodo di rete comune (NN2) rispetto al nodo di rete (NN1) che hanno in comune con l'istanza 4 e sono quindi più vicine tra loro di quanto non lo siano all'istanza 4.

In questo esempio non ci sono istanze in esecuzione nel nodo di rete 7 (NN7) e pertanto l'output dell'API non includerà NN7.

Come interpretare l'output DescribeInstanceTopology

È possibile descrivere la topologia dell'istanza utilizzando l'DescribeInstanceTopologyAPI. L'output fornisce una visualizzazione gerarchica della topologia di rete sottostante per un'istanza.

Il seguente output di esempio corrisponde alle informazioni sulla topologia di rete delle quattro istanze del diagramma precedente. Ai fini di questo esempio, i commenti sono inclusi nell'output di esempio.

È importante tenere presente le seguenti informazioni nell'output:

- `NetworkNodes` descrive il set di nodi di rete di una singola istanza.
- In ogni set di nodi di rete, i nodi di rete sono elencati in ordine gerarchico dall'alto verso il basso.
- Il nodo di rete connesso all'istanza è l'ultimo nodo di rete nell'elenco (il livello inferiore).
- Per capire quali istanze sono vicine tra loro, individua innanzitutto i nodi di rete comuni nel livello inferiore. Se non ci sono nodi di rete comuni nel livello inferiore, individua i nodi di rete comuni nei livelli superiori.

Nel seguente output di esempio, le istanze `i-1111111111example` e `i-2222222222example` sono posizionate più vicine l'una all'altra rispetto alle altre istanze di questo esempio, perché hanno il nodo di rete `nn-4444444444example` in comune nel livello inferiore.

> **Note**
>
> La risposta contiene 3 o più nodi di rete. Per ulteriori informazioni sul numero di nodi di rete nella risposta per ogni tipo di istanza supportato, consulta Tipi di istanza.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",  //Corresponds to instance 1
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 in layer i
                "nn-2222222222example",           //Corresponds to NN2 in layer ii
                "nn-4444444444example"            //Corresponds to NN4 in layer iii -
 bottom layer, connected to the instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",  //Corresponds to instance 2
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-4444444444example"            //Corresponds to NN4 - layer iii -
 connected to instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",  //Corresponds to instance 3
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
```

```
                "nn-5555555555example"           //Corresponds to NN5 - layer iii -
 connected to instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-444444444example",  //Corresponds to instance 4
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",          //Corresponds to NN1 - layer i
                "nn-3333333333example",          //Corresponds to NN3 - layer ii
                "nn-6666666666example"           //Corresponds to NN6 - layer iii -
 connected to instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Come interpretare l'output DescribeCapacityReservationTopology

È possibile descrivere la topologia di prenotazione della capacità utilizzando l'DescribeCapacityReservationTopologyAPI. L'output offre una visualizzazione gerarchica della topologia di rete sottostante per la capacità riservata.

L'output di esempio riportato di seguito corrisponde alle informazioni sulla topologia di rete del diagramma precedente. Ai fini di questo esempio, i commenti sono inclusi nell'output di esempio.

È importante tenere presente le seguenti informazioni nell'output:

- `NetworkNodes` descrive il set di nodi di rete di una singola prenotazione della capacità.
- In ogni set di nodi di rete, i nodi di rete sono elencati in ordine gerarchico dall'alto verso il basso.
- Il nodo di rete connesso alla prenotazione della capacità è l'ultimo nodo di rete nell'elenco (il livello inferiore).

- Per comprendere se le prenotazioni della capacità saranno vicine tra loro, per prima cosa trova i nodi di rete in comune nel livello inferiore dell'output. Se non ci sono nodi di rete comuni nel livello inferiore, individua i nodi di rete comuni nei livelli superiori.

Nel seguente output di esempio, `cr-1111111111example` si trova in `nn-2222222222example` e `cr-2222222222example` si trova in `nn-3333333333example`. Dato che le prenotazioni della capacità si trovano su nodi di rete diversi in `layer ii`, la comunicazione tra le istanze di una prenotazione della capacità e le istanze dell'altra non sarà efficiente.

> **Note**
>
> La risposta contiene 1, 2 o 3 nodi di rete a seconda del tipo di prenotazione della capacità.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1111111111example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",      //Corresponds to NN1 - layer i
                "nn-2222222222example"       //Corresponds to NN2 - layer ii
                // Visibility of additional nodes requires an instance launch and
                // the DescribeInstanceTopology API
            ],
            "AvailabilityZone": "us-west-2a"
        },
        {
            "CapacityReservationId": "cr-2222222222example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",      //Corresponds to NN1 - layer i
                "nn-3333333333example"       //Corresponds to NN3 - layer ii
                // Visibility of additional nodes requires an instance launch and
                // the DescribeInstanceTopology API
            ],
            "AvailabilityZone": "us-west-2a"
```

```
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Differenze tra e DescribeInstanceTopology DescribeCapacityReservationTopology

La tabella seguente confronta le principali differenze tra le DescribeCapacityReservationTopology API DescribeInstanceTopology e:

Punto di confronto	DescribeInstanceTopology	DescribeCapacityReservation Topology
Fase di utilizzo	Post-launch (modalità di esecuzione)	Pre-launch (modalità di pianificazione e gestione)
Scopo principale	Ottimizzare i carichi di lavoro sulle istanze in esecuzione	Pianificare la capacità e gestire le prenotazioni della capacità (unione, divisione, assegnazione) prima dell'avvio dell'istanza.
Numero di nodi di rete	Mostra tutti i nodi di un'istanz a in esecuzione. Se l'istanza è inclusa in una prenotazi one della capacità, i primi nodi saranno corrispondenti alla topologia della relativa prenotazione della capacità, seguiti da nodi aggiuntivi per la connessione all'istanza.	Mostra un set parziale di nodi che può variare in base allo stato (`pending` o `active`) e al tipo* della prenotazione della capacità.
Stato	Le istanze devono essere nello stato `running`.	Le prenotazioni della capacità devono essere nello stato `pending` o `active`.
Casi d'uso	• Ottimizzazione dei carichi di lavoro • Ottimizzazione prestazioni	• Pianificazione della capacità

Punto di confronto	DescribeInstanceTopology	DescribeCapacityReservationTopology
	• Analisi della topologia del runtime	• Gestione delle prenotazioni di capacità (merge/split/assign) • Pre-launch valutazione della topologia

*Per i blocchi di capacità per Ultraserver, il set di nodi di rete è lo stesso quando si descrive la topologia di una prenotazione della capacità `active` o della relativa istanza in esecuzione.

Prerequisiti per la topologia di Amazon EC2

Per descrivere la topologia di Amazon EC2, assicurati che le istanze e le prenotazioni della capacità soddisfino i seguenti prerequisiti.

Prerequisiti per:

- Regioni AWS
- Tipi di istanza
- Stato
- autorizzazioni IAM

Regioni AWS

Supportato Regioni AWS:

- Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (California settentrionale), Stati Uniti occidentali (Oregon)
- Africa (Città del Capo)
- Asia Pacifico (Giacarta), Asia Pacifico (Hong Kong), Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne), Asia Pacifico (Mumbai), Asia Pacifico (Osaka), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Asia Pacifico (Tokyo)
- Canada (Centrale)
- Europa (Francoforte), Europa (Irlanda), Europa (Londra), Europa (Parigi), Europa (Spagna), Europa (Stoccolma), Europa (Zurigo)

- Israele (Tel Aviv)
- Medio Oriente (Bahrein), Medio Oriente (Emirati Arabi Uniti)
- Sud America (San Paolo)
- AWS GovCloud (US-West)
- AWS European Sovereign Cloud (Germany)

L' DescribeCapacityReservationTopology API non è supportata in Israele (Tel Aviv) e AWS GovCloud (US-West).

Tipi di istanza

Tipi di istanze supportati:

- Restituisce 3* nodi di rete nella risposta:
  - `g6e.xlarge` | `g6e.2xlarge` | `g6e.4xlarge` | `g6e.8xlarge` | `g6e.12xlarge` | `g6e.16xlarge` | `g6e.24xlarge` | `g6e.48xlarge` | `g7e.2xlarge` | `g7e.4xlarge` | `g7e.8xlarge` | `g7e.12xlarge` | `g7e.24xlarge` | `g7e.48xlarge`
  - `hpc6a.48xlarge` | `hpc6id.32xlarge` | `hpc7g.4xlarge` | `hpc7g.8xlarge` | `hpc7g.16xlarge` | `hpc7a.12xlarge` | `hpc7a.24xlarge` | `hpc7a.48xlarge` | `hpc7a.96xlarge` | `hpc8a.96xlarge`
  - `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `p5.48xlarge` | `p5e.48xlarge` | `p5en.48xlarge` | `p6e-gb200.36xlarge`
  - `trn1.2xlarge` | `trn1.32xlarge` | `trn1n.32xlarge` | `trn2.48xlarge` | `trn2u.48xlarge`
- Restituisce 4* nodi di rete nella risposta:
  - `p6-b200.48xlarge` | `p6-b300.48xlarge`

* Il numero di nodi di rete restituiti è applicabile solo quando si utilizza l' DescribeInstanceTopology API. Per l' DescribeCapacityReservationTopology API, il numero di nodi di rete restituiti varierà in base al tipo e allo stato della prenotazione della capacità.

I tipi di istanza disponibili variano in base alla regione. Per ulteriori informazioni, consulta Amazon EC2 instance types by Region.

Stato

- Per `DescribeInstanceTopology`: le istanze devono essere nello stato `running`.

- Per `DescribeCapacityReservationTopology`: le prenotazioni della capacità devono essere nello stato `pending` o `active`.

Non puoi ottenere informazioni sulla topologia delle istanze o delle prenotazioni della capacità in qualsiasi altro stato.

autorizzazioni IAM

L'identità IAM (utente, gruppo di utenti o ruolo) richiede le seguenti autorizzazioni:

- `ec2:DescribeInstanceTopology`
- `ec2:DescribeCapacityReservationTopology`

Esempi di topologia dell'istanza Amazon EC2

Puoi usare il comando describe-instance-topology per descrivere la topologia delle istanze EC2. Inoltre, puoi usare il comando describe-capacity-reservation-topology per descrivere la topologia delle prenotazioni della capacità.

Quando usi il comando `describe-instance-topology` o `describe-capacity-reservation-topology` senza parametri o filtri, la risposta includerà tutte le istanze o le prenotazioni della capacità (a seconda del comando utilizzato) che corrispondono ai tipi di istanza supportati per questo comando nella Regione specificata. È possibile specificare la Regione includendo il parametro `--region` o impostando una Regione predefinita. Per ulteriori informazioni sull'impostazione di una Regione predefinita, consulta Selezione di una regione per le risorse Amazon EC2.

Puoi includere parametri per restituire istanze o prenotazioni della capacità che corrispondono agli ID di istanza o prenotazione della capacità o ai nomi dei gruppi di posizionamento specificati. Puoi inoltre includere filtri per restituire istanze o prenotazioni della capacità che corrispondono a un tipo o a una famiglia di istanze specifici oppure istanze o prenotazioni della capacità in una zona di disponibilità o una zona locale specificata. È possibile includere un singolo parametro o filtro o una combinazione di parametri e filtri.

L'output è impaginato, con un massimo di 20 istanze o prenotazioni della capacità per pagina per impostazione predefinita. Puoi specificare fino a 100 istanze o prenotazioni della capacità per pagina utilizzando il parametro `--max-results`.

Per ulteriori informazioni, consulta describe-instance-topology e describe-reservation-topology-topology.

Autorizzazioni richieste

Sono richieste le seguenti autorizzazioni:

- `ec2:DescribeInstanceTopology`: per descrivere la topologia dell'istanza.
- `ec2:DescribeCapacityReservationTopology`: per descrivere la topologia della prenotazione della capacità.

Esempi

- Esempio 1: DescribeInstanceTopology - ID delle istanze
- Esempio 2: DescribeInstanceTopology - Parametro del nome del gruppo di collocamento
- Esempio 3: DescribeInstanceTopology - Filtro del tipo di istanza
  - Esempio 3a: filtro a corrispondenza esatta per un tipo di istanza specificato
  - Esempio 3b: filtro Wild card per una famiglia di istanze
  - Esempio 3c — Famiglia di istanze combinata e filtri a corrispondenza esatta
- Esempio 4: DescribeInstanceTopology - Filtro Zone ID
  - Esempio 4a — Filtro della zona di disponibilità
  - Esempio 4b — Filtro della zona locale
  - Esempio 4c: filtri combinati per la zona di disponibilità e la zona locale
- Esempio 5: DescribeInstanceTopology - Filtri per tipo di istanza e ID di zona
- Esempio 6: DescribeCapacityReservationTopology - ID di prenotazione della capacità
- Esempio 7: DescribeCapacityReservationTopology - Filtro del tipo di istanza

Esempio 1: DescribeInstanceTopology - ID delle istanze

AWS CLI

Per descrivere la topologia di istanze specifiche

Usa il comando describe-instance-topology con il parametro `--instance-ids`. L'output include solo le istanze che corrispondono agli ID istanza specificati.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --instance-ids i-1111111111example i-2222222222example
```

Di seguito è riportato un output di esempio.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Per descrivere la topologia di istanze specifiche

Utilizza il cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -InstanceId i-1111111111example, i-2222222222example
```

Esempio 2: DescribeInstanceTopology - Parametro del nome del gruppo di collocamento

AWS CLI

Per descrivere la topologia delle istanze in un gruppo di posizionamento specifico

Usa il comando describe-instance-topology con il parametro `group-names`. L'output include solo le istanze presenti in uno dei due gruppi di posizionamento specificati.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --group-names ML-group HPC-group
```

Di seguito è riportato un output di esempio.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
```

```
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Per descrivere la topologia delle istanze in un gruppo di posizionamento specifico

Utilizza il cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -GroupName ML-group, HPC-group
```

Esempio 3: DescribeInstanceTopology - Filtro del tipo di istanza

È possibile filtrare in base a un tipo di istanza specificato (corrispondenza esatta) o a una famiglia di istanze (utilizzando un carattere jolly). È inoltre possibile combinare un filtro per tipo di istanza specificato e un filtro per una famiglia di istanze.

Esempio 3a: filtro a corrispondenza esatta per un tipo di istanza specificato

AWS CLI

Per descrivere la topologia di istanze con un tipo di istanza specifico

Usa il comando describe-instance-topology con il filtro `instance-type`. L'output include solo le istanze con il tipo di istanza specificato.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1n.32xlarge
```

Di seguito è riportato un output di esempio.

```
{
```

```
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Per descrivere la topologia di istanze con un tipo di istanza specifico

Utilizza il cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="trn1n.32xlarge"}
```

Esempio 3b: filtro Wild card per una famiglia di istanze

AWS CLI

Per descrivere la topologia di istanze con una famiglia di istanze specifica

Usa il comando describe-instance-topology con il filtro `instance-type`. L'output include solo le istanze con la famiglia di istanze specificata.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1*
```

Di seguito è riportato un output di esempio.

```
{
```

```
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```


PowerShell

Per descrivere la topologia di istanze con una famiglia di istanze specifica

Utilizza il cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="trn1*"}
```

Esempio 3c — Famiglia di istanze combinata e filtri a corrispondenza esatta

AWS CLI

Per descrivere la topologia di istanze con una famiglia di istanze o un tipo di istanza

Usa il comando describe-instance-topology con il filtro `instance-type`. L'output include solo le istanze che soddisfano i criteri specificati.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge"
```

Di seguito è riportato un output di esempio.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
```

```
                "nn-4343434343example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Per descrivere la topologia di istanze con una famiglia di istanze o un tipo di istanza

Utilizza il cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="p4d*", "trn1n.32xlarge"}
```

Esempio 4: DescribeInstanceTopology - Filtro Zone ID

È possibile utilizzare il filtro `zone-id` per filtrare in base a una zona di disponibilità o una zona locale. È inoltre possibile combinare un filtro per la zona di disponibilità e un filtro per la zona locale.

Esempio 4a — Filtro della zona di disponibilità

AWS CLI

Per descrivere la topologia di istanze in una zona di disponibilità specifica

Usa il comando describe-instance-topology con il filtro `zone-id`. L'output include solo le istanze nella zona di disponibilità specificata.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1
```

Di seguito è riportato un output di esempio.

```
{
    "Instances": [
```

```
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Per descrivere la topologia di istanze in una zona di disponibilità specifica

Utilizza il cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="zone-id"; Values="use1-az1"}
```

Esempio 4b — Filtro della zona locale

AWS CLI

Per descrivere la topologia di istanze in una zona locale specifica

Usa il comando describe-instance-topology con il filtro `zone-id`. L'output include solo le istanze nella zona locale specificata.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-atl2-az1
```

Di seguito è riportato un output di esempio.

```
{
    "Instances": [
```

```
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Per descrivere la topologia di istanze in una zona locale specifica

Utilizza il cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="zone-id"; Values="use1-atl2-az1"}
```

Esempio 4c: filtri combinati per la zona di disponibilità e la zona locale

AWS CLI

Per descrivere la topologia di istanze in una zona specifica

Usa il comando describe-instance-topology con il filtro `zone-id`. L'output include solo le istanze in una delle due zone specificate.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1,use1-atl2-az1
```

Di seguito è riportato un output di esempio.

```
{
```

```
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Per descrivere la topologia di istanze in una zona specifica

Utilizza il cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="zone-id"; Values="use1-az1", "use1-atl2-az1"}
```

Esempio 5: DescribeInstanceTopology - Filtri per tipo di istanza e ID di zona

Puoi combinare i filtri in un singolo comando.

AWS CLI

Per descrivere la topologia di istanze con tipi di istanza, famiglie di istanze e zone specifici

Usa il comando describe-instance-topology con i filtri `instance-type` e `zone-id`. La risposta contiene tutte le istanze con uno dei due tipi di istanza specificati e in una delle due zone specificate.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge" \
              "Name=zone-id,Values=use1-az1,use1-atl2-az1"
```

Di seguito è riportato un output di esempio.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
```

```
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Per descrivere la topologia di istanze con tipi di istanza, famiglie di istanze e zone specifici

Utilizza il cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="p4d*", "trn1n.32xlarge"} `
            @{Name="zone-id"; Values="use1-az1", "use1-atl2-az1"}
```

Esempio 6: DescribeCapacityReservationTopology - ID di prenotazione della capacità

AWS CLI

Per descrivere la topologia di prenotazioni della capacità specifiche

Usa il comando describe-capacity-reservation-topology con il parametro `capacity-reservation-id`. L'output include solo le prenotazioni della capacità che corrispondono agli ID prenotazione della capacità specificati.

```
aws ec2 describe-capacity-reservation-topology \
    --region us-east-1 \
    --capacity-reservation-id cr-1111111111example cr-2222222222example
```

Di seguito è riportato un output di esempio.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1111111111example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p5.48xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example"
            ],
            "AvailabilityZone": "us-east-1a"
```

```
        },
        {
            "CapacityReservationId": "cr-2222222222example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p5en.48xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example"
            ],
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Per descrivere la topologia di prenotazioni della capacità specifiche

Utilizza il cmdlet Get-EC2CapacityReservationTopology.

```
Get-EC2CapacityReservationTopology `
    -CapacityReservationId cr-1111111111example cr-2222222222example
```

Esempio 7: DescribeCapacityReservationTopology - Filtro del tipo di istanza

È possibile filtrare in base a un tipo di istanza specificato (corrispondenza esatta) o a una famiglia di istanze (utilizzando un carattere jolly). È inoltre possibile combinare un filtro per tipo di istanza specificato e un filtro per una famiglia di istanze.

AWS CLI

Per descrivere la topologia di prenotazioni della capacità con un tipo di istanza specifico

Usa il comando describe-capacity-reservation-topology con il filtro `instance-type`. La risposta contiene tutte le istanze con il tipo di istanza specificato.

```
aws ec2 describe-capacity-reservation-topology \
    --region us-east-1 \
    --filters Name=instance-type,Values=p5en.48xlarge
```

Di seguito è riportato un output di esempio.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-2222222222example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p5en.48xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example"
            ],
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

Per descrivere la topologia di prenotazioni della capacità con un tipo di istanza specifico

Utilizza il cmdlet Get-EC2CapacityReservationTopology.

```
Get-EC2CapacityReservationTopology `
    -Filter @{Name="instance-type"; Values="p5en.48xlarge"}
```

Gruppi di collocamento per le tue istanze Amazon EC2

Per soddisfare le esigenze del tuo carico di lavoro, puoi avviare un gruppo di istanze EC2 interdipendenti in un gruppo di collocamento per influire sul collocamento.

A seconda del tipo di carico di lavoro, puoi creare un gruppo di collocamento con una delle strategie seguenti:

- Cluster: raggruppa le istanze in una zona di disponibilità. Questa strategia consente ai carichi di lavoro di raggiungere le prestazioni di rete a bassa latenza necessarie per una comunicazione strettamente accoppiata da nodo a nodo, tipica delle applicazioni HPC (High Performance Computing).

- Partizione: distribuisce le istanze su partizioni logiche in modo che gruppi di istanze in una partizione non condividano l'hardware sottostante con gruppi di istanze in partizioni diverse. Questa strategia di solito viene utilizzata in grandi carichi di lavoro distribuiti e replicati, come Hadoop, Cassandra e Kafka.
- Distribuzione: distribuisce un piccolo gruppo di istanze in uno specifico hardware sottostante per ridurre gli errori correlati.
- Tempo di precisione: colloca le istanze sull'hardware supportato con accesso diretto a sorgenti temporali ad alta precisione nell'infrastruttura. AWS

I gruppi di collocamento sono facoltativi. Se non avvii le istanze in un gruppo di collocamento, EC2 prova a posizionarle in modo che tutte le istanze siano distribuite in tutto l'hardware sottostante, così da ridurre al minimo gli errori correlati.

Prezzi

La creazione dei gruppi di collocamento non prevede l'applicazione di costi.

Regole e limitazioni

Prima di utilizzare i gruppi di collocamento, tieni presente le regole seguenti:

- Puoi collocare un'istanza in un gruppo di collocamento alla volta; l'istanza non può essere presente in più gruppi di collocamento.
- Non è possibile unire i gruppi di collocamento.
- On-Demand Le prenotazioni di capacità e le istanze riservate zonali consentono di riservare la capacità per le istanze EC2 nelle zone di disponibilità. Quando si avvia un'istanza, se gli attributi dell'istanza corrispondono a quelli specificati da una prenotazione di On-Demand capacità o da un'istanza riservata zonale, la capacità riservata viene utilizzata automaticamente dall'istanza. Questo vale anche se avvii l'istanza in un gruppo di collocamento.
- Non puoi eseguire l'avvio di host dedicati nei gruppi di posizionamento.
- Non puoi avviare un'istanza spot configurata per l'arresto o l'ibernazione in caso di interruzione in un gruppo di posizionamento.

Indice

- Strategie di posizionamento per i vostri gruppi di collocamento
- Crea un gruppo di collocamento per le tue istanze EC2

- Modifica del collocamento per un'istanza EC2
- Eliminazione di un gruppo di collocamento
- Gruppi di posizionamento condivisi
- Gruppi di collocamento attivi AWS Outposts

Strategie di posizionamento per i vostri gruppi di collocamento

È possibile creare un gruppo di posizionamento per le tue istanze EC2 utilizzando una delle seguenti strategie.

Strategie di posizionamento

- Gruppi di collocazione cluster
- Gruppi di collocamento di partizione
- Gruppi di collocazione sparsi
- Gruppi di collocamento cronologico di precisione

Gruppi di collocazione cluster

Un gruppo di collocazione cluster è un raggruppamento logico di istanze all'interno di una singola zona di disponibilità. Le istanze non sono isolate in un singolo rack. Un gruppo di posizionamento cluster può comprendere reti private virtuali (VPC) collegate in peering che si trovano nella stessa Regione. Le istanze appartenenti allo stesso gruppo di posizionamento del cluster godono di un limite di throughput per flusso più elevato per TCP/IP flusso e sono collocate nello stesso segmento di larghezza di banda ad alta bisezione della rete.

La seguente immagine mostra istanze collocate in un gruppo di collocazione cluster.



I gruppi di posizionamento cluster sono consigliati per le applicazioni a bassa latenza di rete, throughput di rete elevata o entrambe. Sono consigliati anche quando la maggior parte del traffico di rete si trova tra le istanze del gruppo. Per ottenere la latenza più bassa e le prestazioni di rete a livello di pacchetto al secondo più elevate per il gruppo di collocamento, scegli un tipo di istanza in grado di supportare le reti avanzate. Per ulteriori informazioni, consulta la sezione relativa alle reti avanzate.

Puoi assicurarti che le istanze avviate in un gruppo di posizionamento del cluster vengano collocate su hardware con funzionalità di precisione temporale specificando un gruppo di posizionamento temporale di precisione principale quando crei il gruppo di posizionamento del cluster. Utilizza il `--parent-group-id` parametro quando crei il gruppo di posizionamento del cluster per stabilire questa relazione.

Si consiglia di avviare le istanze nel modo seguente:

- Utilizzare una singola richiesta di avvio per avviare il numero di istanze necessarie nel gruppo di posizionamento.
- Utilizzare lo stesso tipo di istanza per tutte le istanze del gruppo di posizionamento.

Se provi ad aggiungere altre istanze al gruppo di collocamento in un secondo momento o se provi ad avviare più di un tipo di istanza nel gruppo di collocamento, avrai più possibilità di ricevere un errore di capacità non sufficiente.

Se arresti un'istanza in un gruppo di collocamento e poi la riavvii, quest'ultima continua a essere eseguita nel gruppo di collocamento. Tuttavia, l'avvio non riesce se non è presente capacità sufficiente per l'istanza.

Se ricevi un errore di capacità durante l'avvio di un'istanza in un gruppo di collocamento nel quale sono già in esecuzione delle istanze, arresta e avvia tutte le istanze del gruppo di collocamento e prova a ripetere l'accesso. L'avvio delle istanze potrebbe migrarle su un hardware con capacità per tutte le istanze richieste.

Regole e limitazioni

Ai gruppi di collocazione cluster si applicano le regole seguenti:

- Sono supportati i seguenti tipi di istanza:
  - Istanze di generazione attuale, ad eccezione delle istanze a prestazioni ??? prolungate (ad esempio, T2), delle istanze Mac1 e delle istanze. ??? M7i-flex
  - Le seguenti istanze di generazione precedente: A1, C3, C4, I2, M4, R3 ed R4.

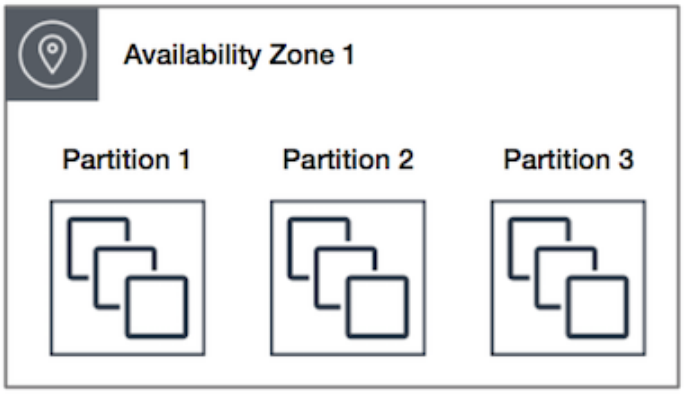
- Un gruppo di collocazione cluster non può estendersi in più zone di disponibilità.
- Il throughput massimo di rete del traffico tra due istanze di un gruppo di posizionamento cluster è limitata dall'istanza più lenta tra le due. Per le applicazioni con requisiti di throughput elevato, scegli un tipo di istanza con connettività di rete in grado di soddisfare i tuoi requisiti.
- Per i tipi di istanza abilitati per le reti avanzate, si applicano le seguenti regole:
  - Le istanze all'interno di un gruppo di collocazione cluster possono utilizzare fino a 10 Gbps per il traffico a flusso singolo. Le istanze che non si trovano all'interno di un gruppo di collocazione cluster possono utilizzare fino a 5 Gbps per il traffico di un flusso singolo.
  - Il traffico verso e dai bucket Amazon S3 all'interno della stessa regione sullo spazio dell'indirizzo IP pubblico o tramite un endpoint VPC può utilizzare tutta la larghezza di banda aggregata dell'istanza disponibile.
- Puoi avviare più tipi di istanza in un gruppo di collocazione cluster. Tuttavia, ciò riduce le probabilità che la capacità necessaria sia disponibile per garantire la riuscita dell'avvio. Consigliamo di utilizzare lo stesso tipo di istanza per tutte le istanze in un gruppo di collocazione cluster.
- Ti consigliamo di riservare la capacità in modo esplicito nel gruppo di posizionamento del cluster creando una On-Demand prenotazione di capacità nel gruppo di posizionamento del cluster. Tieni presente che non puoi riservare la capacità utilizzando le istanze riservate zonali, poiché non possono riservare la capacità in modo esplicito in un gruppo di collocamento.
- I Capacity Block non supportano i gruppi di collocamento. Per ulteriori informazioni, consulta Blocchi di capacità per ML.
- Il traffico di rete verso Internet e tramite una Direct Connect connessione a risorse locali è limitato a 5 Gbps per i gruppi di posizionamento dei cluster.

Gruppi di collocamento di partizione

I gruppi di collocamento di partizione contribuiscono a ridurre le probabilità di errori correlati all'hardware per l'applicazione. Quando si utilizzano gruppi di collocamento di partizione, Amazon EC2 divide ogni gruppo in segmenti logici denominati partizioni. Amazon EC2 assicura che ogni partizione nell'ambito di un gruppo di collocamento abbia un proprio set di rack. Ciascun rack dispone di rete e alimentazione proprie. Due partizioni nell'ambito di un gruppo di collocazione non possono condividere gli stessi rack, consentendoti di isolare l'impatto degli errori hardware all'interno della tua applicazione.

L'immagine seguente è una semplice rappresentazione visiva di un gruppo di collocazione di una partizione in una singola zona di disponibilità. Mostra istanze collocate in un gruppo di collocamento

con tre partizioni—Partition 1 (Partizione 1), Partition 2 (Partizione 2) e Partition 3 (Partizione 3). Ogni partizione include più istanze. Le istanze di una partizione non condividono i rack con le istanze di altre partizioni, limitando così l'impatto di un singolo errore hardware alla sola partizione associata.



I gruppi di collocamento di partizione possono essere impiegati per distribuire carichi di lavoro ampiamente diffusi e replicati come HDFS, HBase e Cassandra su rack diversi. Quando si avviano istanze in un gruppo di collocamento di partizione, Amazon EC2 tenta di distribuirle in modo omogeneo nel numero di partizioni specificato. È inoltre possibile avviare le istanze in una partizione specifica per avere maggior controllo sulla destinazione delle istanze.

Un gruppo di collocamento di partizione può avere partizioni in più zone di disponibilità della stessa regione. Un gruppo di collocamento di partizione può avere al massimo sette partizioni per zona di disponibilità. Il numero di istanze avviabili in un gruppo di collocamento di partizione è limitato solo dalle restrizioni vigenti nel proprio account.

Inoltre, i gruppi di posizionamento delle partizioni offrono visibilità sulle partizioni: puoi vedere quali istanze si trovano in quali partizioni. Puoi condividere queste informazioni con applicazioni che supportano la topologia, come HDFS, HBase e Cassandra. Questa applicazioni utilizzano queste informazioni per prendere decisioni intelligenti sulla replica dei dati per aumentare la disponibilità e la durabilità dei dati.

Se si avvia un'istanza in un gruppo di collocamento di partizione e l'hardware univoco è insufficiente per l'esecuzione della richiesta, quest'ultima produce un errore. Amazon EC2 rende disponibile ulteriore hardware separato nel tempo, per consentire di riprovare a effettuare la richiesta in un secondo momento.

Regole e limitazioni

Ai gruppi di collocamento di partizione si applicano le regole seguenti:

- Un gruppo di collocamento di partizione supporta al massimo sette partizioni per zona di disponibilità. Il numero di istanze avviabili in un gruppo di collocamento di partizione pe limitato solo dalle restrizioni vigenti nel proprio account.
- Quando si avviano istanze in un gruppo di collocamento di partizione, Amazon EC2 tenta di distribuirle in modo omogeneo in tutte le partizioni. Amazon EC2 non garantisce una distribuzione omogenea delle istanze in tutte le partizioni.
- Un gruppo di collocamento di partizione con Istanze dedicate può avere al massimo due partizioni.
- Le prenotazioni della capacità non riservano capacità in un gruppo di collocamento di partizione.

Gruppi di collocazione sparsi

Un gruppo di posizionamento sparso è un gruppo di istanze, ognuna delle quali collocata su un hardware distinto.

I gruppi di collocamento sparsa sono consigliati per le applicazioni con un numero ridotto di istanze critiche che è necessario tenere separate. L'avvio delle istanze in un gruppo di collocazione sparso riduce il rischio di errori simultanei che possono verificarsi quando le istanze condividono la stessa apparecchiatura. I gruppi di posizionamento distribuito forniscono l'accesso a hardware distinti e sono quindi adatti per mescolare tipi di istanze o avviare istanze nel tempo.

Se si avvia un'istanza in un gruppo di collocamento sparso e l'hardware univoco è insufficiente per l'esecuzione della richiesta, quest'ultima produce un errore. Amazon EC2 rende disponibile ulteriore hardware separato nel tempo, per consentire di riprovare a effettuare la richiesta in un secondo momento.

I gruppi di posizionamento distribuito possono distribuire le istanze tra rack o host. Per ulteriori informazioni, consulta the section called “Gruppi di collocamento attivi AWS Outposts”.

L'immagine seguente mostra sette istanze in un gruppo di posizionamento distribuito in una singola zona di disponibilità. Ogni istanza è posizionata su un rack diverso, in cui ogni rack dispone di una propria rete e di una propria fonte di alimentazione.



Regole e limitazioni

Ai gruppi di collocamento sparsa si applicano le regole seguenti:

- Rack-level i gruppi di collocamento diffuso sono supportati nelle AWS Regioni e in altre aree AWS Outposts.
- Host-level i gruppi di spread placement sono supportati solo su AWS Outposts.
- Un gruppo di posizionamento distribuito a livello di rack può estendersi su più zone di disponibilità nella stessa regione, ma supporta un massimo di sette istanze in esecuzione in ciascuna zona di disponibilità.

  Ad esempio, in una regione con tre zone di disponibilità, puoi eseguire un totale di 21 istanze in un gruppo di collocamento distribuito, con sette istanze in ciascuna zona di disponibilità. Se provi ad avviare un'ottava istanza in una zona di disponibilità che ha già sette istanze, l'istanza non viene avviata.

  Se occorrono più di 7 istanze in una zona di disponibilità, è preferibile utilizzare più gruppi di posizionamento sparso. L'utilizzo di più gruppi di distribuzione distribuita non garantisce che le istanze siano distribuite tra i gruppi, ma garantisce che siano distribuite all'interno di ciascun gruppo, il che limita l'impatto di determinate classi di errori.
- Sì AWS Outposts, un gruppo di spread placement a livello di rack può contenere tante istanze quanti sono i rack presenti nella distribuzione Outpost, mentre un gruppo di spread placement a livello di host può contenere tante istanze quanti sono gli host.
- I gruppi di collocazione sparsa non sono supportati per le Istanze dedicate.
- Le prenotazioni della capacità non riservano capacità in un gruppo di collocamento sparso.

Gruppi di collocamento cronologico di precisione

Un gruppo di collocazione temporale di precisione colloca le istanze sull'hardware supportato con accesso diretto alle sorgenti temporali ad alta precisione nell' AWS infrastruttura. Le istanze avviate in un gruppo di collocazione temporale di precisione possono accedere al servizio avanzato Amazon Time Sync, che fornisce sorgenti di ora locale con maggiore precisione rispetto all'endpoint NTP locale standard disponibile per tutte le istanze Amazon EC2.

I gruppi di collocamento temporale di precisione sono consigliati per le applicazioni che richiedono una sincronizzazione dell'orologio accurata al microsecondo, come i database distribuiti che richiedono l'ordinamento e la coerenza delle transazioni, i servizi finanziari che richiedono una

marcatura temporale precisa e i sistemi distribuiti che ordinano gli eventi utilizzando letture dell'orologio locale.

Le istanze di un gruppo di collocazione temporale di precisione traggono vantaggio da quanto segue:

- Un'origine temporale NTP locale migliorata con maggiore precisione, disponibile per tutti i sistemi operativi supportati senza configurazione aggiuntiva.
- Accesso a un dispositivo PTP Hardware Clock (PHC) per una sincronizzazione accurata al microsecondo (solo istanze Linux).
- Timestamping dei pacchetti hardware per misurazioni di rete con risoluzione in nanosecondi (solo istanze Linux).

Per informazioni sulla configurazione dell'istanza per l'utilizzo delle sorgenti temporali avanzate, consulta. Configurazione del rifermento temporale sull'istanza EC2 per l'utilizzo del servizio di sincronizzazione oraria di Amazon locale

Le seguenti regole si applicano ai gruppi di collocamento temporale di precisione:

Regole e limitazioni

- Per l'elenco attuale delle famiglie di istanze supportate, consultaConfigurazione del rifermento temporale sull'istanza EC2 per l'utilizzo del servizio di sincronizzazione oraria di Amazon locale.
- Se avvii o avvii un'istanza in un gruppo di collocamento temporale di precisione e l'hardware non è sufficiente per fornire l'accesso al servizio avanzato Amazon Time Sync Service, la richiesta ha esito negativo. Riprova più tardi o prova un'altra zona di disponibilità.
- Non è possibile eliminare un gruppo di collocamento temporale di precisione che è padre di un gruppo di posizionamento del cluster.
- Non è previsto alcun costo aggiuntivo per l'utilizzo dei gruppi di posizionamento temporale di precisione.

Crea un gruppo di collocamento per le tue istanze EC2

Puoi utilizzare un gruppo di posizionamento per controllare il posizionamento delle istanze tra loro. Dopo aver creato un gruppo di posizionamento, puoi avviare istanze all'interno del gruppo.

Limitazione

In ogni Regione puoi creare un massimo di 500 gruppi di posizionamento.

Console

Come creare un gruppo di posizionamento

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Placement Groups (Gruppi di collocamento).
3. Scegli Crea gruppo di collocamento.
4. Per Nome, specificate un nome per il gruppo.
5. Per Strategia di posizionamento, scegli la strategia di posizionamento per il gruppo: Cluster, Spread, Partition o Precision time.
   a. Se hai scelto Spread, per il livello Spread, scegli Host o Rack.
   b. Se hai scelto Partizione, in Numero di partizioni, inserisci il numero di partizioni per il gruppo.
   c. Se hai scelto Cluster, puoi facoltativamente specificare un gruppo di posizionamento temporale di precisione principale per garantire che le istanze del gruppo di posizionamento del cluster vengano avviate su hardware compatibile con il tempo di precisione.
6. (Facoltativo) Per aggiungere un tag, in Tag, scegli Aggiungi nuovo tag, quindi inserisci una chiave e un valore.
7. Seleziona Crea gruppo.

AWS CLI

Utilizzare il comando create-placement-group.

Per creare un gruppo di posizionamento cluster

Nell'esempio seguente viene creato un gruppo di collocazione che utilizza la strategia di collocazione `cluster` e viene applicato un tag con una chiave `purpose` e un valore pari a `production`.

```
aws ec2 create-placement-group \
    --group-name my-cluster \
    --strategy cluster \
    --tag-specifications 'ResourceType=placement-
group,Tags={Key=purpose,Value=production}'
```

Per creare un gruppo di posizionamento del cluster con un gruppo di collocamento temporale di precisione principale

L'esempio seguente crea un gruppo di posizionamento del cluster che specifica un gruppo di posizionamento temporale di precisione principale utilizzando il `--parent-group-id` parametro.

```
aws ec2 create-placement-group \
    --group-name my-cluster \
    --strategy cluster \
    --parent-group-id pg-0aaa1111111111111
```

Per creare un gruppo di posizionamento delle partizioni

Nell'esempio seguente viene creato un gruppo di collocamento che utilizza la strategia di collocamento `partition` e vengono specificate le cinque partizioni utilizzando il parametro `--partition-count`.

```
aws ec2 create-placement-group \
    --group-name HDFS-Group-A \
    --strategy partition \
    --partition-count 5
```

Per creare un gruppo di posizionamento temporale di precisione

L'esempio seguente crea un gruppo di collocamento che utilizza la strategia di `precision-time` posizionamento.

```
aws ec2 create-placement-group \
    --group-name my-precision-time-pg \
    --strategy precision-time
```

PowerShell

Utilizza il cmdlet New-EC2PlacementGroup.

Per creare un gruppo di posizionamento cluster

Il seguente esempio crea un gruppo di posizionamento cluster.

```
New-EC2PlacementGroup `
```

```
    -GroupName my-placement-group `
    -Strategy cluster
```

Per creare un gruppo di posizionamento del cluster con un gruppo di collocamento temporale di precisione principale

L'esempio seguente crea un gruppo di posizionamento del cluster che specifica un gruppo di posizionamento temporale di precisione principale utilizzando il `-ParentGroupId` parametro.

```
New-EC2PlacementGroup `
    -GroupName my-placement-group `
    -Strategy cluster `
    -ParentGroupId pg-0aaa1111111111111
```

Come creare un gruppo di posizionamento delle partizioni

Il seguente esempio crea un gruppo di posizionamento delle partizioni.

```
New-EC2PlacementGroup `
    -GroupName my-placement-group `
    -Strategy partition `
    -PartitionCount 5
```

Per creare un gruppo di posizionamento temporale di precisione

L'esempio seguente crea un gruppo di posizionamento temporale di precisione.

```
New-EC2PlacementGroup `
    -GroupName my-precision-time-pg `
    -Strategy precision-time
```

Modifica del collocamento per un'istanza EC2

È possibile modificare il gruppo di collocamento per un'istanza in questo modo:

- Aggiungere un'istanza in un gruppo di collocamento
- Spostare un'istanza da un gruppo di posizionamento a un altro
- Rimuovere un'istanza da un gruppo di posizionamento

Requisito

Prima di poter modificare il gruppo di posizionamento di un'istanza, questa deve trovarsi nello stato `stopped`.

Console

Per modificare il posizionamento dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Seleziona Actions (Operazioni), Instance settings (Impostazioni istanza), Modify instance placement (Modifica posizionamento delle istanze).
5. Per il Gruppo collocamento, effettua una delle seguenti operazioni:
   - Per aggiungere l'istanza a un gruppo di collocamento, seleziona il gruppo di collocamento.
   - Per spostare l'istanza da un gruppo di collocamento a un altro, seleziona il gruppo di collocamento.
   - Per rimuovere l'istanza dal gruppo di collocamento, scegli Nessuno.
6. Selezionare Salva.

AWS CLI

Per spostare un'istanza in un gruppo di collocamento

Usa il seguente comando modify-instance-placement.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name MySpreadGroup
```

Per rimuovere un'istanza da un gruppo di posizionamento

Usa il seguente comando modify-instance-placement. Quando specifichi una stringa vuota come nome del gruppo di posizionamento, questa operazione rimuove l'istanza dal suo attuale gruppo.

```
aws ec2 modify-instance-placement \
```

```
    --instance-id i-0123a456700123456 \
    --group-name ""
```

PowerShell

Per spostare un'istanza in un gruppo di collocamento

Utilizzare il Edit-EC2InstancePlacement cmdlet con il nome del gruppo di collocamento.

```
Edit-EC2InstancePlacement `
    -InstanceId i-0123a456700123456 `
    -GroupName MySpreadGroup
```

Per rimuovere un'istanza da un gruppo di posizionamento

Utilizzare il Edit-EC2InstancePlacement cmdlet con una stringa vuota per il nome del gruppo di collocamento.

```
Edit-EC2InstancePlacement `
    -InstanceId i-0123a456700123456 `
    -GroupName ""
```

Eliminazione di un gruppo di collocamento

Puoi eliminare un gruppo di collocamento se devi sostituirlo o se non ti serve più. Prima di poter eliminare un gruppo di posizionamento, non deve contenere istanze. Puoi terminare le istanze, spostarle in un altro gruppo di collocamento oppure eliminarle dal gruppo di collocamento.

Non è possibile eliminare un gruppo di collocamento che è padre di un gruppo di collocamento del cluster. Elimina prima i gruppi di posizionamento del cluster.

Console

Come eliminare un gruppo di posizionamento

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Placement Groups (Gruppi di collocamento).
3. Selezionare il gruppo di collocamento e scegliere Actions (Operazioni, Delete (Elimina).
4. Quando viene richiesta la conferma, immettere **Delete** e quindi scegliere Elimina.

AWS CLI

Come eliminare un gruppo di posizionamento

Usa il comando delete-placement-group.

```
aws ec2 delete-placement-group --group-name my-cluster
```

PowerShell

Come eliminare un gruppo di posizionamento

Utilizza il cmdlet Remove-EC2PlacementGroup.

```
Remove-EC2PlacementGroup -GroupName my-cluster
```

Gruppi di posizionamento condivisi

La condivisione dei gruppi di posizionamento consente di influenzare il posizionamento di istanze interdipendenti di proprietà di Account AWS separati. Un proprietario può condividere un gruppo di collocamento tra più persone Account AWS o all'interno della propria organizzazione. Un partecipante può avviare istanze in un gruppo di posizionamento condiviso con il proprio account.

Il proprietario di un gruppo di posizionamento può condividere un gruppo di posizionamento con:

- Specifico Account AWS all'interno o all'esterno della sua organizzazione
- Un'unità organizzativa all'interno dell'organizzazione
- L'intera organizzazione

Puoi utilizzare il peering VPC per connettere istanze di proprietà separate Account AWS e ottenere tutti i vantaggi in termini di latenza offerti dai gruppi di collocamento dei cluster condivisi.

Indice

- Regole e limitazioni
- Autorizzazioni richieste
- Condivisione tra le zone di disponibilità
- Condivisione gruppo di collocamento

- Annullamento della condivisione del gruppo di

Regole e limitazioni

Le seguenti regole e limitazioni si applicano quando condividi un gruppo di posizionamento o quando un gruppo di posizionamento viene condiviso con te.

- Per condividere un gruppo di collocamento, devi possederlo nel tuo. Account AWS Non puoi condividere un gruppo di posizionamento che è stato condiviso con te.
- Quando si condivide una partizione o un gruppo di posizionamento degli spread, i limiti del gruppo di posizionamento non cambiano. Un gruppo di posizionamento delle partizioni condiviso supporta al massimo sette partizioni per zona di disponibilità, mentre un gruppo di posizionamento degli spread supporta un massimo di sette istanze in esecuzione per zona di disponibilità.
- Per condividere un gruppo di posizionamento con la tua organizzazione Wo un'unità organizzativa nella tua organizzazione , devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta la pagina Condivisione delle risorse AWS.
- Quando utilizzi il Console di gestione AWS per avviare un'istanza, puoi selezionare tutti i gruppi di collocamento che sono stati condivisi con te. Quando si utilizza il AWS CLI per avviare un'istanza, è necessario specificare un gruppo di collocamento condiviso per ID, non per nome. Puoi utilizzare il nome del gruppo di posizionamento solo se sei il proprietario del gruppo di posizionamento condiviso.
- La gestione delle istanze di tua proprietà in un gruppo di posizionamento condiviso è una tua responsabilità.
- Non è possibile visualizzare o modificare le istanze e le prenotazioni della capacità associate a un gruppo di posizionamento condiviso con te ma non di tua proprietà.
- Il nome della risorsa Amazon (ARN) di un gruppo di posizionamento contiene l'ID dell'account proprietario del gruppo di posizionamento. Puoi utilizzare la parte relativa all'ID account dell'ARN di un gruppo di collocamento per identificare il proprietario di un gruppo di collocamento condiviso con te.

Autorizzazioni richieste

Per condividere un gruppo di posizionamento, gli utenti devono disporre delle autorizzazioni per le seguenti azioni:

- `ec2:PutResourcePolicy`

- `ec2:DeleteResourcePolicy`

Condivisione tra le zone di disponibilità

Per garantire che le risorse vengano distribuite tra le zone di disponibilità di una regione, mappiamo in modo indipendente le zone di disponibilità ai nomi per ciascun account. Questo potrebbe comportare una diversa denominazione delle zone di disponibilità tra i diversi account. Ad esempio, la tua zona `us-east-1a` di disponibilità Account AWS potrebbe non avere la stessa sede `us-east-1a` di un'altra Account AWS.

Per specificare la posizione dell'Host dedicati relativamente ai tuoi account, devi utilizzare l'ID della zona di disponibilità. L'ID AZ è univoco ed è lo stesso identificatore di una zona di disponibilità per tutti gli account AWS . Ad esempio, `use1-az1` è un ID di zona di disponibilità per la regione `us-east-1` e identifica la stessa posizione in ogni account AWS . Per ulteriori informazioni, consulta AZ IDs.

Condivisione gruppo di collocamento

Per condividere un gruppo di posizionamento, devi aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una AWS RAM risorsa che ti consente di condividere le tue risorse tra loro Account AWS. Una condivisione di risorse specifica le risorse da condividere e i consumatori con cui sono condivise.

Se fai parte di un'organizzazione in AWS Organizations, la condivisione all'interno della tua organizzazione è abilitata e ai consumatori dell'organizzazione viene concesso l'accesso al gruppo di collocamento condiviso.

Se il gruppo di collocamento è condiviso con una persona Account AWS esterna all'organizzazione, il Account AWS proprietario riceve un invito a partecipare alla condivisione delle risorse. Potrà accedere al gruppo di posizionamento condiviso dopo aver accettato l'invito.

Puoi condividere un gruppo di collocamento Account AWS tramite Using AWS Resource Access Manager. Per ulteriori informazioni, consulta l'argomento relativo alla creazione di una condivisione di risorse nella Guida per l'utente di AWS RAM .

Annullamento della condivisione del gruppo di

Il proprietario del gruppo di posizionamento può annullare la condivisione di un gruppo di posizionamento condiviso in qualsiasi momento. Quando annulli la condivisione di un gruppo di posizionamento condiviso, le modifiche seguenti avranno effetto:

- Le persone Account AWS con cui è stato condiviso un gruppo di collocamento non sono più in grado di avviare istanze o riservare capacità.
- Tutte le istanze in esecuzione in un gruppo di collocamento condiviso vengono dissociate dal gruppo di collocamento, ma continuano a essere eseguite nel tuo. Account AWS
- Qualsiasi prenotazione di capacità in un gruppo di collocamento condiviso viene dissociata dal gruppo di collocamento, ma rimane a tua disposizione nel tuo. Account AWS

Per ulteriori informazioni, consulta Eliminazione di una condivisione di risorse nella Guida per l'utente AWS RAM .

Gruppi di collocamento attivi AWS Outposts

AWS Outposts è un servizio completamente gestito che estende l' AWS infrastruttura, i servizi, le API e gli strumenti alle sedi dei clienti. Fornendo l'accesso locale all'infrastruttura AWS gestita, AWS Outposts consente ai clienti di creare ed eseguire applicazioni in locale utilizzando le stesse interfacce di programmazione AWS delle regioni, utilizzando al contempo risorse di elaborazione e archiviazione locali per esigenze di latenza inferiore e di elaborazione locale dei dati.

Un Outpost è un pool di capacità di AWS elaborazione e archiviazione distribuito presso la sede del cliente. AWS opera, monitora e gestisce questa capacità come parte di una regione. AWS

Puoi creare gruppi di posizionamento su Outpost creati nel tuo account. In tal modo è possibile distribuire istanze sull'hardware sottostante su un outpost nel tuo sito. Puoi creare e utilizzare gruppo di posizionamento su outpost nella stessa maniera con cui crei e utilizzi gruppi di posizionamento in zone di disponibilità normali. Quando crei un gruppo di posizionamento con una strategia di diffusione su un outpost, puoi scegliere di distribuire le istanze del gruppo di posizionamento tra host o rack. La distribuzione delle istanze tra gli host consente di utilizzare una strategia di diffusione con un Outpost a rack singolo.

Considerazioni

- Un gruppo di spread placement a livello di rack può contenere tante istanze quanti sono i rack presenti nella distribuzione Outpost.
- Un gruppo di spread placement a livello di host può contenere tante istanze quanti sono gli host presenti nella distribuzione Outpost.

Prerequisito

Devi avere un Outpost installato presso il tuo sito. Per ulteriori informazioni, consulta Creazione di un Outpost e ordinazione della capacità Outpost nella Guida per l'utente di AWS Outposts .

Per utilizzare un gruppo di posizionamento su un outpost

1. Creare una sottorete nell'Outpost. Per ulteriori informazioni, consulta Creazione di una sottorete nella Guida per l'utente di AWS Outposts .
2. Crea un gruppo di posizionamento nella regione dell'outpost associata. Se crei un gruppo di collocamento con una strategia di spread, puoi scegliere uno spread a livello di host o di rack per determinare in che modo il gruppo distribuisce le istanze sull'hardware sottostante del tuo Outpost. Per ulteriori informazioni, consulta the section called "Creazione di un gruppo di collocamento".
3. Avvia un'istanza nel gruppo di posizionamento. Per Subnet (Sottorete) scegli la sottorete creata nel passaggio 1 e per Placement group name (Nome gruppo di posizionamento) seleziona il gruppo di posizionamento creato nel passaggio 2. Per ulteriori informazioni, consulta Avvio di un'istanza sull'Outpost nella Guida per l'utente di AWS Outposts .

Unità massima di trasmissione (MTU) di rete per istanza EC2

L'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto maggiore consentito trasferibile attraverso la connessione. Maggiore è la MTU di una connessione, maggiore è la quantità di dati trasferibili in un unico pacchetto. I pacchetti Ethernet sono costituiti dal pacchetto o dai dati effettivi che invii e le informazioni sul sovraccarico della rete circostante.

I frame Ethernet possono presentarsi in diversi formati; il formato più comune è il formato di frame standard Ethernet v2. Supporta 1500 MTU, ovvero la dimensione del pacchetto Ethernet maggiore supportata nella maggior parte di Internet. La MTU massima supportata per un'istanza dipende dal tipo di istanza.

Tutti i tipi di istanza EC2 supportano 1500 MTU.

Indice

- Frame jumbo (9001 MTU)
- Rilevamento della MTU del percorso
- Imposta la MTU per le istanze Amazon EC2
- Risoluzione dei problemi

Frame jumbo (9001 MTU)

Con i frame jumbo, puoi aumentare la dimensione di payload per pacchetto, incrementando quindi la percentuale del pacchetto che non suppone un sovraccarico dello stesso. Con i frame jumbo, è necessario un numero minore di pacchetti per inviare la stessa quantità di dati utilizzabili. Tuttavia, alcuni tipi di traffico sono soggetti ai seguenti limiti di payload massimo:

Limite MTU di 1.500 byte

- Traffico su un gateway Internet
- Traffico su connessioni VPN
- Traffico tra AWS le regioni, a meno che non venga utilizzato un gateway di transito

Limite MTU di 8.500 byte

- Traffico su una connessione di peering VPC tra regioni

Se i pacchetti superano il limite MTU, vengono frammentati o annullati se è impostato il flag `Don't Fragment` nell'intestazione IP.

I frame jumbo devono essere utilizzati con cautela per il traffico vincolato a Internet o qualsiasi traffico che esca da un VPC. I pacchetti vengono frammentati da sistemi intermedi, i quali rallentano tale traffico. Per utilizzare i frame jumbo all'interno di un VPC e non rallentare il traffico vincolato al di fuori del VPC, puoi configurare la dimensione della MTU in base alla route oppure puoi utilizzare più interfacce di rete elastica con diverse dimensioni dell'MTU e diverse route.

Per le istanze collocate in un gruppo di collocazione cluster, i frame jumbo aiutano a raggiungere il massimo throughput della rete possibile, per cui li consigliamo in questo caso. Per ulteriori informazioni, consulta Gruppi di collocamento per le tue istanze Amazon EC2.

È possibile utilizzare i frame jumbo per il traffico tra i VPC e le proprie reti on-premises su Direct Connect. Per ulteriori informazioni e per scoprire come verificare la funzionalità dei frame jumbo, consulta MTU for private virtual interfaces or transit virtual interfaces nella Guida per l'utente di Direct Connect .

Tutti i tipi di istanza della generazione corrente supportano i frame jumbo. I seguenti tipi di istanza della generazione precedente supportano i frame jumbo A1, C3, I2, M3 e R3.

Risorse correlate

- Per configurare gateway NAT, consulta Nozioni di base di Gateway NAT nella Guida per l'utente di Amazon VPC.
- Per i gateway di transito, consulta la pagina Unità massima di trasmissione nella Guida per l'utente di Amazon VPC Transit Gateway.
- Per le zone locali, consulta Considerazioni nella Guida per l'utente delle zone locali AWS .
- Per AWS Wavelength, vedere Unità di trasmissione massima nella Guida AWS Wavelength per l'utente.
- Per Outposts, consulta i requisiti massimi dell'unità di trasmissione di Service link nella Guida per l'utente AWS Outposts .

Rilevamento della MTU del percorso

Il rilevamento della MTU del percorso (PMTUD) è utilizzato per determinare la MTU del percorso tra due dispositivi. La MTU del percorso è la dimensione massima del pacchetto che è supportata nel percorso tra l'host di origine e quello ricevente. In presenza di una differenza della dimensione della MTU nella rete tra due host, PMTUD consente all'host ricevente di rispondere all'host di origine con un messaggio ICMP. Questo messaggio ICMP indica all'host di origine di utilizzare la dimensione della MTU più piccola sul percorso di rete per inviare nuovamente la richiesta. Senza questa negoziazione, può verificarsi la perdita del pacchetto perché la richiesta è troppo grande per l'host ricevente.

Per IPv4, se un host invia un pacchetto più grande della MTU dell'host ricevente o della MTU di un dispositivo lungo il percorso, l'host o il dispositivo ricevente rifiuta il pacchetto e restituisce il seguente messaggio ICMP: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipo 3, Codice 4). Questo indica all'host trasmittente di dividere il payload in più pacchetti più piccoli e quindi di trasmetterli di nuovo.

Il protocollo IPv6 non supporta la frammentazione nella rete. Se un host invia un pacchetto più grande della MTU dell'host ricevente o della MTU di un dispositivo lungo il percorso, l'host o il dispositivo ricevente elimina il pacchetto e restituisce il seguente messaggio ICMP: `ICMPv6 Packet Too Big (PTB)` (Tipo 2). Questo indica all'host trasmittente di dividere il payload in più pacchetti più piccoli e quindi di trasmetterli di nuovo.

Le connessioni effettuate tramite alcuni componenti, come i gateway NAT e i sistemi di bilanciamento del carico, sono monitorati automaticamente. Ciò significa che il monitoraggio dei gruppi di

sicurezza viene abilitato automaticamente per i tentativi di connessione in uscita. Se le connessioni vengono tracciate automaticamente o non vengono tracciate o se le regole del gruppo di sicurezza consentono il traffico ICMP in entrata, è possibile ricevere risposte PMTUD.

Tieni presente che il traffico ICMP può essere bloccato anche se è consentito a livello di gruppo di sicurezza, ad esempio se hai una voce della lista di controllo degli accessi alla rete che nega il traffico ICMP alla sottorete.

> **Important**
>
> Il rilevamento della MTU del percorso non garantisce che i frame jumbo non vengano interrotti da alcuni router. Un Internet gateway nel tuo VPC invia pacchetti fino a soli 1500 byte. Consigliamo pacchetti di 1500 MTU per il traffico Internet.

Per le regole MTU sui gateway NAT, consulta Unità massima di trasmissione (MTU) nella Guida per l'utente VPC di Amazon. Per le regole MTU sui gateway di transito, consulta Unità massima di trasmissione (MTU) nella Guida per l'utente sui gateway di transito AWS .

Imposta la MTU per le istanze Amazon EC2

L'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto maggiore consentito trasferibile attraverso la connessione. Tutte le istanze Amazon EC2 supportano i frame standard (1500 MTU) e tutti i tipi di istanza della generazione attuale supportano i frame jumbo (9001 MTU).

Puoi visualizzare l'MTU per le tue istanze Amazon EC2, visualizzare il percorso MTU tra l'istanza e un altro host e configurare le istanze per utilizzare frame standard o jumbo.

Processi

- Verifica della MTU del percorso tra due host
- Controlla l'MTU per la tua istanza
- Imposta la MTU per la tua istanza

Verifica della MTU del percorso tra due host

Puoi verificare la MTU del percorso tra la tua istanza EC2 e un altro host. Puoi specificare un nome DNS o un indirizzo IP come destinazione. Se la destinazione è un'altra istanza EC2, verificare che il suo gruppo di sicurezza permetta il traffico UDP in entrata.

La procedura utilizzata dipende dal sistema operativo dell'istanza.

Istanze Linux

Eseguire il comando tracepath sull'istanza per verificare la MTU del percorso tra la tua istanza EC2 e la destinazione specificata. Questo comando fa parte del pacchetto `iputils`, disponibile per impostazione predefinita in molte distribuzioni Linux.

Nell'esempio viene verificata la MTU del percorso tra l'istanza EC2 e `amazon.com`.

```
[ec2-user ~]$ tracepath amazon.com
```

In questo output di esempio, la MTU del percorso è 1500.

```
 1?: [LOCALHOST]     pmtu 9001
 1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)   0.187ms pmtu 1500
 1:  no reply
 2:  no reply
 3:  no reply
 4:  100.64.16.241 (100.64.16.241)                              0.574ms
 5:  72.21.222.221 (72.21.222.221)                             84.447ms asymm 21
 6:  205.251.229.97 (205.251.229.97)                           79.970ms asymm 19
 7:  72.21.222.194 (72.21.222.194)                             96.546ms asymm 16
 8:  72.21.222.239 (72.21.222.239)                             79.244ms asymm 15
 9:  205.251.225.73 (205.251.225.73)                           91.867ms asymm 16
...
31:  no reply
     Too many hops: pmtu 1500
     Resume: pmtu 1500
```

Istanze Windows

Verifica della MTU del percorso tramite mturoute

1. Effettua il download sulla tua istanza EC2 da. mturoute.exe https://elifulkerson.com/projects/mturoute.php

2. Aprire una finestra del prompt dei comandi e passare alla directory in cui è stato scaricato mturoute.exe.
3. Utilizza il comando seguente per verificare la MTU del percorso tra la tua istanza EC2 e la destinazione specificata. Nell'esempio viene verificata la MTU del percorso tra l'istanza EC2 e `www.elifulkerson.com`.

```
.\mturoute.exe www.elifulkerson.com
```

In questo output di esempio, la MTU del percorso è 1500.

```
* ICMP Fragmentation is not permitted. *
* Speed optimization is enabled. *
* Maximum payload is 10000 bytes. *
+ ICMP payload of 1472 bytes succeeded.
- ICMP payload of 1473 bytes is too big.
Path MTU: 1500 bytes.
```

Controlla l'MTU per la tua istanza

Puoi controllare il valore MTU per la tua istanza. Alcune istanze sono configurate per l'utilizzo di frame jumbo, mentre altre sono configurate per l'utilizzo di dimensioni di frame standard.

La procedura utilizzata dipende dal sistema operativo dell'istanza.

Istanze Linux

Verifica dell'impostazione della MTU su un'istanza Linux

Eseguire il seguente comando ip sull'istanza EC2. Se l'interfaccia di rete principale non è `eth0`, sostituisci `eth0` con la tua interfaccia di rete.

```
[ec2-user ~]$ ip link show eth0
```

In questo output di esempio, *`mtu 9001`* indica che l'istanza utilizza frame jumbo.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode
 DEFAULT group default qlen 1000
    link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

Istanze Windows

La procedura utilizzata dipende dal driver dell'istanza.

ENA driver

Versione 2.1.0 e successive

Per ottenere il valore MTU, usa il seguente comando Get-NetAdapterAdvancedProperty sulla tua istanza EC2. Utilizza il jolly (asterisco) per ottenere tutti i nomi Ethernet. Verifica l'output del nome dell'interfaccia `*JumboPacket`. Un valore di 9015 indica che i frame jumbo sono abilitati. I frame jumbo sono disabilitati per impostazione predefinita.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet*"
```

Versione 1.5 e precedenti

Per ottenere il valore MTU, usa il seguente comando Get-NetAdapterAdvancedProperty sulla tua istanza EC2. Verifica l'output del nome dell'interfaccia `MTU`. Un valore di 9001 indica che i frame jumbo sono abilitati. I frame jumbo sono disabilitati per impostazione predefinita.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Intel SRIOV 82599 driver

Per ottenere il valore MTU, usa il seguente comando Get-NetAdapterAdvancedProperty sulla tua istanza EC2. Verificare la voce del nome dell'interfaccia `*JumboPacket`. Un valore di 9014 indica che i frame jumbo sono abilitati. Tieni presente che la dimensione della MTU include l'intestazione e il payload. I frame jumbo sono disabilitati per impostazione predefinita.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

AWS PV driver

Per ottenere il valore MTU, usa il seguente comando sulla tua istanza EC2. Il nome dell'interfaccia può variare. Nell'output, cercare una voce denominata "Ethernet", "Ethernet 2" o "Local Area Connection". Il nome dell'interfaccia sarà necessario per abilitare o disabilitare i frame jumbo. Un valore di 9001 indica che i frame jumbo sono abilitati.

```
netsh interface ipv4 show subinterface
```

Imposta la MTU per la tua istanza

Potrebbe essere necessario utilizzare i frame jumbo per il traffico di rete all'interno del VPC e utilizzare frame standard per il traffico Internet. Qualunque sia il caso d'uso, consigliamo di verificare che le istanze si comportino nel modo previsto.

La procedura utilizzata dipende dal sistema operativo dell'istanza.

Istanze Linux

Impostazione del valore della MTU su un'istanza Linux

1. Eseguire il seguente comando ip sull'istanza. Imposta il valore delle MTU desiderato su 1500, ma puoi in alternativa utilizzare 9001. Se l'interfaccia di rete principale non è `eth0`, sostituisci `eth0` con l'interfaccia di rete effettiva.

   ```
   [ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
   ```

2. (Opzionale) Per mantenere l'impostazione della MTU della rete dopo un riavvio, modificare i file di configurazione seguenti, in base al tipo di sistema operativo.

   - Amazon Linux 2023: modifica la sezione `[Link]` del file di configurazione. Il file di configurazione predefinito è`/usr/lib/systemd/network/80-ec2.network`, oppure è possibile aggiornare qualsiasi file di configurazione personalizzato creato in/run/systemd/network/, il cui nome del file è - .network. *`priority interface`* Per ulteriori informazioni, consulta Networking service nella documentazione di Amazon Linux.

     ```
     MTUBytes=1500
     ```

   - Amazon Linux 2: aggiungi la seguente riga al file `/etc/sysconfig/network-scripts/ifcfg-`*`eth0`*:

     ```
     MTU=1500
     ```

     Aggiungere la seguente riga al file `/etc/dhcp/dhclient.conf`:

     ```
     request subnet-mask, broadcast-address, time-offset, routers, domain-name,
      domain-search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-
     servers;
     ```

- Altre distribuzioni Linux: consultare la relativa documentazione specifica.

3. (Opzionale) Riavviare l'istanza e verificare che l'impostazione della MTU sia corretta.

Istanze Windows

La procedura utilizzata dipende dal driver dell'istanza.

ENA driver

È possibile modificare la MTU tramite Gestione dispositivi o il comando Set-NetAdapterAdvancedProperty nella tua istanza.

Versione 2.1.0 e successive

Utilizza il seguente comando per abilitare i frame jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9015
```

Utilizza il seguente comando per disabilitare i frame jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

Versione 1.5 e precedenti

Utilizza il seguente comando per abilitare i frame jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 9001
```

Utilizza il seguente comando per disabilitare i frame jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 1500
```

Intel SRIOV 82599 driver

È possibile modificare la MTU tramite Gestione dispositivi o il comando Set-NetAdapterAdvancedProperty nella tua istanza.

Utilizza il seguente comando per abilitare i frame jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9014
```

Utilizza il seguente comando per disabilitare i frame jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

AWS PV driver

È possibile modificare la MTU tramite il netsh comando sull'istanza. Non è possibile modificare la MTU tramite Gestione dispositivi.

Utilizza il seguente comando per abilitare i frame jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=9001
```

Utilizza il seguente comando per disabilitare i frame jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500
```

Risoluzione dei problemi

Se riscontri problemi di connettività tra l'istanza EC2 e un cluster Amazon Redshift durante l'utilizzo di frame jumbo, consulta Queries appear to hang and sometimes fail to reach the cluster nella Guida alla gestione di Amazon Redshift.

Cloud privati virtuali per le istanze EC2

Amazon Virtual Private Cloud (Amazon VPC) ti consente di definire una rete virtuale nella tua area logicamente isolata all'interno del AWS cloud, nota come cloud privato virtuale o VPC. Puoi creare AWS risorse, come istanze Amazon EC2, nelle sottoreti del tuo VPC. Il VPC è molto simile a una rete tradizionale gestibile nel data center locale, ma con i vantaggi legati all'utilizzo dell'infrastruttura scalabile di AWS. Puoi configurare il VPC, selezionare l'intervallo di indirizzi IP, creare sottoreti e

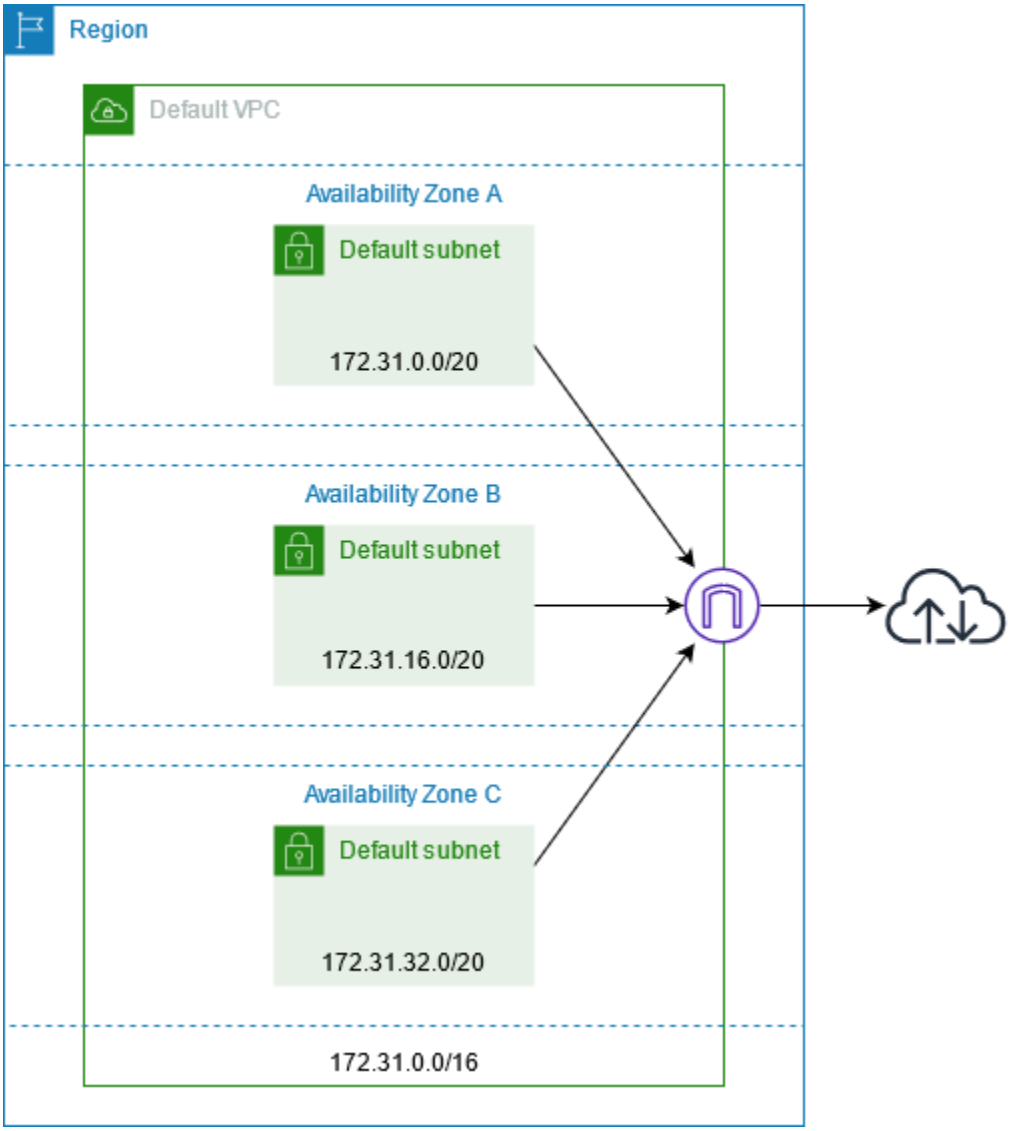
configurare tabelle di routing, gateway di rete e impostazioni di sicurezza. È possibile connettere le istanze del VPC a Internet o al proprio data center.

Indice

- I tuoi VPC predefiniti
- VPC non predefiniti
- Accesso a Internet
- Sottoreti condivise
- IPv6-only sottoreti

I tuoi VPC predefiniti

Quando crei il tuo AWS account, creiamo un VPC predefinito in ogni regione. Un VPC predefinito è un VPC già configurato e pronto all'uso. Ad esempio, esiste una sottorete predefinita per ogni zona di disponibilità in ogni VPC predefinito, un gateway Internet collegato al VPC e c'è una route nella tabella di routing principale che invia tutto il traffico (0.0.0. 0/0) al gateway Internet. È possibile modificare la configurazione dei VPC predefiniti secondo necessità. Ad esempio, è possibile aggiungere sottoreti e tabelle di routing.



VPC non predefiniti

Invece di utilizzare un VPC predefinito per le risorse, è possibile creare un VPC proprio, come descritto in Creare un VPC nella Guida per l'utente di Amazon VPC.

Di seguito sono riportati alcuni aspetti da considerare quando si crea un VPC per le istanze EC2.

- È possibile utilizzare il suggerimento predefinito per il blocco CIDR IPv4 oppure inserire il blocco CIDR richiesto dall'applicazione o dalla rete.
- Per garantire una disponibilità elevata, è necessario creare sottoreti in più zone di disponibilità.
- Se le istanze devono essere accessibili da Internet, procedi in uno dei seguenti modi:

- Se le istanze possono trovarsi in una sottorete pubblica, aggiungi sottoreti pubbliche. Mantieni abilitate entrambe le opzioni DNS. Facoltativamente, puoi aggiungere sottoreti private adesso o in seguito.
- Se le istanze devono trovarsi in una sottorete privata, aggiungi solo sottoreti private. È possibile aggiungere un gateway NAT per fornire l'accesso a Internet alle istanze nelle sottoreti private. Se le istanze inviano o ricevono un volume significativo di traffico tra zone di disponibilità, crea un gateway NAT in ogni zona di disponibilità. Altrimenti, è possibile creare un gateway NAT in una sola zona di disponibilità e avviare istanze che inviano o ricevono traffico tra zone nella stessa zona di disponibilità rispetto al gateway NAT.

Accesso a Internet

Le istanze avviate in una sottorete predefinita all'interno di un VPC predefinito hanno accesso a Internet, poiché i VPC predefiniti sono configurati per assegnare indirizzi IP pubblici e nomi host DNS e la tabella di routing principale è configurata con un percorso verso un gateway Internet collegato al VPC.

Per le istanze avviate nelle sottoreti e nei VPC non predefiniti, puoi utilizzare una delle seguenti opzioni per assicurarti che le istanze avviate in queste sottoreti abbiano accesso a Internet:

- Configurazione di un gateway Internet. Per ulteriori informazioni, consulta Collegamento delle sottoreti a Internet tramite un gateway Internet nella Guida per l'utente di Amazon VPC.
- Configurazione di un Gateway NAT pubblico. Per ulteriori informazioni, consulta Accesso a Internet da una sottorete privata nella Guida per l'utente di Amazon VPC.

Sottoreti condivise

Quando avvii istanze EC2 in sottoreti VPC condivise, tieni presente quanto segue:

- I partecipanti possono eseguire istanze in una sottorete condivisa specificando l'ID della sottorete condivisa. I partecipanti devono possedere eventuali interfacce di rete specificate.
- I partecipanti possono avviare, interrompere, terminare e descrivere le istanze che hanno creato in una sottorete condivisa. I partecipanti non possono avviare, interrompere, terminare o descrivere le istanze create dal proprietario del VPC nella sottorete condivisa.
- I proprietari del VPC non possono avviare, interrompere, terminare o descrivere le istanze create dai partecipanti in una sottorete condivisa.

- I partecipanti possono connettersi a un'istanza in una sottorete condivisa utilizzando un endpoint EC2 Instance Connect. Il partecipante deve creare l'endpoint EC2 Instance Connect nella sottorete condivisa. I partecipanti non possono utilizzare un endpoint EC2 Instance Connect creato dal proprietario del VPC nella sottorete condivisa.

Per ulteriori informazioni sulle risorse condivise di Amazon EC2, consultare:

- the section called "Gestire la condivisione di un'AMI con un'organizzazione o un'unità organizzativa"
- the section called "Prenotazioni della capacità condivise"
- the section called "Gruppi di posizionamento condivisi"
- Cross-account Condivisione di host dedicati Amazon EC2

Per ulteriori informazioni sulle sottoreti condivise, consultare Condivisione del VPC con altri account nella Guida per l'utente di Amazon VPC.

IPv6-only sottoreti

Un'istanza EC2 avviata in una IPv6-only sottorete riceve un indirizzo IPv6 ma non un indirizzo IPv4. Tutte le istanze avviate in una sottorete devono essere istanze. IPv6-only Nitro-based

Reti secondarie

Le reti secondarie sono reti virtuali create appositamente per casi d'uso di rete specializzati. Queste reti sono logicamente isolate all'interno di partizioni del cloud. AWS È possibile creare risorse come sottoreti secondarie all'interno della rete secondaria. Le reti secondarie sono strettamente collegate ad Amazon VPC, pertanto alcune istanze sono multi-home e avviate sia in un VPC che in una rete secondaria.

Le reti secondarie sono attualmente disponibili per determinati tipi di istanze e tramite prenotazioni di capacità con impegni a lungo termine. Contatta il team del tuo account per ulteriori informazioni se ritieni che le reti secondarie possano essere utili per il tuo carico di lavoro.

Indice

- Cosa sono le reti secondarie?
- Concetti chiave

- Architecture
- Ulteriori considerazioni
- Nozioni di base
- Gestione delle risorse di rete secondarie
- Best practice per la progettazione della rete
- Risoluzione dei problemi
- Quote e limiti

Cosa sono le reti secondarie?

Le reti secondarie forniscono una rete logica isolata, utilizzata in combinazione con una rete VPC, in modo tale che le istanze siano collegate in più home in due reti indipendenti. I vantaggi delle reti secondarie includono:

- High-performance rete per casi d'uso e protocolli specializzati, come la connettività est-ovest per carichi di lavoro ML
- Multi-tenant supporto con isolamento logico
- Le istanze si integrano perfettamente con VPC e servizi AWS

Concetti chiave

Rete secondaria

: Un costrutto di rete regionale che fornisce una rete logica di livello 3 con un blocco CIDR IPv4 (compreso tra /28 e /12). Le reti secondarie operano indipendentemente dai VPC su un'infrastruttura di rete fisicamente partizionata.

Sottorete secondaria

: Un Zone-specific costrutto di disponibilità all'interno di una rete secondaria, simile alle sottoreti VPC. Le sottoreti secondarie supportano blocchi CIDR compresi tra /28 e /12.

Interfaccia secondaria

: Interfacce di rete collegate a schede di rete secondarie, che forniscono connettività est-ovest all'interno di sottoreti secondarie. Queste interfacce sono fisicamente e logicamente separate dalle Elastic Network Interfaces (ENI).

Architecture

Le istanze EC2 che supportano le reti secondarie sono multi-homed, il che significa che possono comunicare contemporaneamente all'interno di un VPC e di una rete secondaria:

- VPC: fornisce TCP/IP connettività nord-sud a AWS servizi, storage, database, servizi di rete e Internet
- Rete secondaria: fornisce connettività est-ovest tra istanze specializzate supportate

Ulteriori considerazioni

- Le interfacce secondarie sono gestite tramite RunInstances e non possono essere create o eliminate in modo indipendente.
- Le interfacce secondarie non possono essere utilizzate attached/detached dopo l'avvio dell'istanza.
- Interfacce secondarie Gli indirizzi IP non possono essere modificati una volta avviate.
- Le funzionalità VPC come Security Groups, NACL e Flow Logs non sono supportate nelle reti secondarie.

Nozioni di base

Prerequisiti

Prima di avviare le istanze con le reti secondarie, assicurati di aver configurato anche il tuo VPC nella regione di destinazione e una sottorete nella zona di disponibilità di destinazione della tua capacità EC2.

Fase 1: creazione di una rete secondaria

Crea una rete secondaria nella stessa regione del tuo VPC. Si tratta di una risorsa regionale che fornisce l'isolamento logico del traffico RDMA.

```
aws ec2 create-secondary-network \
  --network-type rdma \
  --ipv4-cidr-block 172.31.0.0/16 \
  --region us-east-2
```

Parametri:

- `--network-type`: tipo di rete (attualmente è supportato solo rdma)
- `--ipv4-cidr-block`: blocco CIDR IPv4 compreso tra /28 e /12
- `--region` AWS : US-East-2 Regione ()

> **Note**
>
> Procedura consigliata: scegli un blocco CIDR che non si sovrapponga al tuo CIDR VPC per semplificare il routing a livello di istanza.

Fase 2: Creare una sottorete secondaria

Crea una sottorete secondaria nella stessa zona di disponibilità della sottorete VPC. Questa è una risorsa. AZ-specific

```
aws ec2 create-secondary-subnet \
  --secondary-network-id sn-1234567890abcdef0 \
  --ipv4-cidr-block 172.31.24.0/24 \
  --availability-zone us-east-2a
```

> **Note**
>
> Prenotazione dell'indirizzo IP: come le sottoreti VPC, Amazon riserva i primi 4 indirizzi IP e l'ultimo indirizzo IP in ciascuna sottorete secondaria per uso interno.

Fase 3. Avvio di un'istanza

Avvia un'istanza sia nella sottorete VPC che nella sottorete secondaria. L'istanza sarà multi-home con connettività a entrambe le reti.

```
aws ec2 run-instances \
  --image-id ami-12345678 \
  --count 1 \
  --instance-type <instance> \
  --key-name MyKeyPair \
  --instance-market-options '{"MarketType": "capacity-block"}' \
  --capacity-reservation-specification '{"CapacityReservationTarget": \
  {"CapacityReservationId": "cr-1234567890abcdef0"}}' \
```

```
  --network-interfaces \
    "NetworkCardIndex=0,DeviceIndex=0,Groups=sg-12345678,\
    SubnetId=subnet-0987654321fedcba0,InterfaceType=interface" \
  --secondary-interfaces \
    "NetworkCardIndex=1,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=2,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=3,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=4,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=5,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=6,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=7,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true", \
    "NetworkCardIndex=8,DeviceIndex=0,SecondarySubnetId=ss-98765421yxz,\
    InterfaceType=secondary,PrivateIpAddressCount=1,DeleteOnTermination=true"
```

Parametri chiave:

- `--network-interfaces`: Specifica il Nitro ENI principale per la connettività VPC (Network Card Index 0)
- `--secondary-interfaces`: Specifica 8 interfacce secondarie per la connettività est-ovest all'interno delle sottoreti secondarie (indici delle schede di rete 1-8)
- `InterfaceType=secondary`: indica un'interfaccia secondaria

Gestione delle risorse di rete secondarie

Descrivere le reti secondarie

Visualizza i dettagli sulle tue reti secondarie:

```
aws ec2 describe-secondary-networks \
  --secondary-network-id sn-1234567890abcdef0
```

Descrizione delle sottoreti secondarie

Visualizza i dettagli sulle tue sottoreti secondarie:

```
aws ec2 describe-secondary-subnets \
  --secondary-subnet-id ss-98765421yxz
```

Descrizione delle interfacce secondarie

Visualizza i dettagli sulle interfacce di rete secondarie collegate alle tue istanze:

```
aws ec2 describe-secondary-interfaces \
  --filters "Name=attachment.instance-id,Values=i-1234567890abcdef0"
```

Eliminazione delle risorse

Elimina una sottorete secondaria:

```
aws ec2 delete-secondary-subnet \
  --secondary-subnet-id ss-98765421yxz
```

Elimina una rete secondaria:

```
aws ec2 delete-secondary-network \
  --secondary-network-id sn-1234567890abcdef0
```

> **Important**
>
> È necessario terminare tutte le istanze ed eliminare tutte le sottoreti secondarie prima di eliminare una rete secondaria.

Best practice per la progettazione della rete

Pianificazione CIDR

Evita la sovrapposizione dei CIDR: mentre le reti secondarie sono fisicamente isolate dai VPC, l'utilizzo di blocchi CIDR non sovrapposti semplifica la configurazione del routing a livello di sistema operativo dell'istanza.

> **Note**
>
> Amazon riserva 5 indirizzi IP per sottorete.

Segregazione del traffico

Separa per rete secondaria: crea reti secondarie separate per diversi progetti, team o limiti di sicurezza. Le reti secondarie forniscono l'isolamento logico tra le istanze. Le istanze non possono comunicare tra reti secondarie diverse.

Usa più sottoreti: all'interno di una rete secondaria, utilizza più sottoreti secondarie per segmentare il traffico per indice GPU, zona di disponibilità o tipo di carico di lavoro. Ad esempio, un modello di architettura comune consiste nell'implementazione di un'unica rete secondaria con 4 o 8 sottoreti secondarie, in cui ciascuna sottorete secondaria è allineata a un gruppo di GPU con indici comuni.

Risoluzione dei problemi

Errori di avvio dell'istanza

Problema: l'istanza non viene avviata con le interfacce di rete secondarie.

Soluzioni:

- Verifica che la tua AMI includa un supporto adeguato per i driver
- Assicurati che la tua sottorete secondaria abbia un numero sufficiente di indirizzi IP disponibili
- Conferma che la prenotazione della capacità sia in stato «attivo»
- Verifica che la sottorete secondaria si trovi nella stessa zona di disponibilità della sottorete VPC

Problemi di connettività

Problema: impossibile stabilire la connettività RDMA tra le istanze.

Soluzioni:

- Verifica che tutte le istanze si trovino nella stessa rete secondaria e sottorete secondaria
- Verifica che i driver di interfaccia secondari siano caricati correttamente sull'istanza
- Assicurati che l'applicazione sia vincolata alle interfacce di rete corrette
- Le istanze all'interno della stessa sottorete secondaria sono raggiungibili tramite percorsi diretti. La comunicazione tra sottoreti è disponibile tramite una route statica fornita tramite DHCP.

errori API

Problema: le chiamate API per le operazioni sulla rete secondaria e sulla sottorete secondaria non riescono.

Soluzioni:

- Verifica le autorizzazioni IAM per ec2:CreateSecondaryNetwork, ec2:. CreateSecondarySubnet
- Verifica che i blocchi CIDR rientrino nell'intervallo supportato (da /28 a /12)
- Verifica di utilizzare la regione e la zona di disponibilità corrette

Quote e limiti

Per richiedere aumenti delle quote, utilizza le quote AWS di servizio o contatta l' AWS assistenza.

Quote e limiti delle reti secondarie

Risorsa	Limite	Regolabile
Reti secondarie per regione	5	Sì
Sottoreti secondarie per rete secondaria	200	Sì
Dimensione del blocco CIDR	Da /28 a /12	No

Sicurezza in Amazon EC2

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 modello come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in sicurezza. Third-party gli auditor testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità Programmi di AWS conformità Programmi Per ulteriori informazioni sui programmi di conformità che si applicano ad Amazon EC2, consulta AWS Services in Scope by Compliance Program
- Sicurezza nel cloud - La tua responsabilità include le seguenti aree.
  - Controllo dell'accesso di rete alle istanze, ad esempio mediante la configurazione del VPC e dei gruppi di sicurezza. Per ulteriori informazioni, consulta Controllo del traffico di rete.
  - Gestione delle credenziali utilizzate per connettersi alle istanze.
  - Gestione del sistema operativo guest e del software distribuiti nel sistema operativo guest, inclusi aggiornamenti e patch di sicurezza. Per ulteriori informazioni, consulta Gestione degli aggiornamenti per le istanze Amazon EC2.
  - Configurazione dei ruoli IAM collegati all'istanza e le autorizzazioni associate a tali ruoli. Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando si usa Amazon EC2. Viene illustrato come configurare Amazon EC2 per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Amazon EC2.

Indice

- Protezione dei dati in Amazon EC2
- Sicurezza dell'infrastruttura in Amazon EC2
- Resilienza in Amazon EC2
- Convalida della conformità per Amazon EC2

- Identity and Access Management per Amazon EC2
- Gestione degli aggiornamenti per le istanze Amazon EC2
- Procedure ottimali relative alla sicurezza delle istanze Windows
- Coppie di chiavi Amazon EC2 e istanze Amazon EC2
- Gruppi di sicurezza Amazon EC2 per le istanze EC2
- NitroTPM per istanze Amazon EC2
- Attestazione dell'istanza Amazon EC2
- Credential Guard per istanze Windows
- Accesso ad Amazon EC2 utilizzando un endpoint VPC di interfaccia

Protezione dei dati in Amazon EC2

Il modello di responsabilità AWS https://aws.amazon.com/compliance/shared-responsibility-model/ si applica alla protezione dei dati in Amazon Elastic Compute Cloud. 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 della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi Domande frequenti sulla privacy dei dati Termini legali della regione . Per ulteriori informazioni sulla protezione dei dati in Europa, consulta il Centro generale sulla protezione dei dati (GDPR).

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con Centro identità AWS IAM 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 Usalo 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'uso 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 Servizi AWS.
- 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 Amazon EC2 o altro Servizi AWS utilizzando la console, l'API o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i 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.

Indice

- Sicurezza dei dati di Amazon EBS
- Crittografia dei dati a riposo
- Crittografia dei dati in transito

Sicurezza dei dati di Amazon EBS

I volumi di Amazon EBS sono presentati come dispositivi a blocchi non elaborati e non formattati. Sono dispositivi logici creati sull'infrastruttura EBS e il servizio Amazon EBS garantisce che siano logicamente vuoti (ovvero che i blocchi non elaborati vengano azzerati o contengano dati crittograficamente pseudocasuali) prima di qualsiasi utilizzo o riutilizzo da parte di un cliente.

Se disponi di procedure che richiedono la cancellazione di tutti i dati usando un metodo specifico, dopo o prima dell'utilizzo (o in entrambi i casi), come quelli indicati in modo dettagliato in DoD 5220.22-M (National Industrial Security Program Operating Manual, Manuale operativo del programma nazionale di sicurezza industriale) o NIST 800-88 (Guidelines for Media Sanitization, Linee guida per la sanificazione dei supporti), hai la possibilità di eseguire questa operazione su Amazon EBS. Tale attività a livello di blocco si rifletterà sui supporti di archiviazione sottostanti all'interno del servizio Amazon EBS.

Crittografia dei dati a riposo

Volumi EBS

La crittografia Amazon EBS è una soluzione di crittografia per i volumi e gli snapshot EBS che utilizza AWS KMS keys. Per ulteriori informazioni, consulta Crittografia Amazon EBS nella Guida per l'utente di Amazon EBS.

[Istanze Windows] Puoi inoltre utilizzare le autorizzazioni Microsoft EFS e NTFS per la crittografia a livello di cartella e file.

Volumi di archivio dell'istanza

I dati sui volumi degli store di istanze NVMe sono crittografati utilizzando un XTS-AES-256 codice, implementato su un modulo hardware sull'istanza. Le chiavi utilizzate per crittografare i dati scritti sui dispositivi di archiviazione NVMe collegati localmente sono per cliente e per volume. Le chiavi sono generate e risiedono solo all'interno del modulo hardware, che è inaccessibile al personale AWS . Quando l'istanza viene arrestata o terminata, le chiavi crittografiche vengono distrutte e non possono essere ripristinate. Non è possibile disattivare questa cifratura e non è possibile fornire una propria chiave crittografica.

I dati sui volumi di archiviazione delle istanze HDD sulle istanze H1, D3 e D3en vengono crittografati utilizzando chiavi monouso. XTS-AES-256

Quando arresti, sospendi o termini un'istanza, ogni blocco di archiviazione nel volume dell'archivio istanza viene ripristinato. Pertanto, non è possibile accedere ai dati attraverso l'instance store di un'altra istanza.

Memoria

La crittografia della memoria è abilitata nelle seguenti istanze:

- Le istanze con processori AWS Graviton2 o successivi supportano la crittografia della memoria sempre attiva. AWS Le chiavi di crittografia vengono generate in modo sicuro all'interno del sistema host, non lasciano il sistema host e vengono distrutte quando l'host viene riavviato o spento. Per ulteriori informazioni, consulta la pagina Processori AWS Graviton.
- Istanze con processori scalabili Intel Xeon di terza generazione (Ice Lake), come le istanze M6i, e processori scalabili Intel Xeon di quarta generazione (Sapphire Rapids), come le istanze M7i. Questi processori supportano la crittografia della memoria sempre attiva utilizzando Intel Total Memory Encryption (TME).
- Istanze con processori AMD EPYC di terza generazione (Milan), come le istanze M6a, e processori AMD EPYC di quarta generazione (Genoa), come le istanze M7a. Questi processori supportano la crittografia della memoria sempre attiva utilizzando AMD Secure Memory Encryption (SME).

- AMD Secure Encrypted Virtualization-Secure Nested Paging () è supportato per alcuni tipi di istanze. SEV-SNP AMD-based Per ulteriori informazioni, consulta Trova i tipi di istanze EC2 che supportano AMD SEV-SNP.

Crittografia dei dati in transito

Crittografia a livello fisico

Tutti i dati che fluiscono tra AWS le regioni sulla rete AWS globale vengono automaticamente crittografati a livello fisico prima di lasciare le AWS strutture protette. Tutto il traffico tra le AZ è crittografato. Ulteriori livelli di crittografia, inclusi quelli elencati in questa sezione, possono fornire ulteriore protezione.

Crittografia fornita da peering di Amazon VPC e peering fra regioni Transit Gateway

Tutto il traffico tra regioni che utilizza il peering Amazon VPC e Transit Gateway viene automaticamente crittografato in massa quando esce da una regione. Un ulteriore livello di crittografia viene fornito automaticamente a livello fisico per tutto il traffico prima che lasci le strutture AWS protette, come indicato in precedenza in questa sezione.

Crittografia tra istanze

AWS fornisce una connettività sicura e privata tra istanze EC2 di tutti i tipi. Inoltre, alcuni tipi di istanza utilizzano le funzionalità di offload dell'hardware Nitro System sottostante per crittografare automaticamente il traffico in transito tra le istanze. Questa crittografia utilizza algoritmi AEAD (Authenticated Encryption with Associated Data), con crittografia a 256 bit. Non vi è alcun impatto sulle prestazioni della rete. Per supportare questa crittografia aggiuntiva del traffico in transito tra istanze, è necessario soddisfare i seguenti requisiti:

- Le istanze utilizzano i seguenti tipi di istanza:
  - Uso generale: M5dn, M5n, M5zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7g, M7gd, M7i, M8a, M8azn, M8g, M8gb, M8gd, M8gn, M8i, M8id, M8in, M8in M7i-flex, M8n 8idn, M8ine, M8ib, M8idb, M9g, M9gd,, M8i-flex Mac-m4 Mac-m4pro
  - Ottimizzato per il calcolo: C5n, C6a, C6gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gd, C7gn C7i-flex, C7i,, C8a, C8g, C8gb, C8gd, C8gn, C8i, C8id C8i-flex, C8in, C8ine, C8ib, C9g, C9gd
  - Memoria ottimizzata: R5dn, R5n, R6a, R6i, R6id, R6idn, R6in, R7a, R7g, R7gd, R7i, R7iz, R8a, R8g, R8gb, R8gd, R8gd, R8gn, R8i, R8id, R8in, R8iN, R8ib, R8idb R8i-flex, R9g,

R9gd,,,,,,,,,,,,,,,,,,, X2idn U-3tb1, X2iEDN U-6tb1 U-9tb1 U-12tb1 U-18tb1 U-24tb1, X2iZn U7i-6tb U7i-8tb U7i-12tb U7in-16tb, X8g U7in-24tb U7in-32tb U7inh-32tb, X8aedz, X8i

- Ottimizzate per l'archiviazione: D3, D3en, I3en, I4g, I4i, I7i, I7ie, I8g, I8ge, Im4gn, Is4gen
- Calcolo accelerato: DL1, DL2q, F2, G4ad, G4dn, G5, G6, G6e, G6f, Gr6, Gr6f, G7, G7e, Inf1, Inf2, P3dn, P4d, P4de, P5, P5e, P5en, P6-B200, P6-B300, P6e-GB200, Trn1, Trn1n, Trn2, TrN2u, VT1
- High-performance elaborazione: HPC6a, HPC6id, HPC7a, HPC7g, HPC8a

- Le istanze si trovano nella stessa regione.
- Le istanze si trovano nello stesso VPC o VPC con peering e il traffico non passa attraverso un dispositivo di rete virtuale, ad esempio un load balancer (load balancer) o un Transit Gateway.

Un ulteriore livello di crittografia viene fornito automaticamente a livello fisico per tutto il traffico prima che lasci le strutture protette, come indicato in precedenza in questa sezione. AWS

Per visualizzare i tipi di istanze che crittografano il traffico in transito tra le istanze utilizzando il AWS CLI

Utilizza il seguente comando: describe-instance-types.

```
aws ec2 describe-instance-types \
    --filters Name=network-info.encryption-in-transit-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Crittografia da e verso AWS Outposts

Un Outpost crea connessioni di rete speciali denominate service links alla sua regione di AWS origine e, facoltativamente, connettività privata a una sottorete VPC specificata dall'utente. Tutto il traffico su tali connessioni è completamente crittografato. Per ulteriori informazioni, consulta Connettività tramite collegamenti per servizio e Crittografia in transito nella Guida per l'utente di AWS Outposts .

Crittografia dell'accesso remoto

I protocolli SSH e RDP forniscono canali di comunicazione sicuri per l'accesso remoto alle istanze, sia direttamente che tramite EC2 Instance Connect. L'accesso remoto alle istanze tramite AWS Systems Manager Session Manager o Run Command è crittografato utilizzando TLS 1.2 e le richieste di creazione di una connessione sono firmate utilizzando https://docs.aws.amazon.com/IAM/latest/

UserGuide/reference_sigv.html Sigv4 e autenticate e autorizzate da. AWS Identity and Access Management

È responsabilità dell'utente utilizzare un protocollo di crittografia quale Transport Layer Security (TLS) per eseguire la crittografia dei dati sensibili in transito tra i client e le istanze Amazon EC2.

(Istanze Windows) Assicurati di consentire solo connessioni crittografate tra istanze EC2 e gli endpoint API AWS o altri servizi di rete remota sensibili. È possibile applicare questa operazione tramite un gruppo di sicurezza in uscita o regole di Windows Firewall.

Sicurezza dell'infrastruttura in Amazon EC2

In quanto servizio gestito, Amazon Elastic Compute Cloud è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi le chiamate API AWS pubblicate per accedere ad Amazon EC2 attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di crittografia con Perfect Forward Secrecy (PFS) come DHE (Ephemeral) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Per ulteriori informazioni, vedere Infrastructure Protection in the Security Pillar — Framework. https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/infrastructure-protection.html AWS Well-Architected

Isolamento della rete

Un cloud privato virtuale (VPC) è una rete virtuale situata nella tua area logicamente isolata nel cloud. AWS Utilizza VPC separati per isolare l'infrastruttura in base a carico di lavoro o entità dell'organizzazione.

Una sottorete è un intervallo di indirizzi IP in un VPC. Quando avvii un'istanza, questa operazione viene eseguita in una sottorete nel VPC. Utilizza sottoreti per isolare i livelli dell'applicazione (ad

esempio, web, applicazione e database) all'interno di un singolo VPC. Utilizza sottoreti private per le istanze se non devono essere accessibili direttamente da Internet.

Per chiamare l'API di Amazon EC2 dal tuo VPC utilizzando indirizzi IP privati, utilizza AWS PrivateLink. Per ulteriori informazioni, consulta Accesso ad Amazon EC2 utilizzando un endpoint VPC di interfaccia.

Isolamento su host fisici

Istanze EC2 differenti sullo stesso host fisico sono tra loro isolate come se si trovassero su host fisici separati. L'hypervisor isola CPU e memoria e le istanze vengono fornite su dischi virtualizzati anziché accedere a dispositivi vergini non formattati.

Quando si interrompe o termina un'istanza, la memoria ad essa allocata viene annullata (impostata su zero) dall'hypervisor prima che venga allocata a una nuova istanza e ogni blocco di archiviazione viene ripristinato. Questo garantisce che i dati non vengano involontariamente esposti a un'altra istanza.

Gli indirizzi MAC di rete vengono assegnati dinamicamente alle istanze dall'infrastruttura di rete. AWS Gli indirizzi IP vengono assegnati dinamicamente a istanze dall'infrastruttura di rete AWS o assegnati da un amministratore EC2 tramite richiese API autenticate. La AWS rete consente alle istanze di inviare traffico solo dagli indirizzi MAC e IP loro assegnati. In caso contrario, il traffico viene interrotto.

Per impostazione predefinita, un'istanza non può ricevere traffico che non è specificatamente indirizzato ad essa. Se devi eseguire servizi di traduzione degli indirizzi di rete (NAT), routing o firewall sulla tua istanza, puoi disattivare il source/destination controllo dell'interfaccia di rete.

Controllo del traffico di rete

Valuta le opzioni seguenti per il controllo del traffico di rete alle istanze EC2:

- Limita l'accesso alle istanze mediante gruppi di sicurezza. Configura regole che consentano il traffico di rete minimo richiesto. Ad esempio, è possibile consentire il traffico solo dagli intervalli di indirizzi per la rete aziendale o solo per protocolli specifici, come HTTPS. Per le istanze Windows, consenti il traffico di gestione Windows e connessioni minime in uscita.
- Sfrutta i gruppi di sicurezza come meccanismo principale per controllare l'accesso della rete alle istanze Amazon EC2. Se necessario, utilizza liste di controllo degli accessi di rete con parsimonia per fornire un controllo di rete stateless di tipo granulare. I gruppi di sicurezza sono più versatili delle liste di controllo degli accessi di rete grazie alla loro capacità di eseguire il filtro dei pacchetti con stato e creare regole che fanno riferimento ad altri gruppi di sicurezza. Tuttavia, le liste di

controllo degli accessi di rete possono essere efficaci come controllo secondario per negare un sottoinsieme specifico di traffico o fornire alla sottorete una protezione di alto livello. Inoltre, le liste di controllo degli accessi di rete si applicano a un'intera sottorete, possono essere utilizzate come difesa in profondità nel caso in cui un'istanza venga avviata involontariamente senza un gruppo di sicurezza corretto.

- [Istanze Windows] Gestisci centralmente le impostazioni di Windows Firewall con Group Policy Objects (GPO) per migliorare ulteriormente i controlli di rete. I clienti utilizzano spesso Windows Firewall per un'ulteriore visibilità sul traffico di rete e per integrare i filtri dei gruppi di sicurezza, creando regole avanzate per impedire l'accesso alla rete ad applicazioni specifiche o per filtrare il traffico da un sottoinsieme di indirizzi IP. Ad esempio, Windows Firewall può limitare l'accesso all'indirizzo IP del servizio di metadati EC2 a specifici utenti o applicazioni. In alternativa, un servizio pubblico potrebbe utilizzare gruppi di sicurezza per limitare il traffico a porte specifiche e Windows Firewall per mantenere un elenco di indirizzi IP bloccati in modo esplicito.
- Utilizza sottoreti private per le istanze se non devono essere accessibili direttamente da Internet. Utilizza un host bastione o gateway NAT per l'accesso Internet da un'istanza in una sottorete privata.
- [Istanze Windows] Utilizza protocolli di amministrazione sicuri come l'incapsulamento RDP over. SSL/TLS Il Remote Desktop Gateway Quick Start fornisce le migliori pratiche per l'implementazione del gateway desktop remoto, inclusa la configurazione dell'RDP da utilizzare. SSL/TLS
- [Istanze Windows] Utilizza Active Directory o Directory Service per controllare e monitorare in modo rigoroso e centralizzato l'accesso interattivo di utenti e gruppi alle istanze di Windows ed evitare le autorizzazioni degli utenti locali. Evita inoltre di utilizzare gli amministratori di dominio e crea account basati sui ruoli più granulari e specifici dell'applicazione. Just Enough Administration (JEA) consente di gestire le modifiche alle istanze di Windows senza accesso interattivo o amministratore. Inoltre, JEA consente alle organizzazioni di bloccare l'accesso amministrativo al sottoinsieme di PowerShell comandi Windows necessari per l'amministrazione delle istanze. Per ulteriori informazioni, consulta Best Practices for Security, Identity e Compliance.
- [Istanze Windows] Gli amministratori di sistema devono utilizzare account Windows con accesso limitato per eseguire attività quotidiane e aumentare i diritti di accesso solo quando necessario per eseguire specifiche modifiche alla configurazione. Inoltre, accedi solo alle istanze di Windows direttamente quando è assolutamente necessario. Utilizza invece i sistemi di gestione della configurazione centralizzata come EC2 Run Command, Systems Center Configuration Manager (SCCM), Windows PowerShell DSC o Amazon EC2 Systems Manager (SSM) per inviare modifiche ai server Windows.

- Configura le tabelle di routing della sottorete di Amazon VPC con le route di rete minime richieste. Ad esempio, inserisci solo istanze Amazon EC2 che richiedono l'accesso diretto a Internet nelle sottoreti con route a un gateway Internet e le istanze Amazon EC2 che richiedono l'accesso diretto solo alle reti interne in sottoreti con route a un gateway privato virtuale.
- Prendi in considerazione l'utilizzo di gruppi di sicurezza aggiuntivi per controllare e verificare il traffico di gestione delle istanze Amazon EC2 separatamente dal normale traffico delle applicazioni. Questo approccio consente ai clienti di implementare criteri IAM speciali per il controllo delle modifiche, semplificando l'audit delle modifiche apportate alle regole dei gruppi di sicurezza o agli script di verifica automatica delle regole. L'utilizzo di più interfacce di rete fornisce inoltre opzioni aggiuntive per il controllo del traffico di rete, inclusa la possibilità di creare policy di instradamento basate su host o sfruttare diverse regole di instradamento delle sottoreti VPC basate sulla sottorete assegnata dell'interfaccia di rete.
- Usa AWS Virtual Private Network o Direct Connect per stabilire connessioni private dalle tue reti remote ai tuoi VPC. Per ulteriori informazioni, consulta Opzioni di connettività Network-to-Amazon VPC.
- Utilizza Log di flusso VPC per monitorare il traffico che raggiunge le istanze.
- Usa GuardDuty Malware Protection per identificare comportamenti sospetti indicativi della presenza di software dannoso sulle tue istanze che potrebbero compromettere il carico di lavoro, riutilizzare le risorse per usi dannosi e ottenere l'accesso non autorizzato ai tuoi dati.
- Usa GuardDuty Runtime Monitoring per identificare e rispondere a potenziali minacce alle tue istanze. Per ulteriori informazioni, consulta Come funziona il monitoraggio del runtime con le istanze Amazon EC2.
- Utilizza AWS Security Hub CSPM, Reachability Analyzer o Strumento di analisi degli accessi alla rete per verificare l'accessibilità indesiderata alla rete dalle istanze.
- Utilizza Connessione all'istanza EC2 per connetterti alle istanze utilizzando Secure Shell (SSH) senza la necessità di condividere e gestire chiavi SSH.
- Utilizza AWS Systems Manager Session Manager per accedere alle istanze in remoto anziché aprire porte SSH o RDP in entrata e gestire coppie di chiavi.
- Utilizza AWS Systems Manager Run Command per automatizzare attività amministrative comuni che non dovranno così connettersi alle istanze.
- [Istanze Windows] Molti dei ruoli del sistema operativo Windows e delle applicazioni aziendali Microsoft offrono anche funzionalità avanzate come le restrizioni dell'intervallo di indirizzi IP in IIS, i criteri di TCP/IP filtro in Microsoft SQL Server e i criteri di filtro delle connessioni in Microsoft

Exchange. La funzionalità di restrizione di rete all'interno del livello dell'applicazione può fornire ulteriori livelli di difesa per i server applicazioni aziendali critici.

Amazon VPC supporta controlli di sicurezza di rete aggiuntivi, come gateway, server proxy e opzioni di monitoraggio della rete. Per ulteriori informazioni, consulta Controllo del traffico di rete nella Guida per l'utente di Amazon VPC.

Resilienza in Amazon EC2

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo.

Se occorre replicare i dati o le applicazioni su distanze geografiche più ampie, utilizza AWS Local Zones. Una zona AWS locale è un'estensione di una AWS regione situata in prossimità geografica degli utenti. Le zone locali hanno le loro connessioni a Internet e supportano Direct Connect. Come tutte le AWS Regioni, le AWS Local Zones sono completamente isolate dalle altre AWS Zone.

Se è necessario replicare i dati o le applicazioni in una zona AWS locale, si AWS consiglia di utilizzare una delle seguenti zone come zona di failover:

- Un'altra Local Zone
- Zona di disponibilità nella regione che non è la zona padre. È possibile utilizzare il describe-availability-zonescomando per visualizzare la zona principale.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, vedere AWS Global Infrastructure.

Oltre all'infrastruttura AWS globale, Amazon EC2 offre le seguenti funzionalità per supportare la resilienza dei dati:

- Copia AMIs tra regioni
- Copia di snapshot EBS tra regioni
- Automazione supportata da EBS AMIs con Amazon Data Lifecycle Manager
- Automazione degli snapshot EBS mediante Amazon Data Lifecycle Manager

- Mantenimento dell'integrità e della disponibilità del parco istanze mediante Amazon EC2 Auto Scaling
- Distribuzione del traffico in entrata tra più istanze in una singola zona di disponibilità o in più zone di disponibilità mediante Elastic Load Balancing.

Convalida della conformità per Amazon EC2

La nostra nuova esperienza AWS di iscrizione non è progettata per carichi di lavoro regolamentati. Se stai utilizzando la nostra nuova esperienza di AWS registrazione, ma desideri utilizzarla AWS per carichi di lavoro regolamentati, puoi iscriverti a AWS (avanzato) o attivare funzionalità avanzate per il tuo ambiente. AWS

Per sapere se un Servizio AWS rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program e scegli il programma di conformità che ti interessa. Per informazioni generali, vedere Programmi di AWS conformità Programmi di

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, vedere Scaricamento dei report in AWS Artifact .

La responsabilità dell'utente in materia di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità dell'utente in materia di conformità durante l'utilizzo Servizi AWS, consulta AWS la Documentazione sulla sicurezza.

Identity and Access Management per Amazon EC2

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 (accesso effettuato) e autorizzato (dispone di autorizzazioni) per utilizzare le risorse Amazon EC2. IAM è un programma Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Le tue credenziali di sicurezza ti identificano ai servizi in uso AWS e ti consentono di accedere alle AWS risorse, come le risorse Amazon EC2. Puoi utilizzare le caratteristiche di Amazon EC2 e IAM per consentire ad altri utenti, servizi e applicazioni di utilizzare le risorse Amazon EC2 senza condividere le credenziali di sicurezza. Puoi utilizzare IAM per controllare in che modo gli altri utenti utilizzano le risorse nelle tue Account AWS e puoi utilizzare i gruppi di sicurezza per controllare

l'accesso alle tue istanze Amazon EC2. Puoi decidere di consentire l'uso completo o limitato delle risorse Amazon EC2.

Se sei uno sviluppatore, puoi utilizzare i ruoli IAM per gestire le credenziali di sicurezza necessarie alle applicazioni eseguite sulle tue istanze EC2. Dopo aver associato un ruolo IAM all'istanza, le applicazioni in esecuzione sull'istanza possono recuperare le credenziali dal servizio di metadati di istanza (IMDS).

Per le best practice per proteggere le AWS risorse tramite IAM, consulta le best practice di sicurezza in IAM nella IAM User Guide.

Indice

- Identity-based politiche per Amazon EC2
- Policy di esempio da utilizzare all'API Amazon EC2
- Policy di esempio per controllare l'accesso alla console Amazon EC2
- AWS policy gestite per Amazon EC2
- Ruoli IAM per Amazon EC2

Identity-based politiche per Amazon EC2

Per impostazione predefinita, gli utenti non sono autorizzati a creare o modificare le risorse Amazon EC2 o a eseguire attività tramite l'API Amazon EC2, la console Amazon EC2 o la CLI. Per permettere agli utenti di creare o modificare le risorse ed eseguire le attività, devi creare policy IAM che concedano agli utenti l'autorizzazione a utilizzare specifiche risorse e operazioni API e quindi collegare tali policy agli utenti, gruppi o ruoli IAM che richiedono tali autorizzazioni.

Quando si collega una policy a un utente, un gruppo di utenti o un ruolo, viene concessa o rifiutata agli utenti l'autorizzazione per eseguire attività specificate sulle risorse specificate. Per ulteriori informazioni generali sulle policy IAM, consulta la sezione relativa a Policy e autorizzazioni in IAM nella Guida per l'utente IAM. Per ulteriori informazioni sulla gestione e creazione di policy IAM, consulta la sezione relativa alla gestione delle policy IAM.

Una policy IAM deve concedere o rifiutare le autorizzazioni necessarie per l'utilizzo di una o più operazioni Amazon EC2. Deve inoltre specificare le risorse che possono essere utilizzate con l'operazione, vale a dire tutte le risorse oppure, in alcuni casi, risorse specifiche. La policy può anche includere condizioni applicabili alla risorsa.

Per iniziare, puoi verificare se le policy AWS gestite per Amazon EC2 soddisfano le tue esigenze. Altrimenti, puoi creare delle policy personalizzate. Per ulteriori informazioni, consulta the section called "AWS politiche gestite".

Indice

- Sintassi delle policy
- Operazioni per Amazon EC2
- Autorizzazioni a livello di risorsa supportate per le operazioni API Amazon EC2
- Nome della risorsa Amazon (ARN) per Amazon EC2
- Chiavi di condizione per Amazon EC2
- Controllare l'accesso mediante l'accesso basato sugli attributi
- Concedere autorizzazioni a utenti, gruppi e ruoli
- Verificare che gli utenti dispongano delle autorizzazioni necessarie

Sintassi delle policy

Una policy IAM è un documento JSON costituito da una o più dichiarazioni. Ogni dichiarazione è strutturata come segue.

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

Una dichiarazione è costituita da diversi elementi:

- Effetto: l'elemento effect può essere `Allow` o `Deny`. Per impostazione predefinita, gli utenti non dispongono dell'autorizzazione per l'utilizzo di risorse e operazioni API, pertanto tutte le richieste

vengono rifiutate. Un permesso esplicito sostituisce l'impostazione predefinita. Un rifiuto esplicito sovrascrive tutti i consensi.

- Action (Operazione): l'elemento action corrisponde all'operazione API specifica per la quale si concede o si nega l'autorizzazione. Per informazioni su come specificare l'elemento action, consulta Operazioni per Amazon EC2.
- Resource (Risorsa): la risorsa che viene modificata dall'operazione. Alcune operazioni API di Amazon EC2 ti permettono di includere nella policy risorse specifiche che possono essere create o modificate dall'operazione. Specifica una risorsa utilizzando un nome della risorsa Amazon (ARN) o il carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse. Per ulteriori informazioni, consulta Autorizzazioni a livello di risorsa supportate per le operazioni API Amazon EC2.
- Condition: le condizioni sono facoltative. Possono essere utilizzate per controllare quando è in vigore una policy. Per ulteriori informazioni su come specificare le condizioni per Amazon EC2, consulta Chiavi di condizione per Amazon EC2.

Per ulteriori informazioni su requisiti per le policy, consulta Riferimento alle policy JSON IAM nella Guida per l'utente IAM. Per alcuni esempi di istruzioni di policy IAM per Amazon EC2, consulta Policy di esempio da utilizzare all'API Amazon EC2.

Operazioni per Amazon EC2

In una dichiarazione di policy IAM, è possibile specificare qualsiasi operazione API per qualsiasi servizio che supporta IAM. Per Amazon EC2, utilizza il seguente prefisso con il nome dell'operazione API: `ec2:`. Ad esempio: `ec2:RunInstances` ed `ec2:CreateImage`.

Per specificare più operazioni in una sola dichiarazione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": ["ec2:action1", "ec2:action2"]
```

Puoi anche specificare più operazioni tramite caratteri jolly. Ad esempio, puoi specificare tutte le operazioni il cui nome inizia con la parola "Describe" (Descrivi) come segue:

```
"Action": "ec2:Describe*"
```

> **Note**
>
> Attualmente, le operazioni API Amazon EC2 Describe* non supportano autorizzazioni a livello di risorsa. Per ulteriori informazioni sulle autorizzazioni a livello di risorsa per Amazon EC2, consulta Identity-based politiche per Amazon EC2.

Per specificare tutte le operazioni API Amazon EC2, utilizza il carattere jolly * come mostrato di seguito:

```
"Action": "ec2:*"
```

Per visualizzare un elenco di operazioni di Amazon EC2, consulta Operazioni definite da Amazon EC2 nella Service Authorization Reference.

Autorizzazioni a livello di risorsa supportate per le operazioni API Amazon EC2

Resource-level le autorizzazioni si riferiscono alla capacità di specificare su quali risorse gli utenti sono autorizzati a eseguire azioni. Amazon EC2 supporta parzialmente le autorizzazioni a livello di risorsa. Ciò significa che per determinate operazioni di Amazon EC2, puoi controllare se gli utenti sono autorizzati a utilizzare tali operazioni in base a condizioni che devono essere soddisfatte o a specifiche risorse che gli utenti sono autorizzati a utilizzare. Ad esempio, puoi concedere agli utenti le autorizzazioni per avviare le istanze, ma solo di un determinato tipo e solo utilizzando un AMI specifico.

Per specificare una risorsa nella dichiarazione della policy IAM, si utilizza il suo nome della risorsa Amazon (ARN). Per ulteriori informazioni su come specificare il valore ARN, consulta Nome della risorsa Amazon (ARN) per Amazon EC2. Se l'operazione API non supporta gli ARN individuali, devi utilizzare il carattere jolly (*) per specificare che tutte le risorse possono essere interessate dall'operazione.

Per visualizzare le tabelle che identificano quali operazioni API Amazon EC2 supportano le autorizzazioni a livello di risorse e le chiavi di condizione e gli ARN che è possibile utilizzare in una policy, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

Occorre ricordare che è possibile applicare autorizzazioni a livello di risorsa basate su tag nelle policy IAM utilizzate per la maggior parte delle operazioni API Amazon EC2. In questo modo è possibile controllare meglio le risorse che un utente può creare, modificare o utilizzare. Per ulteriori

informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag Amazon EC2 per le risorse durante la creazione.

Nome della risorsa Amazon (ARN) per Amazon EC2

Ogni dichiarazione di policy IAM si applica alle risorse specificate utilizzando i relativi ARN.

Un ARN presenta la seguente sintassi generale:

```
arn:aws:[service]:[region]:[account-id]:resourceType/resourcePath
```

service

Il servizio (ad esempio `ec2`).

Regione

La regione per la risorsa (ad esempio `us-east-1`).

account-id

L'ID AWS dell'account, senza trattini (ad esempio,). `123456789012`

resourceType

Il tipo di risorsa (ad esempio `instance`).

resourcePath

Un percorso che identifica la risorsa. Nei percorsi puoi utilizzare il carattere jolly *.

Ad esempio, nella tua dichiarazione puoi specificare una determinata istanza (`i-1234567890abcdef0`) utilizzando il relativo ARN come segue:

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

Puoi specificare tutte le istanze appartenenti a un determinato account utilizzando il carattere jolly * come segue:

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Puoi anche specificare tutte le risorse Amazon EC2 appartenenti a un determinato account utilizzando il carattere jolly * come segue:

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:*"
```

Per specificare tutte le risorse o se una determinata operazione API non supporta gli ARN, utilizza il carattere jolly * nell'elemento `Resource` come segue:

```
"Resource": "*"
```

Molte operazioni API di Amazon EC2 coinvolgono più risorse. Ad esempio, `AttachVolume` collega un volume Amazon EBS a un'istanza, pertanto un utente dovrà disporre delle autorizzazioni per utilizzare il volume e l'istanza. Per specificare più risorse in una sola dichiarazione, separa i relativi ARN con una virgola come mostrato di seguito.

```
"Resource": ["arn1", "arn2"]
```

Per un elenco di ARN per le risorse Amazon EC2, consulta Tipi di risorse definiti da Amazon EC2.

Chiavi di condizione per Amazon EC2

In una dichiarazione di policy, puoi specificare facoltativamente le condizioni che controllano quando questa è in vigore. Ogni condizione contiene una o più coppie chiave/valore. Le chiavi di condizione non distinguono tra maiuscole e minuscole. Abbiamo definito chiavi di condizione AWS globali, oltre a chiavi di condizione aggiuntive specifiche del servizio.

Per un elenco di chiavi di condizione specifiche del servizio per Amazon EC2, consulta Chiavi di condizione per Amazon EC2. Amazon EC2 implementa anche le chiavi di condizione globali. AWS Per ulteriori informazioni, consulta la pagina relativa alle informazioni disponibili in tutte le richieste nella Guida per l'utente di IAM.

Tutte le operazioni Amazon EC2 supportano le chiavi di condizione `aws:RequestedRegion` e `ec2:Region`. Per ulteriori informazioni, consulta Esempio: limitazione dell'accesso a una regione specifica.

Per utilizzare una chiave di condizione nella policy IAM, utilizzare l'istruzione `Condition`. Ad esempio, la policy seguente concede agli utenti l'autorizzazione per aggiungere ed eliminare regole in entrata e in uscita per qualsiasi gruppo di sicurezza. Utilizza la chiave di condizione `ec2:Vpc` per specificare che queste azioni possono essere eseguite solo su gruppi di sicurezza in un VPC specifico.

JSON

```
{
"Version":"2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupEgress"],
     "Resource": "arn:aws:ec2:us-east-1:111122223333:security-group/*",
      "Condition": {
        "StringEquals": {
          "ec2:Vpc": "arn:aws:ec2:us-east-1:111122223333:vpc/
vpc-11223344556677889"
        }
      }
    }
  ]
}
```

Se specifichi più condizioni o più chiavi in una sola condizione le valutiamo utilizzando un'operazione AND logica. Se specifichi una sola condizione con più valori per una sola chiave, valutiamo la condizione utilizzando un'operazione OR logica. Affinché le autorizzazioni vengano concesse, tutte le condizioni devono essere soddisfatte.

Puoi anche utilizzare i segnaposto quando specifichi le condizioni. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

> **Important**
>
> Molte chiavi di condizione sono specifiche di una risorsa e alcune operazioni API utilizzano più risorse. Se scrivi una policy con una chiave di condizione, utilizza l'elemento `Resource` della dichiarazione per specificare la risorsa a cui viene applicata la chiave di condizione. In caso contrario, la policy potrebbe impedire agli utenti di eseguire operazioni perché il controllo della condizione ha esito negativo per le risorse alle quali non viene applicata la chiave di condizione. Se non vuoi specificare una risorsa oppure se hai scritto l'elemento `Action` della policy in modo da includere più operazioni API, devi utilizzare il tipo di condizione

`...IfExists` per assicurarti che la chiave di condizione venga ignorata per le risorse che non la utilizzano. Per ulteriori informazioni, consulta... IfExists Condizioni nella Guida per l'utente IAM.

Chiavi di condizione

- EC2: attributo chiave di condizione
- EC2: ResourceID chiavi di condizione
- ec2: ARN SourceInstance chiave di condizione

EC2: attributo chiave di condizione

La chiave di condizione `ec2:Attribute` può essere utilizzata per le condizioni che filtrano l'accesso da un attributo di una risorsa.

Questa chiave di condizione supporta solo proprietà di tipo di dati primitivo (come stringhe o numeri interi) o AttributeValue oggetti complessi che contengono solo una proprietà Value (come la Descrizione o ImdsSupport gli oggetti dell'azione API). ModifyImageAttribute La chiave di condizione non può essere utilizzata con oggetti complessi che contengono più proprietà, come l'LaunchPermissionoggetto di. ModifyImageAttribute

Ad esempio, la seguente policy utilizza la chiave di `ec2:Attribute/Description` condizione per filtrare l'accesso in base all'oggetto Description complesso dell'azione ModifyImageAttribute API. La chiave di condizione consente solo le richieste che modificano la descrizione di un'immagine a `Production` o `Development`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute/Description": [
```

```
            "Production",
            "Development"
          ]
        }
      }
    }
  ]
}
```

La seguente policy di esempio utilizza la chiave di `ec2:Attribute` condizione per filtrare l'accesso in base alla proprietà primitiva Attribute dell'azione ModifyImageAttribute API. La chiave di condizione respinge tutte le richieste che modificano la descrizione di un'immagine.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute": "Description"
        }
      }
    }
  ]
}
```

EC2: ResourceID chiavi di condizione

Quando si utilizza quanto segue`ec2:ResourceID`chiavi di condizione con le azioni API specificate, il valore della chiave di condizione viene utilizzato per specificare la risorsa risultante creata dall'azione API.`ec2:ResourceID`le chiavi di condizione non possono essere utilizzate per specificare una risorsa di origine specificata nella richiesta API. Se si utilizza uno dei seguenti`ec2:ResourceID`condition keys con un'API specificata, quindi devi sempre specificare la wildcard (*). Se si specifica un valore diverso, la condizione si risolve sempre in * durante il runtime.

Ad esempio, per utilizzare la chiave di `ec2:ImageId` condizione con l'CopyImageAPI, è necessario specificare la chiave di condizione come segue:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:ImageID": "*"
        }
      }
    }
  ]
}
```

Ti consigliamo di evitare l'uso di queste chiavi di condizione con queste azioni API:

- `ec2:DhcpOptionsID` – `CreateDhcpOptions`
- `ec2:ImageID`: `CopyImage`, `CreateImage`, `ImportImage` e `RegisterImage`
- `ec2:InstanceID`: `RunInstances` e `ImportInstance`
- `ec2:InternetGatewayID` – `CreateInternetGateway`
- `ec2:NetworkAclID` – `CreateNetworkAcl`
- `ec2:NetworkInterfaceID` – `CreateNetworkInterface`
- `ec2:PlacementGroupName` – `CreatePlacementGroup`
- `ec2:RouteTableID` – `CreateRouteTable`
- `ec2:SecurityGroupID` – `CreateSecurityGroup`
- `ec2:SnapshotID`: `CopySnapshot`, `CreateSnapshot`, `CreateSnapshots` e `ImportSnapshots`
- `ec2:SubnetID` – `CreateSubnet`
- `ec2:VolumeID`: `CreateVolume` e `ImportVolume`

- `ec2:VpcID` – `CreateVpc`
- `ec2:VpcPeeringConnectionID` – `CreateVpcPeeringConnection`

Per filtrare l'accesso in base a ID di risorse specifici, ti consigliamo di usare l'elemento della policy `Resource`, come segue.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-01234567890abcdef"
    }
  ]
}
```

ec2: ARN SourceInstance chiave di condizione

Usa `ec2:SourceInstanceARN` per specificare l'ARN dell'istanza in base alla quale è stata effettuata una richiesta. Si tratta di una chiave di condizione globale AWS, il che significa che puoi utilizzarla con servizi diversi da Amazon EC2. Per un esempio di policy, consulta Esempio: consenti a un'istanza specifica di visualizzare le risorse in altre AWS services.

Controllare l'accesso mediante l'accesso basato sugli attributi

Quando crei una policy IAM che concede agli utenti l'autorizzazione a utilizzare le risorse EC2, puoi includere informazioni sui tag nell'elemento `Condition` della policy per controllare l'accesso in base ai tag. Questo è noto come controllo degli accessi basato su attributi (ABAC). Il controllo ABAC fornisce un miglior controllo su quali risorse possono essere modificate, utilizzate o eliminate da un utente. Per ulteriori informazioni, consulta Che cos'è ABAC per AWS?

Ad esempio, è possibile creare una policy che consente agli utenti di terminare un'istanza ma che neghi l'operazione se l'istanza presenta il tag `environment=production`. A tale scopo, è possibile utilizzare la chiave di condizione `aws:ResourceTag` per consentire o negare l'accesso alla risorsa in base ai tag collegati alla risorsa.

```
"StringEquals": { "aws:ResourceTag/environment": "production" }
```

Per sapere se un'operazione API Amazon EC2 supporta il controllo degli accessi utilizzando la chiave di condizione `aws:ResourceTag`, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2. Tieni a mente che le operazioni `Describe` non supportano le autorizzazioni a livello di risorsa, pertanto è necessario specificarle in una dichiarazione separata senza condizioni.

Per esempi di policy IAM, consulta Policy di esempio da utilizzare all'API Amazon EC2.

Se consenti o neghi a un utente l'accesso a risorse in base ai tag, devi considerare esplicitamente di negare agli utenti la possibilità di aggiungere o rimuovere tali tag dalle stesse risorse. In caso contrario, un utente può eludere le restrizioni e ottenere l'accesso a una risorsa modificandone i tag.

Concedere autorizzazioni a utenti, gruppi e ruoli

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- 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 Create a role for a third-party identity provider (federation) della Guida per l'utente IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina Create a role for an IAM user della Guida per l'utente IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente IAM.

Verificare che gli utenti dispongano delle autorizzazioni necessarie

Dopo aver creato una policy IAM, prima di metterla in produzione, ti consigliamo di verificare se vengono concesse agli utenti le autorizzazioni per l'utilizzo di specifiche risorse e operazioni API necessarie.

In primo luogo, crea un utente a scopo di test e collega la policy IAM creata all'utente del test. In seguito, effettua una richiesta come utente di test.

Se l'operazione Amazon EC2 di cui stai eseguendo il test crea o modifica una risorsa, devi effettuare la richiesta utilizzando il parametro `DryRun` (o eseguire il comando della AWS CLI con l'opzione `--dry-run`). In questo caso, la chiamata completa la verifica dell'autorizzazione, ma non completa l'operazione. Ad esempio, puoi controllare se l'utente è in grado di interrompere una determinata istanza senza effettivamente terminarla. Se l'utente del test dispone delle autorizzazioni necessarie, la richiesta restituisce `DryRunOperation`, altrimenti restituisce `UnauthorizedOperation`.

Se la policy non concede all'utente le autorizzazioni previste oppure è eccessivamente permissiva, puoi modificarla in base alle esigenze e ripetere il test fino a ottenere i risultati desiderati.

> **Important**
>
> La propagazione delle modifiche alla policy e la loro validità potrebbe richiedere alcuni minuti. Ti consigliamo quindi di attendere 5 minuti prima di effettuare il test degli aggiornamenti delle policy.

Se una verifica dell'autorizzazione ha esito negativo, la richiesta restituisce un messaggio codificato con informazioni di diagnostica. Il messaggio può essere decodificato tramite l'operazione `DecodeAuthorizationMessage`. Per ulteriori informazioni, consulta DecodeAuthorizationMessage le sezioni Servizio di token di sicurezza AWS API Reference e https://docs.aws.amazon.com/cli/latest/reference/sts/decode-authorization-message.html decode-authorization-message.

Policy di esempio da utilizzare all'API Amazon EC2

È possibile utilizzare le policy IAM per concedere agli utenti le autorizzazioni richieste per utilizzare Amazon EC2. Per istruzioni dettagliate, consulta Creazione di politiche IAM nella Guida per l'utente IAM.

I seguenti esempi mostrano le dichiarazioni di policy che è possibile utilizzare per concedere le autorizzazioni agli utenti per utilizzare Amazon EC2. Queste politiche sono progettate per le richieste effettuate utilizzando AWS CLI o un AWS SDK. Negli esempi seguenti, sostituisci ciascuno *`user input placeholder`* con le tue informazioni.

Esempi

- Esempio: Read-only accesso
- Esempio: limitazione dell'accesso a una regione specifica
- Utilizzo delle istanze
- Istanze di avvio () RunInstances
- Utilizzo delle Istanze spot
- Esempio: utilizzo delle Istanze riservate
- Esempio: aggiunta di tag alle risorse
- Esempio: utilizzo dei ruoli IAM
- Esempio: utilizzo delle tabelle di routing
- Esempio: consenti a un'istanza specifica di visualizzare le risorse in altre AWS services
- Esempio: utilizzo dei modelli di avvio
- Utilizzo dei metadati delle istanze
- Lavora con volumi e snapshot Amazon EBS

Per le policy di esempio da utilizzare nella console Amazon EC2, consultare Policy di esempio per controllare l'accesso alla console Amazon EC2.

Esempio: Read-only accesso

La policy seguente concede agli utenti le autorizzazioni per utilizzare tutte le operazioni dell'API Amazon EC2 i cui nomi iniziano con `Describe`. L'elemento `Resource` utilizza un carattere jolly per indicare che tutti gli utenti possono specificare tutte le risorse con queste operazioni dell'API. Il carattere jolly * è necessario inoltre nei casi in cui l'operazione dell'API non supporta le autorizzazioni a livello di risorsa. Per ulteriori informazioni sugli ARN che è possibile utilizzare con le operazioni API Amazon EC2, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

Per impostazione predefinita, agli utenti non viene concessa l'autorizzazione per eseguire le operazioni dell'API sulle risorse (a meno che un'altra istruzione non conceda loro l'autorizzazione corrispondente).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    }
   ]
}
```

Esempio: limitazione dell'accesso a una regione specifica

La policy seguente nega agli utenti le autorizzazioni per utilizzare tutte le operazioni dell'API Amazon EC2, a meno che la regione sia Europa (Francoforte). Utilizza la chiave di condizione globale `aws:RequestedRegion`, che è supportato da tutte le operazioni API di Amazon EC2.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "eu-central-1"
        }
      }
    }
  ]
}
```

In alternativa, è possibile utilizzare la chiave di condizione `ec2:Region`, specifica per Amazon EC2 ed è supportata da tutte le operazioni API di Amazon EC2.

JSON

```
{
  "Version":"2012-10-17",
```

```
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "eu-central-1"
        }
      }
    }
  ]
}
```

Utilizzo delle istanze

Esempi

- Esempio: descrizione, avvio, arresto e terminazione di tutte le istanze
- Esempio: descrizione di tutte le istanze e arresto, avvio e terminazione soltanto di determinate istanze

Esempio: descrizione, avvio, arresto e terminazione di tutte le istanze

La policy seguente concede agli utenti le autorizzazioni per utilizzare le operazioni dell'API specificate nell'elemento `Action`. L'elemento `Resource` utilizza un carattere jolly * per indicare che tutti gli utenti possono specificare tutte le risorse con queste operazioni dell'API. Il carattere jolly * è necessario inoltre nei casi in cui l'operazione dell'API non supporta le autorizzazioni a livello di risorsa. Per ulteriori informazioni sugli ARN che è possibile utilizzare con le operazioni API Amazon EC2, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

Gli utenti non dispongono dell'autorizzazione per utilizzare altre operazioni dell'API (a meno che un'altra istruzione non conceda loro l'autorizzazione corrispondente) perché, per impostazione predefinita, agli utenti non viene concessa l'autorizzazione per utilizzare le operazioni dell'API.

JSON

```
{
   "Version":"2012-10-17",
```

```
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "*"
    }
   ]
}
```

Esempio: descrizione di tutte le istanze e arresto, avvio e terminazione soltanto di determinate istanze

La policy seguente consente agli utenti di descrivere tutte le istanze, di avviare e arrestare soltanto le istanze i-1234567890abcdef0 e i-0598c7d356eba48d7 e di terminare soltanto le istanze in della regione `us-east-1` con il tag di risorsa "`purpose=test`".

La prima istruzione utilizza il carattere jolly * per l'elemento `Resource` per indicare che gli utenti possono specificare tutte le risorse con questa operazione; in questo caso, possono elencare tutte le istanze. Il carattere jolly * è necessario inoltre nei casi in cui l'operazione dell'API non supporta le autorizzazioni a livello di risorsa (in questo caso, `ec2:DescribeInstances`). Per ulteriori informazioni sugli ARN che è possibile utilizzare con le operazioni API Amazon EC2, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

La seconda istruzione utilizza le autorizzazioni a livello di risorsa per le operazioni `StopInstances` e `StartInstances`. Le istanze specifiche sono indicate dai relativi ARN nell'elemento `Resource`.

La terza dichiarazione consente agli utenti di chiudere tutte le istanze nella `us-east-1` regione che appartengono all' AWS account specificato, ma solo se l'istanza ha il tag. `"purpose=test"` L'elemento `Condition` qualifica l'istruzione della policy applicata.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/i-1234567890abcdef0",
        "arn:aws:ec2:us-east-1:111122223333:instance/i-0598c7d356eba48d7"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/purpose": "test"
         }
      }
   }

   ]
}
```

Istanze di avvio () RunInstances

L'azione RunInstances API avvia una o più On-Demand istanze o una o più istanze Spot. `RunInstances`richiede un'AMI e crea un'istanza. Gli utenti possono specificare nella richiesta una coppia di chiavi e un gruppo di sicurezza. L'avvio in un VPC richiede una sottorete e crea un'interfaccia di rete. L'avvio da un' EBS-backedAMI Amazon crea un volume. Pertanto, gli

utenti devono disporre delle autorizzazioni per utilizzare queste risorse Amazon EC2. Puoi creare un'istruzione della policy che richiede agli utenti di specificare un parametro facoltativo su `RunInstances` o limitare l'accesso degli utenti a determinati valori dei parametri.

Per ulteriori informazioni sulle autorizzazioni a livello di risorse richieste per avviare un'istanza, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

Per impostazione predefinita, gli utenti non dispongono delle autorizzazioni per descrivere, avviare, arrestare o terminare le istanze risultanti. Un modo per concedere agli utenti l'autorizzazione per gestire le istanze risultanti, consiste nel creare un tag specifico per ciascuna istanza e nel creare quindi un'istruzione che consenta loro di gestire le istanze con tale tag. Per ulteriori informazioni, consulta Utilizzo delle istanze.

Resources

- AMI
- Tipi di istanza
- Sottoreti
- Volumi EBS
- Tag
- Tag in un modello di avvio
- GPU elastiche
- Modelli di avvio

AMI

La policy seguente consente gli utenti di avviare le istanze soltanto tramite le AMI specificate, `ami-9e1670f7` e `ami-45cf5c3c`. Gli utenti non possono avviare un'istanza con altre AMI (a meno che un'altra istruzione non conceda loro l'autorizzazione corrispondente).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
```

```
      "Resource": [
        "arn:aws:ec2:us-east-1::image/ami-9e1670f7",
        "arn:aws:ec2:us-east-1::image/ami-45cf5c3c",
        "arn:aws:ec2:us-east-1:111122223333:instance/*",
        "arn:aws:ec2:us-east-1:111122223333:volume/*",
        "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
        "arn:aws:ec2:us-east-1:111122223333:security-group/*",
        "arn:aws:ec2:us-east-1:111122223333:subnet/*",
        "arn:aws:ec2:us-east-1:111122223333:network-interface/*"
      ]
    }
   ]
}
```

In alternativa, la policy seguente consente agli utenti di avviare le istanze da tutte le AMI di proprietà di Amazon o di determinati partner sicuri e verificati. L'elemento `Condition` della prima istruzione verifica se `ec2:Owner` è `amazon`. Gli utenti non possono avviare un'istanza con altre AMI (a meno che un'altra istruzione non conceda loro l'autorizzazione corrispondente).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
         {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:Owner": "amazon"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:instance/*",
```

```
            "arn:aws:ec2:us-east-1:111122223333:subnet/*",
            "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
            "arn:aws:ec2:us-east-1:111122223333:security-group/*"
            ]
        }
    ]
}
```

Tipi di istanza

La policy seguente consente agli utenti di avviare le istanze soltanto tramite il tipo di istanza `t2.micro` o `t2.small` per consentire di tenere sotto controllo i costi. Gli utenti non possono avviare istanze di dimensioni maggiori perché l'elemento `Condition` della prima istruzione verifica se `ec2:InstanceType` è `t2.micro` o `t2.small`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
```

```
            "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
            "arn:aws:ec2:us-east-1:111122223333:security-group/*"
            ]
        }
    ]
}
```

In alternativa, puoi creare una policy che nega agli utenti le autorizzazioni per avviare le istanze a eccezione dei tipi di istanza `t2.micro` e `t2.small`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
        {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringNotEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:instance/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:volume/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*"
         ]
      }
```

```
    ]
}
```

Sottoreti

La policy seguente consente agli utenti di avviare le istanze soltanto tramite la sottorete `subnet-12345678` specificata. Il gruppo non può avviare le istanze in altre sottoreti (a meno che un'altra istruzione non conceda agli utenti l'autorizzazione corrispondente).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:subnet/subnet-12345678",
        "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
        "arn:aws:ec2:us-east-1:111122223333:instance/*",
        "arn:aws:ec2:us-east-1:111122223333:volume/*",
        "arn:aws:ec2:us-east-1::image/ami-*",
        "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
        "arn:aws:ec2:us-east-1:111122223333:security-group/*"
      ]
    }
   ]
}
```

In alternativa, puoi creare una policy che rifiuti agli utenti le autorizzazioni per avviare le istanze nelle altre sottoreti. Questa istruzione rifiuta l'autorizzazione per la creazione di un'interfaccia di rete, tranne se viene specificata la sottorete `subnet-12345678`. Questa negazione sostituisce le altre policy create per consentire l'avvio delle istanze in altre sottoreti.

JSON

```
{
   "Version":"2012-10-17",
```

```
   "Statement": [
         {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*"
      ],
      "Condition": {
         "ArnNotEquals": {
            "ec2:Subnet": "arn:aws:ec2:us-east-1:111122223333:subnet/
subnet-12345678"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:instance/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:volume/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*"
         ]
      }
   ]
}
```

Volumi EBS

La policy seguente consente agli utenti di avviare le istanze soltanto se i volumi EBS dell'istanza sono crittografati. Per assicurarsi che il volume root sia crittografato, gli utenti devono avviare un'istanza da un'AMI creata con snapshot crittografate. Anche gli altri eventuali volumi collegati dagli utenti all'istanza durante l'avvio devono essere crittografati.

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
                {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        }
    ]
}
```

Tag

Tag di istanze durante la creazione

La policy seguente consente agli utenti di avviare le istanze e di aggiungervi dei tag durante la creazione. Per le operazioni di creazione delle risorse in cui vengono applicati i tag, gli utenti devono disporre delle autorizzazioni per utilizzare l'operazione `CreateTags`. La seconda istruzione utilizza la chiave di condizione `ec2:CreateAction` per consentire agli utenti di creare i tag soltanto nel contesto di `RunInstances` e soltanto per le istanze. Tramite la richiesta `RunInstances`, gli utenti non possono aggiungere tag alle risorse esistenti e ai volumi.

Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag Amazon EC2 per le risorse durante la creazione.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Tag di istanze e volumi durante la creazione con tag specifici

La policy seguente include la chiave di condizione `aws:RequestTag` che richiede agli utenti di applicare tag alle istanze e ai volumi creati da `RunInstances` con i tag `environment=production` e `purpose=webserver`. Se gli utenti non indicano questi tag specifici, o se non specificano nessun tag, la richiesta non riesce.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
```

```
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:us-east-1::image/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:us-east-1:111122223333:volume/*",
          "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "aws:RequestTag/environment": "production" ,
            "aws:RequestTag/purpose": "webserver"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
            "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Tag di istanze e volumi durante la creazione con almeno un tag specifico

La policy seguente utilizza il modificatore `ForAnyValue` sulla condizione `aws:TagKeys` per indicare che occorre specificare almeno un tag nella richiesta e che deve contenere la chiave `environment` o `webserver`. I tag devono essere applicati alle istanze e ai volumi. È possibile specificare nella richiesta qualsiasi valore di tag.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:us-east-1::image/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:us-east-1:111122223333:volume/*",
          "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
          "ForAnyValue:StringEquals": {
              "aws:TagKeys": ["environment","webserver"]
          }
       }
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
          "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
          "StringEquals": {
              "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Se vengono applicati tag alle istanze durante la creazione, è necessario applicare un tag specifico

Nella policy seguente non è necessario che gli utenti specifichino i tag nella richiesta, ma se lo fanno, i tag devono essere di tipo `purpose=test`. Non sono consentiti altri tag. Gli utenti possono applicare i tag alle risorse compatibili con l'applicazione dei tag nella richiesta `RunInstances`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "RunInstances"
```

```
            },
            "ForAllValues:StringEquals": {
                "aws:TagKeys": "purpose"
            }
        }
    }
  ]
}
```

Per impedire a chiunque abbia chiamato tag on create for RunInstances

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Consenti solo tag specifici per spot-instances-request. L'incoerenza numero 2 entra in gioco qui. In circostanze normali, se non si specifica alcun tag, il risultato è che non viene autenticato. Nel caso di spot-instances-request, questa policy non viene valutata se non ci sono tag spot-instances-request, quindi una richiesta Spot on Run senza tag ha esito positivo.

Tag in un modello di avvio

Nell'esempio seguente, gli utenti possono avviare le istanze, ma solo tramite un modello di avvio specifico (`lt-09477bcd97b0d310e`). La chiave di condizione `ec2:IsLaunchTemplateResource` impedisce agli utenti di sovrascrivere le risorse specificate nel modello di avvio. La seconda parte dell'istruzione consente agli utenti di assegnare tag alle istanze al momento della creazione; questa parte dell'istruzione è necessaria se sono stati specificati dei tag per l'istanza nel modello di avvio.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/lt-09477bcd97b0d310e"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
```

```
        }
      }
    ]
}
```

GPU elastiche

Nella policy seguente, gli utenti possono avviare un'istanza e specificare una GPU elastica da collegare all'istanza. Gli utenti possono avviare le istanze in qualsiasi regione, ma possono collegare una GPU elastica durante l'avvio soltanto nella regione `us-east-2`.

La chiave di condizione `ec2:ElasticGpuType` garantisce che le istanze utilizzino il tipo di GPU elastica `eg1.medium` o `eg1.large`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
             {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:111122223333:elastic-gpu/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-2",
                    "ec2:ElasticGpuType": [
                        "eg1.medium",
                        "eg1.large"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
```

```
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:111122223333:network-interface/*",
                "arn:aws:ec2:*:111122223333:instance/*",
                "arn:aws:ec2:*:111122223333:subnet/*",
                "arn:aws:ec2:*:111122223333:volume/*",
                "arn:aws:ec2:*:111122223333:key-pair/*",
                "arn:aws:ec2:*:111122223333:security-group/*"
            ]
        }
    ]
}
```

Modelli di avvio

Nell'esempio seguente, gli utenti possono avviare le istanze, ma solo tramite un modello di avvio specifico (`lt-09477bcd97b0d310e`). Gli utenti possono sovrascrivere i parametri nel modello di avvio specificandolo nell'operazione `RunInstances`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/lt-09477bcd97b0d310e"
          }
       }
    }
  ]
}
```

In questo esempio, gli utenti possono avviare le istanze solo se utilizzano un modello di avvio specifico. La policy utilizza la chiave di condizione `ec2:IsLaunchTemplateResource` per impedire agli utenti di sovrascrivere qualsiasi ARN preesistente del modello di avvio.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

La policy di esempio seguente consente agli utenti di avviare le istanze, ma solo tramite un modello di avvio. Gli utenti non possono sovrascrivere i parametri di sottorete e interfaccia di rete della richiesta; tali parametri possono essere specificati soltanto nel modello di avvio. La prima parte dell'istruzione utilizza l'NotResourceelemento per consentire tutte le altre risorse tranne le sottoreti e le interfacce di rete. La seconda parte dell'istruzione consente le risorse di sottorete e interfaccia di rete, ma soltanto se provenienti dal modello di avvio.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": ["arn:aws:ec2:us-east-1:111122223333:subnet/*",
                      "arn:aws:ec2:us-east-1:111122223333:network-interface/*" ],
      "Condition": {
```

```
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          }
       }
    },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": ["arn:aws:ec2:us-east-1:111122223333:subnet/*",
                   "arn:aws:ec2:us-east-1:111122223333:network-interface/*" ],
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          },
          "Bool": {
            "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

L'esempio seguente consente agli utenti di avviare le istanze solo tramite un modello di avvio e solo se quest'ultimo dispone del tag `Purpose=Webservers`. Gli utenti non possono sovrascrivere nessuno dei parametri del modello di avvio nell'operazione `RunInstances`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
```

```
            },
            "Bool": {
                "ec2:IsLaunchTemplateResource": "true"
            }
        }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
      "Condition": {
       "StringEquals": {
           "aws:ResourceTag/Purpose": "Webservers"
        }
       }
     }
  ]
}
```

Utilizzo delle Istanze spot

È possibile utilizzare l' RunInstances azione per creare richieste di istanza Spot e contrassegnare le richieste di istanza Spot al momento della creazione. La risorsa da specificare RunInstances è`spot-instances-request`.

La risorsa `spot-instances-request` viene valutata nella policy IAM come segue:

- Se non contrassegni una richiesta di istanza Spot al momento della creazione, Amazon EC2 non valuta la `spot-instances-request` risorsa nella RunInstances dichiarazione.
- Se tagghi una richiesta di istanza Spot al momento della creazione, Amazon EC2 valuta la `spot-instances-request` risorsa contenuta nell'istruzione. RunInstances

Pertanto, per la risorsa `spot-instances-request`, alla policy IAM si applicano le seguenti regole:

- Se lo utilizzi RunInstances per creare una richiesta di istanza Spot e non intendi etichettare la richiesta di istanza Spot al momento della creazione, non è necessario consentire esplicitamente la `spot-instances-request` risorsa; la chiamata avrà esito positivo.

- Se lo utilizzi RunInstances per creare una richiesta di istanza Spot e intendi etichettare la richiesta di istanza Spot al momento della creazione, devi includere la `spot-instances-request` risorsa nell'istruzione RunInstances allow, altrimenti la chiamata avrà esito negativo.
- Se lo utilizzi RunInstances per creare una richiesta di istanza Spot e intendi contrassegnare la richiesta di istanza Spot al momento della creazione, devi specificare la `spot-instances-request` risorsa o il * carattere jolly nell'istruzione CreateTags allow, altrimenti la chiamata avrà esito negativo.

Puoi richiedere le istanze Spot utilizzando RunInstances o. RequestSpotInstances Il seguente esempio di policy IAM si applica solo quando si richiedono istanze Spot utilizzando. RunInstances

Esempio: richiedi istanze Spot utilizzando RunInstances

La seguente politica consente agli utenti di richiedere istanze Spot utilizzando l'azione RunInstances . La `spot-instances-request` risorsa, creata da RunInstances, richiede le istanze Spot.

> **Note**
>
> Da utilizzare RunInstances per creare richieste di istanze Spot, puoi ometterle `spot-instances-request` dall'`Resource`elenco se non intendi taggare le richieste di istanza Spot al momento della creazione. Questo perché Amazon EC2 non valuta la `spot-instances-request` risorsa nella RunInstances dichiarazione se la richiesta di istanza Spot non è contrassegnata al momento della creazione.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
```

```
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        }
    ]
}
```

⚠ Warning

NON SUPPORTATO — Esempio: negare agli utenti il permesso di richiedere istanze Spot utilizzando RunInstances

La seguente policy non è supportata per la risorsa `spot-instances-request`.

La seguente politica ha lo scopo di concedere agli utenti il permesso di avviare On-Demand istanze, ma negare agli utenti il permesso di richiedere istanze Spot. La `spot-instances-request` risorsa, creata da RunInstances, è la risorsa che richiede le istanze Spot. La seconda dichiarazione ha lo scopo di negare l' RunInstances azione per la `spot-instances-request` risorsa. Tuttavia, questa condizione non è supportata perché Amazon EC2 non valuta la `spot-instances-request` risorsa nella RunInstances dichiarazione se la richiesta dell'istanza Spot non è contrassegnata al momento della creazione.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
```

```
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequestsNOTSUPPORTEDDONOTUSE",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
        }
    ]
}
```

Esempio: tag di richieste di istanze spot durante la creazione

La seguente policy consente agli utenti di applicare un tag a tutte le risorse create durante l'avvio dell'istanza. La prima istruzione consente di RunInstances creare le risorse elencate. La `spot-instances-request` risorsa, creata da RunInstances, è la risorsa che richiede le istanze Spot. La seconda istruzione include il carattere jolly * per consentire a tutte le risorse l'applicazione di tag quando vengono create all'avvio dell'istanza.

> **Note**
>
> Se contrassegni una richiesta di istanza Spot al momento della creazione, Amazon EC2 valuta la `spot-instances-request` risorsa nella dichiarazione. RunInstances Pertanto, è necessario consentire esplicitamente alla `spot-instances-request` risorsa di eseguire l' RunInstances azione, altrimenti la chiamata avrà esito negativo.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Esempio: assegnazione di tag di diniego durante la creazione per richieste di istanze spot

La seguente policy nega agli utenti l'autorizzazione di applicare un tag alle risorse create durante l'avvio dell'istanza.

La prima istruzione consente di RunInstances creare le risorse elencate. La `spot-instances-request` risorsa, creata da RunInstances, è la risorsa che richiede le istanze Spot. La seconda istruzione include il carattere jolly * per negare a tutte le risorse l'applicazione di tag quando vengono create all'avvio dell'istanza. Se `spot-instances-request` o qualsiasi altra risorsa è contrassegnata in fase di creazione, la RunInstances chiamata avrà esito negativo.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenyTagResources",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Warning

NON SUPPORTATO - Esempio: autorizzazione per la creazione di una richiesta di istanza spot solo se è stato applicato un tag specifico

La seguente policy non è supportata per la risorsa `spot-instances-request`.

La seguente politica ha lo scopo di concedere RunInstances l'autorizzazione a creare una richiesta di istanza Spot solo se la richiesta è contrassegnata con un tag specifico.

La prima dichiarazione consente RunInstances di creare le risorse elencate.

La seconda istruzione intende concedere agli utenti l'autorizzazione a creare una richiesta di istanza spot solo se alla richiesta è applicato il tag `environment=production`. Se questa condizione viene applicata ad altre risorse create da RunInstances, l'assenza di tag genera un `Unauthenticated` errore. Tuttavia, se non viene specificato alcun tag per la richiesta di istanza Spot, Amazon EC2 non valuta la `spot-instances-request` risorsa nella RunInstances dichiarazione, il che comporta la creazione di richieste di istanza Spot senza tag da parte di. RunInstances

Nota che specificare un altro tag diverso da quello `environment=production` genera un `Unauthenticated` errore, perché se un utente tagga una richiesta di istanza Spot, Amazon EC2 valuta la `spot-instances-request` risorsa nella dichiarazione. RunInstances

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid":
 "RequestSpotInstancesOnlyIfTagIsEnvironmentProductionNOTSUPPORTEDDONOTUSE",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/
*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
```

```
            "Resource": "*"
        }

    ]
}
```

Esempio: diniego della creazione di una richiesta di istanza spot se ha un tag specifico applicato

La seguente politica nega RunInstances l'autorizzazione a creare una richiesta di istanza Spot se la richiesta è contrassegnata con. `environment=production`

La prima dichiarazione consente di RunInstances creare le risorse elencate.

La seconda istruzione nega agli utenti l'autorizzazione per creare una richiesta di istanza spot se la richiesta ha il tag `environment=production`. Se si specifica `environment=production` come tag, viene generato un errore `Unauthenticated`. Se si specificano altri tag o se non si specifica alcun tag, verrà creata una richiesta di istanza spot.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
```

```
        {
            "Sid": "DenySpotInstancesRequests",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Esempio: utilizzo delle Istanze riservate

La policy seguente fornisce agli utenti l'autorizzazione per visualizzare, modificare e acquistare le Istanze riservate nell'account.

Non è possibile impostare le autorizzazioni a livello di risorsa per singole Istanze riservate. Questa policy significa che gli utenti hanno accesso a tutte le Istanze riservate dell'account.

L'elemento `Resource` utilizza il carattere jolly * per indicare che gli utenti possono specificare tutte le risorse tramite questa operazione; in questo caso, possono elencare e modificare tutte le Istanze riservate nell'account. Possono inoltre acquistare le Istanze riservate con le credenziali dell'account. Il carattere jolly * è necessario inoltre nei casi in cui l'operazione dell'API non supporta le autorizzazioni a livello di risorsa.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
    }
   ]
}
```

Per consentire agli utenti di visualizzare e modificare le Istanze riservate nell'account, ma non di acquistare nuove Istanze riservate.

JSON

```
{
  "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    }
  ]
}
```

Esempio: aggiunta di tag alle risorse

La policy seguente consente agli utenti di utilizzare l'operazione `CreateTags` per applicare tag a un'istanza soltanto se il tag contiene la chiave `environment` e il valore `production`. Non sono consentiti altri tag e l'utente non può aggiungere tag ad altri tipi di risorse.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

La policy seguente consente agli utenti di assegnare tag a tutte le risorse compatibili con l'assegnazione di tag e che dispongono già di un tag con una chiave `owner` e un valore corrispondente al nome utente. Inoltre, gli utenti devono specificare nella richiesta un tag con la chiave `anycompany:environment-type` e un valore `test` o `prod`. Gli utenti possono specificare altri tag nella richiesta.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:RequestTag/anycompany:environment-type":
 ["test","prod"],
                    "aws:ResourceTag/owner": "${aws:username}"
                }
            }
        }
    ]
}
```

Puoi creare una policy IAM che consenta agli utenti di eliminare tag specifici per una risorsa. Ad esempio, la policy seguente consente agli utenti di eliminare i tag di un volume se le chiavi di tag specificate nella richiesta sono `environment` o `cost-center`. È possibile specificare qualsiasi valore per il tag, ma la chiave di tag deve corrispondere a una delle chiavi specificate.

> **Note**
>
> Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa. Gli utenti non necessitano delle autorizzazioni per utilizzare l'operazione `ec2:DeleteTags` per eliminare una risorsa con tag; necessitano soltanto delle autorizzazioni per effettuare l'operazione di eliminazione.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Allow",
      "Action": "ec2:DeleteTags",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment","cost-center"]
        }
      }
    }
  ]
}
```

Questa policy consente agli utenti di eliminare soltanto il tag `environment=prod` su qualsiasi risorsa e soltanto se la risorsa dispone già di un tag con una chiave `owner` e di un valore corrispondente al nome utente. Gli utenti non possono eliminare nessun altro tag di una risorsa.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "prod",
          "aws:ResourceTag/owner": "${aws:username}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment"]
        }
      }
    }
  ]
}
```

Esempio: utilizzo dei ruoli IAM

La policy seguente consente agli utenti di collegare, sostituire e scollegare un ruolo IAM dalle istanze che includono il tag `department=test`. Per la sostituzione o lo scollegamento di un ruolo IAM è necessario un ID di associazione, pertanto la policy concede agli utenti anche l'autorizzazione per utilizzare l'operazione `ec2:DescribeIamInstanceProfileAssociations`.

Gli utenti devono disporre dell'autorizzazione per utilizzare l'`iam:PassRole`azione per passare il ruolo all'istanza.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department":"test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeIamInstanceProfileAssociations",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::111122223333:role/DevTeam*"
    }
  ]
}
```

La policy seguente consente agli utenti di collegare o sostituire un ruolo IAM per qualsiasi istanza. Gli utenti possono collegare o sostituire soltanto i ruoli IAM il cui nome inizia con `TestRole-`. Per l'operazione `iam:PassRole`, assicurarsi di specificare il nome del ruolo IAM e non il profilo dell'istanza (se i nomi sono diversi). Per ulteriori informazioni, consulta Profili delle istanze.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIamInstanceProfile",
                "ec2:ReplaceIamInstanceProfileAssociation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeIamInstanceProfileAssociations",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/TestRole-*"
        }
    ]
}
```

Esempio: utilizzo delle tabelle di routing

La policy seguente consente agli utenti di aggiungere, rimuovere e sostituire gli instradamenti delle tabelle di routing associate soltanto al VPC `vpc-ec43eb89`. Per specificare un VPC per la chiave di condizione `ec2:Vpc`, devi specificare l'ARN completo del VPC.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute"
            ],
```

```
            "Resource": [
                "arn:aws:ec2:us-east-1:111122223333:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Vpc": "arn:aws:ec2:us-east-1:111122223333:vpc/vpc-
ec43eb89"
                }
            }
        }
    ]
}
```

Esempio: consenti a un'istanza specifica di visualizzare le risorse in altre AWS services

Di seguito è riportato un esempio di policy che è possibile collegare a un ruolo IAM. La policy consente a un'istanza di visualizzare le risorse in vari AWS servizi. Utilizza la chiave di condizione globale `ec2:SourceInstanceARN` per specificare che l'istanza da cui è stata creata la richiesta deve essere l'istanza `i-093452212644b0dd6`. Se lo stesso ruolo IAM è associato a un'altra istanza, l'altra istanza non può effettuare nessuna di queste operazioni.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes",
                "s3:ListAllMyBuckets",
                "dynamodb:ListTables",
                "rds:DescribeDBInstances"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "ArnEquals": {
                    "ec2:SourceInstanceARN": "arn:aws:ec2:us-
east-1:111122223333:instance/i-093452212644b0dd6"
```

```
                }
            }
        }
    ]
}
```

Esempio: utilizzo dei modelli di avvio

La policy seguente consente agli utenti di creare una versione del modello di avvio e di modificarne uno, ma solo nel caso di un modello di avvio specifico (`lt-09477bcd97b0d3abc`). Gli utenti non possono utilizzare altri modelli di lancio.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/
lt-09477bcd97b0d3abc"
    }
  ]
}
```

La policy seguente consente agli utenti di eliminare i modelli di avvio e la relativa versione, purché il modello di avvio disponga del tag `Purpose=Testing`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Action": [
```

```
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Testing"
        }
      }
    }
  ]
}
```

Utilizzo dei metadati delle istanze

Le policy seguenti assicurano che gli utenti possano recuperare i metadati delle istanze solo utilizzando Servizio di metadati dell'istanza Versione 2 (IMDSv2). Puoi combinare le quattro policy seguenti in un'unica policy con quattro istruzioni. Se vengono combinate in un'unica policy, questa può essere utilizzata come policy di controllo dei servizi (SCP). Può funzionare altrettanto bene come policy deny applicata a una policy IAM esistente (togliendo e limitando le autorizzazioni esistenti) o come policy di controllo dei servizi (SCP) applicata a livello globale a un account, a un'unità organizzativa o a un'intera organizzazione.

> **Note**
>
> Le seguenti politiche relative alle opzioni dei RunInstances metadati devono essere utilizzate insieme a una politica che fornisca le autorizzazioni principali con cui avviare un'istanza. RunInstances Se anche il principale non dispone RunInstances delle autorizzazioni, non sarà in grado di avviare un'istanza. Per ulteriori informazioni, consulta le policy Utilizzo delle istanze e Istanze di avvio () RunInstances.

> **Important**
>
> Se si utilizzano gruppi Auto Scaling e si deve richiedere l'uso di IMDSv2 su tutte le nuove istanze, i gruppi Auto Scaling devono utilizzare i modelli di avvio.
> Quando un gruppo Auto Scaling utilizza un modello di avvio, le `ec2:RunInstances` autorizzazioni del principal IAM vengono controllate quando viene creato un nuovo gruppo

Auto Scaling. Vengono inoltre controllati quando un gruppo Auto Scaling esistente viene aggiornato per utilizzare un nuovo modello di avvio o una nuova versione di un modello di avvio.
Le restrizioni sull'uso di IMDSv1 su principal IAM per `RunInstances` vengono verificate solo quando viene creato o aggiornato un gruppo Auto Scaling che utilizza un modello di avvio. Per un gruppo Auto Scaling configurato per l'utilizzo del modello di avvio `Latest` o `Default`, le autorizzazioni non vengono controllate quando viene creata una nuova versione del modello di avvio. Per controllare le autorizzazioni, è necessario configurare il gruppo Auto Scaling in modo da utilizzare una versione specifica del modello di avvio.

Per applicare l'uso di IMDSv2 su istanze lanciate dai gruppi Auto Scaling, sono necessari i seguenti passaggi aggiuntivi:

1. Disabilitare l'utilizzo delle configurazioni di avvio per tutti gli account dell'organizzazione utilizzando i limiti delle autorizzazioni IAM o le policy di controllo del servizio (SCP) per i nuovi principal creati. Per i principal IAM esistenti con autorizzazioni di gruppo Auto Scaling, aggiornare le policy associate con questa chiave di condizione. Per disabilitare l'utilizzo delle configurazioni di avvio, creare o modificare la policy IAM, il limite delle autorizzazioni o la relativa policy di controllo del servizio con la chiave di condizione `"autoscaling:LaunchConfigurationName"` con il valore specificato come `null`.
2. Per i nuovi modelli di avvio, configurare le opzioni dei metadati dell'istanza nel modello di avvio. Per i modelli di avvio esistenti, creare una nuova versione del modello di avvio e configurare le opzioni dei metadati dell'istanza nella nuova versione.
3. Nella policy che concede a qualsiasi principal l'autorizzazione per utilizzare un modello di avvio, limitare l'associazione di `$latest` e `$default` specificando `"autoscaling:LaunchTemplateVersionSpecified": "true"`. Limitando l'utilizzo a una versione specifica di un modello di avvio, è possibile assicurarsi che vengano avviate nuove istanze utilizzando la versione in cui sono configurate le opzioni dei metadati dell'istanza. Per ulteriori informazioni, consulta LaunchTemplateSpecification Amazon EC2 Auto Scaling API Reference, in particolare il parametro. `Version`
4. Per un gruppo Auto Scaling che utilizza una configurazione di avvio, sostituire la configurazione di avvio con un modello di avvio. Per ulteriori informazioni, consulta Migrate your Auto Scaling groups to launch templates nella Guida per l'utente di Amazon EC2 Auto Scaling.
5. Per un gruppo Auto Scaling che utilizza un modello di avvio, assicurarsi che utilizzi un nuovo modello di avvio con le opzioni di metadati dell'istanza configurate oppure utilizzi

una nuova versione del modello di avvio corrente con le opzioni dei metadati dell'istanza configurate. Per ulteriori informazioni, consulta update-auto-scaling-group.

Esempi

- Richiesta dell'uso di IMDSv2
- Come negare l'esclusione da IMDSv2
- Specificare limite massimo di hop
- Limitazione di chi può modificare le opzioni dei metadati dell'istanza
- Richiesta delle credenziali del ruolo da recuperare da IMDSv2

Richiesta dell'uso di IMDSv2

La seguente policy specifica che non è possibile chiamare l' RunInstances API a meno che l'istanza non richieda anche l'uso di IMDSv2 (indicato da). `"ec2:MetadataHttpTokens": "required"` Se non specifichi che l'istanza richiede IMDSv2, riceverai un errore quando chiami l'API. `UnauthorizedOperation` RunInstances

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
                {
            "Sid": "RequireImdsV2",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:MetadataHttpTokens": "required"
                }
            }
        }
    ]
}
```

Come negare l'esclusione da IMDSv2

La seguente policy specifica che non puoi chiamare l'API `ModifyInstanceMetadataOptions` e consentire l'opzione IMDSv1 o IMDSv2. Se chiami l'API `ModifyInstanceMetadataOptions`, l'attributo `HttpTokens` deve essere impostato su `required`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "DenyIMDSv1HttpTokensModification",
        "Effect": "Deny",
        "Action": "ec2:ModifyInstanceMetadataOptions",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:Attribute/HttpTokens": "required"
            },
            "Null": {
                "ec2:Attribute/HttpTokens": false
            }
        }
    }]
}
```

Specificare limite massimo di hop

La seguente politica specifica che non è possibile chiamare l' RunInstances API a meno che non si specifichi anche un limite di hop e che il limite di hop non può essere superiore a 3. Se non riesci a farlo, ricevi un `UnauthorizedOperation` errore quando chiami l' RunInstances API.

JSON

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

```
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "NumericGreaterThan": {
                    "ec2:MetadataHttpPutResponseHopLimit": "3"
                }
            }
        }
    ]
}
```

Limitazione di chi può modificare le opzioni dei metadati dell'istanza

Con la policy seguente, gli utenti con il ruolo `ec2-imds-admins` potranno apportare modifiche alle opzioni di metadati dell'istanza. Se un responsabile diverso dal `ec2-imds-admins` ruolo tenta di chiamare l' ModifyInstanceMetadataOptions API, riceverà un `Unauthorized0peration` errore. Questa dichiarazione potrebbe essere utilizzata per controllare l'uso dell' ModifyInstanceMetadataOptions API; attualmente non esistono controlli di accesso (condizioni) dettagliati per l'API. ModifyInstanceMetadataOptions

Richiesta delle credenziali del ruolo da recuperare da IMDSv2

La policy seguente specifica che se questa policy viene applicata a un ruolo e il ruolo viene assunto dal servizio EC2 e le credenziali risultanti vengono utilizzate per firmare una richiesta, la richiesta deve essere firmata dalle credenziali del ruolo EC2 recuperate da IMDSv2. In caso contrario, per tutte le relative chiamate all'API si verifica un errore `Unauthorized0peration`. Questo statement/policy può essere applicato in generale perché, se la richiesta non è firmata dalle credenziali del ruolo EC2, non ha alcun effetto.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
                {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
```

```
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

Lavora con volumi e snapshot Amazon EBS

Ad esempio, politiche per l'utilizzo di volumi e snapshot di Amazon EBS, consulta gli esempi di Identity-based policy per Amazon EBS.

Policy di esempio per controllare l'accesso alla console Amazon EC2

È possibile utilizzare le policy IAM per concedere agli utenti le autorizzazioni richieste per utilizzare Amazon EC2. Per istruzioni dettagliate, consulta Creazione di politiche IAM nella Guida per l'utente IAM.

La console utilizza operazioni API aggiuntive per le relative caratteristiche. Pertanto, queste policy potrebbero non funzionare come previsto. Ad esempio, un utente con l'autorizzazione per l'utilizzo solo dell'operazione API `DescribeVolumes` riscontrerà errori quando cerca di visualizzare i volumi nella console. In questa sezione sono descritte le policy che consentono agli utenti di utilizzare parti specifiche della console. Per ulteriori informazioni sulla creazione di policy per la console Amazon EC2, consulta il seguente post sul blog AWS sulla sicurezza: Granting Users Permission to Work in the Amazon EC2 Console.

I seguenti esempi mostrano le dichiarazioni di policy che è possibile utilizzare per concedere le autorizzazioni agli utenti per utilizzare Amazon EC2. Sostituisci ogni *`user input placeholder`* con le tue informazioni. Queste policy sono progettate per le richieste effettuate con Console di gestione AWS. La console Amazon EC2 potrebbe richiamare più azioni API per visualizzare una singola risorsa e ciò potrebbe non essere evidente finché l'utente non tenta di eseguire un'operazione e la console non visualizza un errore. Per ulteriori informazioni, consulta il seguente post sul blog AWS sulla sicurezza: Granting Users Permission to Work in the Amazon EC2 Console.

Esempi

- Esempio: accesso Read-only
- Esempio: utilizzo della procedura guidata per l'avvio dell'istanza EC2

- Esempio: utilizzo dei gruppi di sicurezza
- Esempio: utilizzo degli indirizzi IP elastici
- Esempio: utilizzo delle Istanze riservate

Per individuare le operazioni API necessarie per eseguire le attività nella console, puoi utilizzare un servizio che effettua log di chiamate, come AWS CloudTrail. Se la policy non concede l'autorizzazione per creare o modificare una risorse specifica, nella console viene visualizzato un messaggio codificato con informazioni di diagnostica. Puoi decodificare il messaggio utilizzando l'azione DecodeAuthorizationMessage API for o il comando AWS STShttps://docs.aws.amazon.com/cli/latest/reference/sts/decode-authorization-message.html decode-authorization-message nel. AWS CLI

Esempio: accesso Read-only

Per consentire agli utenti di visualizzare tutte le risorse nella console Amazon EC2, è possibile utilizzare la stessa policy impiegata nel seguente esempio: Esempio: Read-only accesso. Gli utenti non possono eseguire operazioni su queste risorse o creare nuove risorse a meno che un'altra istruzione conceda loro l'autorizzazione corrispondente.

Visualizzazione di istanze, AMI e snapshot

In alternativa, puoi concedere l'accesso in sola lettura a un sottoinsieme di risorse. A tale scopo, sostituisci il carattere jolly * nell'operazione API `ec2:Describe` con operazioni `ec2:Describe` specifiche per ciascuna risorsa. La seguente policy consente agli utenti di visualizzare tutte le istanze, AMI e snapshot nella console Amazon EC2. L'operazione `ec2:DescribeTags` consente agli utenti di visualizzare le AMI pubbliche. La console richiede le informazioni di tagging per visualizzare le AMI pubbliche. Tuttavia, puoi rimuovere questa operazione per consentire agli utenti di visualizzare solo le AMI private.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeTags",
```

```
            "ec2:DescribeSnapshots"
         ],
         "Resource": "*"
      }
      ]
}
```

> **Note**
>
> Le operazioni API di Amazon EC2 `ec2:Describe*` non supportano le autorizzazioni a livello di risorsa, pertanto non è possibile controllare le singole risorse che gli utenti possono visualizzare nella console. Il carattere jolly * è quindi necessario nell'elemento `Resource` dell'istruzione precedente. Per ulteriori informazioni sugli ARN che è possibile utilizzare con le operazioni API Amazon EC2, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

Visualizza istanze e CloudWatch metriche

La seguente policy consente agli utenti di visualizzare le istanze nella console Amazon EC2, nonché gli CloudWatch allarmi e le metriche nella scheda Monitoraggio della pagina Istanze. La console Amazon EC2 utilizza l' CloudWatch API per visualizzare gli allarmi e le metriche, quindi è necessario concedere agli utenti il permesso di utilizzare le azioni,, e. `cloudwatch:DescribeAlarms` `cloudwatch:DescribeAlarmsForMetric` `cloudwatch:ListMetrics` `cloudwatch:GetMetricStatistics` `cloudwatch:GetMetricData`

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "cloudwatch:DescribeAlarms",
         "cloudwatch:DescribeAlarmsForMetric",
         "cloudwatch:ListMetrics",
         "cloudwatch:GetMetricStatistics",
```

```
            "cloudwatch:GetMetricData"
        ],
        "Resource": "*"
    }
    ]
}
```

Esempio: utilizzo della procedura guidata per l'avvio dell'istanza EC2

La procedura guidata per l'avvio dell'istanza Amazon EC2 è una schermata contenente opzioni per la configurazione e l'avvio di un'istanza. La policy deve includere l'autorizzazione per l'utilizzo delle operazioni API che consentono agli utenti di utilizzare le opzioni della procedura guidata. Se la policy non include l'autorizzazione per l'utilizzo di tali operazioni, alcuni elementi della procedura guidata potrebbero non venire caricati correttamente e gli utenti potrebbero non essere in grado di completare il processo di avvio.

Accesso di base alla procedura guidata per l'avvio dell'istanza

Per completare un processo di avvio correttamente, gli utenti devono disporre dell'autorizzazione per l'uso dell'operazione API `ec2:RunInstances` e almeno delle seguenti operazioni API:

- `ec2:DescribeImages`: per visualizzare e selezionare un'AMI.
- `ec2:DescribeInstanceTypes`: per visualizzare e selezionare un tipo di istanza.
- `ec2:DescribeVpcs`: Per visualizzare le opzioni di rete disponibili.
- `ec2:DescribeSubnets`: Per visualizzare tutte le sottoreti disponibili per il VPC scelto.
- `ec2:DescribeSecurityGroups` o `ec2:CreateSecurityGroup`: per visualizzare e selezionare un gruppo di sicurezza esistente o crearne uno nuovo.
- `ec2:DescribeKeyPairs` o `ec2:CreateKeyPair`: per selezionare una coppia di chiavi esistente o per crearne una nuova.
- `ec2:AuthorizeSecurityGroupIngress`: per aggiungere le regole in entrata.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateKeyPair"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```

Puoi aggiungere operazioni API alla policy per mettere a disposizione opzioni aggiuntive per gli utenti, ad esempio:

- `ec2:DescribeAvailabilityZones`: Per visualizzare e selezionare una zona di disponibilità specifica.
- `ec2:DescribeNetworkInterfaces`: Per visualizzare e selezionare le interfacce di rete esistenti per la sottorete selezionata.
- Per aggiungere regole in uscita ai gruppi di sicurezza VPC, è necessario concedere agli utenti l'autorizzazione per utilizzare l'operazione API `ec2:AuthorizeSecurityGroupEgress`. Per modificare o eliminare le regole esistenti, è necessario concedere agli utenti l'autorizzazione per utilizzare l'operazione API `ec2:RevokeSecurityGroup*` corrispondente.
- `ec2:CreateTags`: per applicare tag alle risorse create da `RunInstances`. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag Amazon EC2 per le risorse durante la creazione. Se gli utenti non dispongono dell'autorizzazione per utilizzare questa operazione e tentano di applicare tag nella pagina relativa al tagging della procedura guidata per l'avvio dell'istanza, l'avvio ha esito negativo.

> **Important**
>
> Se si specifica un Name (Nome) durante l'avvio di un'istanza viene creato un tag e viene richiesta l'operazione `ec2:CreateTags`. Prestare particolare attenzione quando si concede agli utenti l'autorizzazione per l'uso dell'operazione `ec2:CreateTags`, perché questo limita la possibilità di utilizzare la chiave di condizione `aws:ResourceTag` per limitare l'utilizzo di altre risorse. Se concedi agli utenti il permesso di utilizzare l'`ec2:CreateTags`azione, possono modificare il tag di una risorsa per aggirare tali restrizioni. Per ulteriori informazioni, consulta Controllare l'accesso mediante l'accesso basato sugli attributi.

- Per utilizzare parametri Systems Manager durante la selezione di un'AMI, è necessario aggiungere `ssm:DescribeParameters` e `ssm:GetParameters` alla policy. `ssm:DescribeParameters` concede agli utenti l'autorizzazione per visualizzare e selezionare i parametri Systems Manager. `ssm:GetParameters` concede agli utenti l'autorizzazione per ottenere i valori dei parametri Systems Manager. Puoi inoltre limitare l'accesso a parametri Systems Manager specifici. Per ulteriori informazioni, consulta Limitare l'accesso a parametri Systems Manager specifici in seguito in questa sezione.

Attualmente, le operazioni API `Describe*` di Amazon EC2 non supportano le autorizzazioni a livello di risorsa, pertanto non è possibile limitare le singole risorse che gli utenti possono visualizzare nella procedura guidata per l'avvio dell'istanza. Puoi tuttavia applicare autorizzazioni a livello di risorsa nell'operazione API `ec2:RunInstances` per limitare le risorse che gli utenti possono utilizzare per avviare un'istanza. L'avvio ha esito negativo se gli utenti selezionano opzioni che non sono autorizzati a usare.

Limitazione dell'accesso a un tipo di istanza, sottorete e regione specifici

La seguente policy consente gli utenti di avviare istanze `t2.micro` tramite le AMI di proprietà di Amazon e solo in una sottorete specifica (`subnet-1a2b3c4d`). Gli utenti possono eseguire l'avvio solo nella regione specificata. Se gli utenti selezionano una regione diversa oppure se selezionano un tipo di istanza, un'AMI o una sottorete diversa nella procedura guidata per l'avvio dell'istanza, l'avvio avrà esito negativo.

La prima istruzione concede agli utenti l'autorizzazione per visualizzare le opzioni nella procedura guidata per l'avvio dell'istanza o di crearne di nuove, come illustrato nell'esempio precedente.
La seconda istruzione concede agli utente l'autorizzazione per utilizzare l'interfaccia di rete, il

volume, la coppia di chiavi, il gruppo di sicurezza e le risorse della sottorete per l'operazione `ec2:RunInstances`. Questi elementi sono obbligatori per l'avvio di un'istanza in un VPC. Per ulteriori informazioni sull'uso dell'operazione `ec2:RunInstances`, consulta Istanze di avvio () RunInstances. La terza e la quarta istruzione concedono agli utenti l'autorizzazione per utilizzare rispettivamente le risorse dell'istanza e le risorse dell'AMI, ma solo se l'istanza è un'istanza `t2.micro` e solo se l'AMI è di proprietà di Amazon o di determinati partner sicuri e verificati.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeKeyPairs",
         "ec2:CreateKeyPair",
         "ec2:DescribeVpcs",
         "ec2:DescribeSubnets", "ec2:DescribeSecurityGroups",
         "ec2:CreateSecurityGroup",
         "ec2:AuthorizeSecurityGroupIngress"
   ],
   "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action":"ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-2:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-2:111122223333:volume/*",
         "arn:aws:ec2:us-east-2:111122223333:key-pair/*",
         "arn:aws:ec2:us-east-2:111122223333:security-group/*",
         "arn:aws:ec2:us-east-2:111122223333:subnet/subnet-1a2b3c4d"
      ]
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-2:111122223333:instance/*"
```

```
      ],
      "Condition": {
         "StringEquals": {
            "ec2:InstanceType": "t2.micro"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
            "arn:aws:ec2:us-east-2::image/ami-*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:Owner": "amazon"
         }
      }
   }
   ]
}
```

Limitazione dell'accesso a parametri Systems Manager specifici

La policy seguente concede l'accesso all'utilizzo di parametri Systems Manager con un nome specifico.

La prima istruzione concede agli utenti l'autorizzazione per visualizzare parametri Systems Manager quando si seleziona un'AMI nella procedura guidata per l'avvio dell'istanza. La seconda istruzione concede agli utenti l'autorizzazione a utilizzare solo i parametri denominati `prod-*`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ssm:DescribeParameters"
      ],
      "Resource": "*"
```

```
   },
   {
      "Effect": "Allow",
      "Action": [
         "ssm:GetParameters"
      ],
     "Resource": "arn:aws:ssm:us-east-2:123456123456:parameter/prod-*"
   }
   ]
}
```

Esempio: utilizzo dei gruppi di sicurezza

Visualizzazione dei gruppi di sicurezza e aggiunta e rimozione delle regole

La seguente policy concede agli utenti l'autorizzazione per visualizzare i gruppi di sicurezza nella console Amazon EC2 e per aggiungere e rimuovere le regole in entrata e in uscita e per elencare e modificare le descrizioni delle regole per i gruppi di sicurezza esistenti associati al tag `Department=Test`.

Nella prima istruzione, l'operazione `ec2:DescribeTags` consente agli utenti di visualizzare i tag nella console e ciò semplifica l'identificazione dei gruppi di sicurezza che gli utenti possono modificare.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeSecurityGroups",
         "ec2:DescribeSecurityGroupRules",
         "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:AuthorizeSecurityGroupIngress",
```

```
            "ec2:RevokeSecurityGroupIngress",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:ModifySecurityGroupRules",
            "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
            "ec2:UpdateSecurityGroupRuleDescriptionsEgress"
        ],
        "Resource": [
            "arn:aws:ec2:us-east-2:111122223333:security-group/*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/Department": "Test"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:ModifySecurityGroupRules"
        ],
        "Resource": [
            "arn:aws:ec2:us-east-2:111122223333:security-group-rule/*"
        ]
    }
]}
```

Utilizzo della finestra di dialogo Create Security Group (Crea un gruppo di sicurezza)

È possibile creare una policy che consenta agli utenti di utilizzare la finestra di dialogo Create Security Group (Crea un gruppo di sicurezza) nella console Amazon EC2. Per utilizzare questa finestra di dialogo, gli utenti devono disporre dell'autorizzazione per l'uso almeno delle seguenti operazioni API:

- `ec2:CreateSecurityGroup`: per creare un nuovo gruppo di sicurezza.
- `ec2:DescribeVpcs`: Per visualizzare un elenco di VPC esistenti nell'elenco VPC.

Con queste autorizzazioni, gli utenti possono creare un nuovo gruppo di sicurezza, ma non possono aggiungervi regole. Per utilizzare regole nella finestra di dialogo Create Security Group (Crea un gruppo di sicurezza), è possibile aggiungere le seguenti operazioni API alla policy:

- `ec2:AuthorizeSecurityGroupIngress`: per aggiungere le regole in entrata.
- `ec2:AuthorizeSecurityGroupEgress`: per aggiungere le regole in uscita al gruppo di sicurezza VPC.
- `ec2:RevokeSecurityGroupIngress`: per modificare o eliminare le regole in uscita esistenti. Ciò risulta utile per consentire agli utenti di utilizzare la caratteristica Copy to new (Copia su nuovo) nella console. Questa caratteristica consente di aprire la finestra di dialogo Create Security Group (Crea un gruppo di sicurezza) e popolarlo con le stesse regole del gruppo di sicurezza selezionato.
- `ec2:RevokeSecurityGroupEgress`: per modificare o eliminare le regole in uscita per i gruppi di sicurezza VPC. Ciò risulta utile per consentire agli utenti di modificare o eliminare la regola in uscita di default che autorizza tutto il traffico in uscita.
- `ec2:DeleteSecurityGroup`: da specificare quando non è possibile salvare regole non valide. La console crea innanzitutto il gruppo di sicurezza e quindi aggiunge le regole specificate. Se le regole non sono valide, l'operazione ha esito negativo e la console cerca di eliminare il gruppo di sicurezza. L'utente rimane nella finestra di dialogo Create Security Group (Crea un gruppo di sicurezza) in modo da consentirgli di correggere la regola non valida e provare a creare di nuovo il gruppo di sicurezza. Questa operazione API non è obbligatoria, ma se un utente non riceve l'autorizzazione per utilizzarla e tenta di creare un gruppo di sicurezza con regole non valide, il gruppo di sicurezza viene creato senza regole. L'utente dovrà quindi aggiungere le regole in un secondo momento.
- `ec2:UpdateSecurityGroupRuleDescriptionsIngress`: per aggiungere o aggiornare le descrizioni delle regole dei gruppi di sicurezza in entrata (inbound).
- `ec2:UpdateSecurityGroupRuleDescriptionsEgress`: per aggiungere o aggiornare le descrizioni delle regole del gruppo di sicurezza in uscita (outbound).
- `ec2:ModifySecurityGroupRules`: per modificare modify-security-group-rules.
- `ec2:DescribeSecurityGroupRules`: per elencare le regole dei gruppi di sicurezza.

La seguente policy concede agli utenti l'autorizzazione per utilizzare la finestra di dialogo Create Security Group (Crea un gruppo di sicurezza) e per creare le regole in entrata e in uscita per i gruppi di sicurezza associati a un VPC specifico (`vpc-1a2b3c4d`). Gli utenti possono creare i gruppi di sicurezza per EC2-Classic o un altro VPC, ma non possono aggiungervi regole. In modo analogo, gli utenti non possono aggiungere regole ai gruppi di sicurezza esistenti che non sono associati al VPC `vpc-1a2b3c4d`. Agli utenti viene inoltre concesso l'autorizzazione per visualizzare tutti i gruppi di sicurezza nella console. Ciò aiuta gli utenti a identificare i gruppi di sicurezza a cui possono

aggiungere regole in entrata. Inoltre, questa policy concede agli utenti l'autorizzazione per eliminare i gruppi di sicurezza associati al VPC `vpc-1a2b3c4d`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource": "arn:aws:ec2:us-east-2:111122223333:security-group/*",
      "Condition":{
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:us-east-2:111122223333:vpc/vpc-1a2b3c4d"
         }
      }
    }
   ]
}
```

Esempio: utilizzo degli indirizzi IP elastici

Per consentire agli utenti di visualizzare gli indirizzi IP elastici nella console Amazon EC2, è necessario concedergli l'autorizzazione per utilizzare l'operazione `ec2:DescribeAddresses`.

Per consentire agli utenti di utilizzare gli indirizzi IP elastici, puoi aggiungere le seguenti operazioni alla policy.

- `ec2:AllocateAddress`: Per allocare un indirizzo IP elastico.
- `ec2:ReleaseAddress`: per rilasciare un indirizzo IP elastico.
- `ec2:AssociateAddress`: per associare un indirizzo IP elastico a un'istanza o un'interfaccia di rete.
- `ec2:DescribeNetworkInterfaces` ed `ec2:DescribeInstances`: Per utilizzare la schermata Associate address (Associa indirizzo). Nella schermata sono visualizzate le istanze disponibili o le interfacce di rete a cui puoi associare un indirizzo IP elastico.
- `ec2:DisassociateAddress`: per annullare l'associazione di un indirizzo IP elastico a un'istanza o un'interfaccia di rete.

La seguente policy consente agli utenti di visualizzare, allocare e associare indirizzi IP elastici alle istanze. Gli utenti non possono associare gli indirizzi IP elastici alle interfacce di rete, annullare l'associazione degli indirizzi IP elastici o rilasciarli.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:AllocateAddress",
                "ec2:DescribeInstances",
                "ec2:AssociateAddress"
            ],
            "Resource": "*"
        }
    ]
}
```

Esempio: utilizzo delle Istanze riservate

La seguente policy consente agli utenti di visualizzare e modificare le istanze riservate nell'account, nonché acquistare nuove istanze riservate nella Console di gestione AWS.

Questa politica consente agli utenti di visualizzare tutte le istanze riservate e le On-Demand istanze dell'account. Non è possibile impostare le autorizzazioni a livello di risorsa per singole Istanze riservate.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeReservedInstances",
         "ec2:ModifyReservedInstances",
         "ec2:PurchaseReservedInstancesOffering",
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeAvailabilityZones",
         "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
   }
   ]
}
```

L'operazione `ec2:DescribeAvailabilityZones` è necessaria affinché la console Amazon EC2 sia in grado di visualizzare le informazioni sulle zone di disponibilità in cui è possibile acquistare le Istanze riservate. L'operazione `ec2:DescribeInstances` non è obbligatoria, ma fa sì che l'utente possa visualizzare le istanze nell'account e possa acquistare prenotazioni conformi alle specifiche corrette.

Puoi modificare le operazioni API per limitare l'accesso utente, ad esempio la rimozione di `ec2:DescribeInstances` ed `ec2:DescribeAvailabilityZones` indica che l'utente dispone dell'accesso in sola lettura.

AWS policy gestite per Amazon EC2

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare policy AWS gestite che scrivere policy da soli. La creazione di policy gestite dai clienti IAM che forniscono al team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente,

puoi utilizzare le nostre politiche AWS gestite. Queste politiche coprono casi d'uso comuni e sono disponibili nel tuo AWS account. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta policy gestite per funzioni lavorative che comprendono più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consultare la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

AWS politica gestita: AmazonEC2FullAccess

Puoi collegare la policy `AmazonEC2FullAccess` alle identità IAM. Questa policy concede le autorizzazioni che consentono l'accesso completo ad Amazon EC2.

Per vedere le autorizzazioni per questa policy, consulta AmazonEC2FullAccess nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: AmazonEC2ReadOnlyAccess

Puoi collegare la policy `AmazonEC2ReadOnlyAccess` alle identità IAM. Questa policy concede le autorizzazioni che consentono l'accesso in sola lettura ad Amazon EC2.

Per vedere le autorizzazioni per questa policy, consulta AmazonEC2ReadOnlyAccess nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: AmazonEC2ImageReferencesAccessPolicy

È possibile allegare la policy `AmazonEC2ImageReferencesAccessPolicy` alle identità IAM. Questa policy concede le autorizzazioni necessarie per utilizzare l'DescribeImageReferences API EC2, inclusa l'autorizzazione per visualizzare le istanze EC2, i modelli di avvio, i parametri di

Systems Manager e le ricette di Image Builder. La policy supporta il `IncludeAllResourceTypes` flag e continuerà a funzionare quando AWS aggiungerà il supporto per nuovi tipi di risorse, eliminando la necessità di futuri aggiornamenti delle policy.

Per vedere le autorizzazioni per questa policy, consulta AmazonEC2ImageReferencesAccessPolicy nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: AWSEC2CapacityReservationFleetRolePolicy

Questa policy è collegata al ruolo collegato ai servizi denominato AWSServiceRoleForEC2CapacityReservationFleet per consentire al servizio di creare, modificare e annullare le prenotazioni della capacità in un parco di prenotazioni della capacità per conto dell'utente. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per il parco istanze di prenotazione della capacità.

Per vedere le autorizzazioni per questa policy, consulta AWSEC2CapacityReservationFleetRolePolicy nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: AWSEC2FleetServiceRolePolicy

Questa policy è collegato al ruolo collegato ai servizi denominato AWSServiceRoleForEC2Fleet per consentire al parco istanze EC2 di richiedere, avviare, terminare e taggare le istanze per il proprio conto. Per ulteriori informazioni, consulta Service-linked ruolo per la flotta EC2.

Per vedere le autorizzazioni per questa policy, consulta AWSEC2FleetServiceRolePolicy nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: AWSEC2SpotFleetServiceRolePolicy

Questa policy è collegata al ruolo collegato ai servizi denominato AWSServiceRoleForEC2SpotFleet per consentire al parco istanze spot di avviare e gestire le istanze per il proprio conto. Per ulteriori informazioni, consulta Service-linked ruolo per Spot Fleet.

Per vedere le autorizzazioni per questa policy, consulta AWSEC2SpotFleetServiceRolePolicy nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: AWSEC2SpotServiceRolePolicy

Questa policy è collegata al ruolo collegato ai servizi denominato AWSServiceRoleForEC2Spot per consentire ad Amazon EC2 di avviare e gestire le istanze spot per il proprio conto. Per ulteriori informazioni, consulta Service-linked ruolo per le richieste di istanza Spot.

Per vedere le autorizzazioni per questa policy, consulta AWSEC2SpotServiceRolePolicy nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: AWSEC2VssSnapshotPolicy

Puoi collegare questa policy gestita al ruolo del profilo dell'istanza IAM che usi per le tue istanze Amazon EC2 Windows. La policy garantisce le autorizzazioni per consentire ad Amazon EC2 di creare e gestire snapshot VSS per tuo conto.

Per vedere le autorizzazioni per questa policy, consulta AWSEC2VssSnapshotPolicy nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: DeclarativePoliciesEC2Report

Questa policy è associata al ruolo collegato al servizio denominato `AWSServiceRoleForDeclarativePoliciesEC2Report` per fornire l'accesso alle API di sola lettura necessarie per generare il report sullo stato dell'account per le policy dichiarative.

Per vedere le autorizzazioni per questa policy, consulta DeclarativePoliciesEC2Report nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: EC2FastLaunchFullAccess

Puoi collegare al tuo profilo dell'istanza o a un altro ruolo IAM la policy `EC2FastLaunchFullAccess`. Questa policy garantisce l'accesso completo alle azioni di avvio rapido EC2 e alle autorizzazioni mirate come segue.

Dettagli delle autorizzazioni

- Avvio rapido EC2: viene concesso l'accesso amministrativo, in modo che il ruolo possa abilitare o disabilitare l'avvio rapido EC2 e descrivere le immagini dell'avvio rapido EC2..
- Amazon EC2: l'accesso è concesso per le operazioni di Amazon EC2 RunInstances,CreateTags, Descrivi e Create and Modify Launch Template. È inoltre consentito l'accesso per creare risorse di rete e gruppi di sicurezza, autorizzare regole di ingresso ed eliminare risorse create da EC2 Fast Launch.
- IAM: viene concesso l'accesso per ottenere e utilizzare i profili dell'istanza il cui nome contiene `ec2fastlaunch` per la creazione del ruolo collegato al servizio EC2FastLaunchServiceRolePolicy.

- CloudFormation— L'accesso è concesso a EC2 Fast Launch per descrivere e creare CloudFormation stack e per eliminare gli stack creati.

Per vedere le autorizzazioni per questa policy, consulta EC2FastLaunchFullAccess nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: AWSEC2CapacityManagerServiceRolePolicy

Questa policy è associata al ruolo collegato al servizio denominato per consentire AWSServiceRoleForEC2CapacityManager a EC2 Capacity Manager di gestire le risorse di capacità e integrarsi con le AWS organizzazioni per tuo conto. Per ulteriori informazioni, consulta Service-linked i ruoli di EC2 Capacity Manager.

Per vedere le autorizzazioni per questa policy, consulta AWSEC2CapacityManagerServiceRolePolicy nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: EC2FastLaunchServiceRolePolicy

Questa policy è associata al ruolo collegato al servizio denominato AWSServiceRoleForEC2FastLaunch per consentire ad Amazon EC2 di creare e gestire un set di snapshot predisposti che riducono il tempo necessario per avviare le istanze dalla tua EC2 Fast AMI. Launch-enabled Per ulteriori informazioni, consulta the section called "Service-linked ruolo".

Per vedere le autorizzazioni per questa policy, consulta EC2FastLaunchServiceRolePolicy nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: Ec2InstanceConnect

È possibile allegare la policy `Ec2InstanceConnect` alle identità IAM. Questa policy concede autorizzazioni che consentono ai clienti di chiamare EC2 Instance Connect per pubblicare chiavi temporanee per le proprie istanze EC2 e connettersi tramite SSH o l'EC2 Instance Connect CLI.

Per vedere le autorizzazioni per questa policy, consulta Ec2InstanceConnect nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: Ec2InstanceConnectEndpoint

Questa policy è associata a un ruolo collegato al servizio denominato AWSServiceRoleForEC2InstanceConnect per consentire a EC2 Instance Connect Endpoint di eseguire azioni per conto dell'utente. Per ulteriori informazioni, consulta Service-linked ruolo per EC2 Instance Connect Endpoint.

Per vedere le autorizzazioni per questa policy, consulta Ec2InstanceConnectEndpoint nella Guida di riferimento sulle policy gestite da AWS . Per una descrizione degli aggiornamenti a questa policy, consulta Amazon EC2 si aggiorna a AWS policy gestite.

Amazon EC2 si aggiorna a AWS policy gestite

Visualizza i dettagli sugli aggiornamenti delle policy AWS gestite per Amazon EC2 da quando questo servizio ha iniziato a tracciare queste modifiche.

Modifica	Descrizione	Data
AWSEC2CapacityManagerServiceRolePolicy: nuova policy	Amazon EC2 ha aggiunto questa policy per consentirti di gestire le risorse di capacità e di integrarti con AWS le organizzazioni per tuo conto.	15 ottobre 2025
AmazonEC2ImageReferencesAccessPolicy: nuova policy	Amazon EC2 ha aggiunto questa policy per fornire l'autorizzazione alla scansione di tutti i tipi di risorse supportati dall'API DescribeImageReferences EC2.	26 agosto 2025
Ec2InstanceConnectEndpoint— Politica aggiornata	Per supportare la modifica degli endpoint Instance Connect esistenti, Amazon EC2 ha aggiornato questa policy aggiungendo autorizzazioni per assegnare e annullare l'assegnazione di indirizzi IPv6 e modificare i gruppi di sicurezza sulle interfacce di rete create dall'endpoint EC2 Instance Connect. Amazon EC2 ha aggiornato questa policy anche per sostituire l'operato	31 luglio 2025

Modifica	Descrizione	Data
	re di condizione `Null` con l'operatore di condizione `StringLike` .	
EC2FastLaunchServiceRolePolicy— Politica aggiornata	Per aiutare a prevenire le risorse orfane, Amazon EC2 ha aggiornato questa policy aggiungendo l'autorizzazione a descrivere volumi, attributi dei volumi e interfacce di rete, nonché a eliminare volumi e interfacce di rete creati da EC2 Fast Launch.	17 luglio 2025
EC2FastLaunchFullAccess— Politica aggiornata	Amazon EC2 ha aggiornato questa policy per includere le operazioni Create and Modify Launch Template, per creare risorse di rete e gruppi di sicurezza, per autorizzare le regole di ingresso ed eliminare le risorse create da EC2 Fast Launch. Può inoltre descriver e e creare stack ed eliminare CloudFormation gli stack creati da EC2 Fast Launch.	14 maggio 2025

Modifica	Descrizione	Data
EC2FastLaunchServiceRolePolicy— Politica aggiornata	Amazon EC2 ha aggiornato questa politica per aggiungere EventBridge l'accesso Amazon per creare e gestire le regole degli eventi per EC2 Fast Launch. Inoltre, EC2 Fast Launch ora può descrivere CloudFormation gli stack, avviare un'istanza da un'AMI a cui è associata AWS License Manager, ottenere un elenco di AWS KMS sovvenzioni create che possono essere ritirate ed eliminare i modelli di avvio creati.	14 maggio 2025
AWSEC2CapacityReservationFleetRolePolicy— Autorizzazioni aggiornate	Amazon EC2 ha aggiornato la policy gestita `AWSEC2CapacityReservationFleetRolePolicy` per utilizzare l'operatore di condizione `ArnLike` anziché l'operatore di condizione `StringLike` .	03 marzo 2025
AmazonEC2ReadOnlyAccess: autorizzazioni aggiunte	Amazon EC2 ha aggiunto un'autorizzazione che consente di recuperare i gruppi di sicurezza utilizzando l'operazione `GetSecurityGroupsForVpc` .	27 dicembre 2024

Modifica	Descrizione	Data
EC2FastLaunchFullAccess: nuova policy	Amazon EC2 ha aggiunto questa policy per eseguire azioni API relative alla funzionalità di avvio rapido EC2 da un'istanza. La policy può essere allegata al profilo dell'istanza per un'istanza lanciata da un'AMI abilitata per l'avvio rapido EC2.	14 maggio 2024
AWSEC2VssSnapshotPolicy: nuova policy	Amazon EC2 ha aggiunto la policy `AWSEC2VssSnapshotPolicy` che contiene le autorizzazioni per creare e aggiungere tag alle Amazon Machine Image (AMI) e agli snapshot EBS.	28 marzo 2024
Ec2InstanceConnectEndpoint: nuova policy	Amazon EC2 ha aggiunto la policy `Ec2InstanceConnectEndpoint` . Questa policy è associata al ruolo AWSServiceRoleForEC2InstanceConnect collegato al servizio, per consentire ad Amazon EC2 di eseguire azioni per tuo conto quando crei un endpoint EC2 Instance Connect.	24 gennaio 2023

Modifica	Descrizione	Data
EC2FastLaunchServiceRolePolicy: nuova policy	Amazon EC2 ha aggiunto la funzione di avvio rapido EC2 di Windows per consentire alle AMI di Windows di avviare le istanze più velocemente creando una serie di snapshot pre-provisioning.	26 novembre 2021
Amazon EC2 ha iniziato a monitorare le modifiche	Amazon EC2 ha iniziato a tracciare le modifiche alle sue politiche gestite AWS	1° marzo 2021

Ruoli IAM per Amazon EC2

Le applicazioni devono firmare le proprie richieste API con le credenziali. AWS Pertanto, se sei uno sviluppatore di applicazioni, avrai bisogno di una strategia per gestire le credenziali per le applicazioni eseguite su istanze EC2. Ad esempio, puoi distribuire in modo sicuro le credenziali AWS alle istanze, consentendo alle applicazioni eseguite su tali istanze di utilizzare le credenziali per firmare le richieste, e contemporaneamente proteggere le credenziali da altri utenti. Tuttavia, è difficile distribuire in modo sicuro le credenziali a ciascuna istanza, specialmente quelle AWS create per tuo conto, come le istanze Spot o le istanze nei gruppi Auto Scaling. Inoltre, devi essere in grado di aggiornare le credenziali su ogni istanza quando ruoti le credenziali. AWS

Abbiamo sviluppato i ruoli IAM in modo da consentire alle applicazioni di eseguire in modo sicuro le richieste API dalle istanze senza la necessità di gestire le credenziali di sicurezza utilizzate dalle applicazioni stesse. Invece di creare e distribuire AWS le tue credenziali, puoi delegare l'autorizzazione per effettuare richieste API utilizzando i ruoli IAM come segue:

1. Crea un ruolo IAM.
2. Definisci quali account o AWS servizi possono assumere il ruolo.
3. Definire le operazioni e le risorse API che l'applicazione può utilizzare dopo l'assunzione del ruolo.
4. Specificare il ruolo quando avvii l'istanza o quando associ il ruolo a un'istanza esistente.
5. Impostare l'applicazione in modo che recuperi un set di credenziali temporanee e le utilizzi.

Ad esempio, puoi utilizzare i ruoli IAM per concedere le autorizzazioni alle applicazioni eseguite su istanze che devono utilizzare un bucket in Amazon S3. Puoi specificare le autorizzazioni per i ruoli IAM mediante la creazione di una policy in formato JSON. Si tratta di policy simili a quelle create per gli utenti . Se modifichi un ruolo, la modifica verrà propagata a tutte le istanze.

> **Note**
>
> Le credenziali del ruolo IAM di Amazon EC2 non sono soggette alla durata massima delle sessioni configurata nel ruolo. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

Durante la creazione di ruoli IAM, associa policy IAM con privilegi minimi che limitano l'accesso alle chiamate API specifiche richieste dall'applicazione. Per la Windows-to-Windows comunicazione, utilizza gruppi e ruoli Windows ben definiti e ben documentati per concedere l'accesso a livello di applicazione tra le istanze di Windows. Gruppi e ruoli consentono ai clienti di definire le autorizzazioni a livello di cartella NTFS con privilegi minimi per l'applicazione e le autorizzazioni a livello di cartella NTFS per limitare l'accesso ai requisiti specifici dell'applicazione.

È possibile associare un solo ruolo IAM a un'istanza, ma è possibile associare lo stesso ruolo a molte istanze. Per ulteriori informazioni sulla creazione e sull'utilizzo dei ruoli IAM, consulta la sezione relativa ai ruoli nella Guida per l'utente di IAM.

Puoi applicare le autorizzazioni a livello di risorsa alle policy IAM per controllare la capacità degli utenti di collegare, sostituire o scollegare i ruoli IAM per un'istanza. Per ulteriori informazioni, consulta Autorizzazioni a livello di risorsa supportate per le operazioni API Amazon EC2 e l'esempio seguente: Esempio: utilizzo dei ruoli IAM.

Indice

- Profili delle istanze
- Caso d'uso delle autorizzazioni
- Recupero delle credenziali di sicurezza dai metadati delle istanze
- Concessione dell'autorizzazione a collegare un ruolo IAM a un'istanza
- Collegamento di un ruolo IAM all'istanza
- Ruoli di identità dell'istanza per le istanze Amazon EC2

Profili delle istanze

Amazon EC2 utilizza un profilo dell'istanza come container per un ruolo IAM. Quando crei un ruolo IAM utilizzando la console IAM, la console crea automaticamente un profilo dell'istanza e le assegna lo stesso nome del ruolo a cui corrisponde. Se utilizzi la console Amazon EC2 per avviare un'istanza con un ruolo IAM o per collegare un ruolo IAM a un'istanza, scegli il ruolo in base all'elenco di nomi di profilo delle istanze.

Se utilizzi l' AWS CLI API o un AWS SDK per creare un ruolo, crei il ruolo e il profilo dell'istanza come azioni separate, con nomi potenzialmente diversi. Se poi utilizzi l'API AWS CLI, o un AWS SDK per avviare un'istanza con un ruolo IAM o per collegare un ruolo IAM a un'istanza, specifica il nome del profilo dell'istanza.

Un profilo dell'istanza può contenere solo un ruolo IAM. Puoi includere un ruolo IAM in più profili dell'istanza.

Per aggiornare le autorizzazioni di un'istanza, sostituisci il suo profilo dell'istanza. Sconsigliamo di rimuovere un ruolo da un profilo dell'istanza, poiché è necessario attendere fino a un'ora prima che la modifica abbia effetto.

Per ulteriori informazioni, consulta Use instance profiles nella Guida per l'utente IAM.

Caso d'uso delle autorizzazioni

Quando si crea per la prima volta un ruolo IAM per le applicazioni, a volte è possibile concedere altre autorizzazioni oltre a quanto richiesto. Prima di avviare l'applicazione nell'ambiente di produzione, è possibile generare una policy IAM basata sull'attività di accesso per un ruolo IAM. IAM Access Analyzer esamina i AWS CloudTrail log e genera un modello di policy che contiene le autorizzazioni utilizzate dal ruolo nell'intervallo di date specificato. È possibile utilizzare il modello per creare una policy gestita con autorizzazioni granulari e quindi collegarla al ruolo IAM. In questo modo, concedi solo le autorizzazioni necessarie al ruolo per interagire con le AWS risorse per il tuo caso d'uso specifico. In questo modo è possibile rispettare la best practice per concedere il minimo privilegio. Per ulteriori informazioni, consulta Generazione delle policy per IAM Access Analyzer nella Guida per l'utente IAM.

Recupero delle credenziali di sicurezza dai metadati delle istanze

Un'applicazione in un'istanza recupera le credenziali di sicurezza fornite dal ruolo dalla voce `iam/security-credentials/`role-name nei metadati dell'istanza. All'applicazione vengono concesse le autorizzazioni per le operazioni e le risorse definite per il ruolo tramite le credenziali di sicurezza

associate al ruolo. Queste credenziali di sicurezza sono temporanee e sono caratterizzate da un piano di rotazione automatica. Ciò significa che rendiamo disponibili nuove credenziali almeno cinque minuti prima della scadenza delle vecchie credenziali.

Per ulteriori informazioni sui metadati delle istanze, consulta Utilizzo dei metadati dell'istanza per gestire l'istanza EC2.

> **Warning**
>
> Se utilizzi servizi che usano metadati delle istanze con i ruoli IAM, assicurati di non esporre le credenziali quando i servizi effettuano chiamate HTTP per tuo conto. I tipi di servizi che potrebbero esporre le tue credenziali includono proxy HTTP, servizi di HTML/CSS validazione e processori XML che supportano l'inclusione XML.

Per i tuoi carichi di lavoro Amazon EC2, ti consigliamo di recuperare le credenziali di sessione utilizzando il metodo descritto di seguito. Queste credenziali dovrebbero consentire al carico di lavoro di effettuare richieste di API AWS , senza dover utilizzare `sts:AssumeRole` per assumere lo stesso ruolo già associato all'istanza. A meno che non sia necessario passare i tag di sessione per il controllo degli accessi basato sugli attributi (ABAC) o passare una policy di sessione per limitare ulteriormente le autorizzazioni del ruolo, tali chiamate di assunzione del ruolo non sono necessarie in quanto creano un nuovo set delle stesse credenziali di sessione del ruolo temporaneo.

Se il carico di lavoro utilizza un ruolo per assumere se stesso, devi creare una policy di attendibilità che consenta esplicitamente a tale ruolo di assumere se stesso. Se non crei la policy di attendibilità, ricevi un errore `AccessDenied`. Per ulteriori informazioni, consulta Update a role trust policy nella Guida per l'utente IAM.

IMDSv2

Linux

Esegui il seguente comando dalla tua istanza Linux per recuperare le credenziali di sicurezza per un ruolo IAM.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
```

Windows

Esegui il seguente cmdlet dalla tua istanza Windows per recuperare le credenziali di sicurezza per un ruolo IAM.

```
[string]$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/role-name
```

IMDSv1

Linux

Esegui il seguente comando dalla tua istanza Linux per recuperare le credenziali di sicurezza per un ruolo IAM.

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
```

Windows

Esegui il seguente cmdlet dalla tua istanza Windows per recuperare le credenziali di sicurezza per un ruolo IAM.

```
Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/role-name
```

Di seguito è riportato un output di esempio. Se non riesci a recuperare le credenziali di sicurezza, consulta Non riesco ad accedere alle credenziali di sicurezza temporanee sulla mia istanza EC2 nella Guida per l'utente IAM.

```
{
  "Code" : "Success",
  "LastUpdated" : "2012-04-26T16:39:16Z",
```

```
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",
  "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "Token" : "token",
  "Expiration" : "2017-05-17T15:09:54Z"
}
```

Per le applicazioni e PowerShell i comandi Tools for Windows eseguiti sull'istanza, non è necessario ottenere esplicitamente le credenziali di sicurezza temporanee: gli AWS SDK e gli Strumenti per Windows ottengono PowerShell automaticamente le credenziali dal servizio di AWS CLI metadati delle istanze EC2 e le utilizzano. AWS CLI Per eseguire una chiamata esternamente all'istanza utilizzando le credenziali di sicurezza temporanee, ad esempio per testare le policy IAM, è necessario fornire la chiave di accesso, la chiave segreta e il token di sessione. Per ulteriori informazioni, consulta Using Temporary Security Credentials to Request Access to Resources nella IAM User Guide. AWS

Concessione dell'autorizzazione a collegare un ruolo IAM a un'istanza

Le tue identità Account AWS, ad esempio gli utenti IAM, devono disporre di autorizzazioni specifiche per avviare un'istanza Amazon EC2 con un ruolo IAM, collegare un ruolo IAM a un'istanza, sostituire il ruolo IAM per un'istanza o scollegare un ruolo IAM da un'istanza. Se necessario, devi concedergli l'autorizzazione per utilizzare le seguenti operazioni API:

- `iam:PassRole`
- `ec2:AssociateIamInstanceProfile`
- `ec2:DisassociateIamInstanceProfile`
- `ec2:ReplaceIamInstanceProfileAssociation`

> **Note**
>
> Se specifichi la risorsa per `iam:PassRole` come `*`, ciò garantisce l'accesso per passare uno qualsiasi dei tuoi ruoli IAM a un'istanza. Per seguire la procedura ottimale del privilegio minimo, specifica gli ARN di ruoli IAM specifici con `iam:PassRole`, come mostrato nella policy di esempio riportata di seguito.

Esempio di policy per l'accesso programmatico

La seguente policy IAM concede le autorizzazioni per avviare istanze con un ruolo IAM, collegare un ruolo IAM a un'istanza o sostituire il ruolo IAM per un'istanza utilizzando AWS CLI o l'API Amazon EC2.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances",
         "ec2:AssociateIamInstanceProfile",
         "ec2:DisassociateIamInstanceProfile",
         "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/DevTeam*"
    }
  ]
}
```

Requisito aggiuntivo per l'accesso alla console

Per concedere le autorizzazioni per eseguire le stesse operazioni mediante la console Amazon EC2, è necessario includere anche l'operazione API `iam:ListInstanceProfiles`.

Collegamento di un ruolo IAM all'istanza

Puoi creare un ruolo IAM e collegarlo a un'istanza durante o dopo l'avvio. Puoi inoltre sostituire o scollegare i ruoli IAM.

Creazione e collegamento di un ruolo IAM durante l'avvio dell'istanza (consigliato)

1. Durante il lancio dell'istanza EC2, espandi i dettagli avanzati.

2. Nella sezione del profilo dell'istanza IAM, scegli Crea nuovo ruolo IAM.
3. Si apre un modulo di creazione dei ruoli in linea che ti consente di:
   - Specificare il nome del ruolo (ad esempio,`EC2-S3-Access-Role`)
   - Definisci le autorizzazioni selezionando politiche AWS gestite o creando politiche personalizzate per la tua istanza

     Ad esempio, per concedere l'accesso a S3, seleziona la policy gestita `AmazonS3ReadOnlyAccess`
   - Rivedi la politica di fiducia che consente di `ec2.amazonaws.com` assumere il ruolo
   - Aggiungi tag opzionali per i metadati
4. Scegli Crea ruolo.

   Il ruolo appena creato viene selezionato automaticamente e verrà associato all'istanza tramite un profilo di istanza all'avvio dell'istanza.

> **Note**
>
> Quando si crea un ruolo utilizzando la console durante l'avvio dell'istanza, viene creato automaticamente un profilo di istanza con lo stesso nome del ruolo. Il profilo dell'istanza è un contenitore che trasmette le informazioni sul ruolo IAM all'istanza all'avvio.

> **Important**
>
> - È possibile associare un solo ruolo IAM a un'istanza, ma è possibile associare lo stesso ruolo a molte istanze.
> - Associa politiche IAM con privilegi minimi che limitano l'accesso alle specifiche chiamate API richieste dall'applicazione.

Per ulteriori informazioni sulla creazione e sull'utilizzo dei ruoli IAM, consulta la sezione relativa ai ruoli nella Guida per l'utente di IAM.

Allegare un ruolo IAM esistente durante l'avvio dell'istanza

Per collegare un ruolo IAM esistente a un'istanza all'avvio utilizzando la console Amazon EC2, espandi i dettagli avanzati. Per il profilo dell'istanza IAM, seleziona il ruolo IAM dall'elenco a discesa.

> **Note**
>
> Se hai creato il ruolo IAM utilizzando la console IAM, il profilo dell'istanza creato automaticamente avrà lo stesso nome del ruolo. Se hai creato il tuo ruolo IAM utilizzando l' AWS CLI API o un AWS SDK, potresti aver assegnato al tuo profilo di istanza un nome diverso dal ruolo.

Puoi collegare un ruolo IAM a un'istanza in esecuzione o interrotta. Se all'istanza è già associato un ruolo IAM, devi sostituirlo con il nuovo ruolo IAM.

Console

Per collegare un ruolo IAM a un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Nel menu Actions (Operazioni), scegliere Security (Sicurezza), Modify IAM role (Modifica ruolo IAM).
5. Per il ruolo IAM, seleziona il profilo dell'istanza IAM.
6. Scegli Aggiorna ruolo IAM.

AWS CLI

Per collegare un ruolo IAM a un'istanza

Utilizza il comando associate-iam-instance-profile per collegare il ruolo IAM all'istanza. Quando specifici il profilo dell'istanza, puoi utilizzare il nome della risorsa Amazon (ARN) del profilo dell'istanza oppure il relativo nome.

```
aws ec2 associate-iam-instance-profile \
    --instance-id i-1234567890abcdef0 \
    --iam-instance-profile Name="TestRole-1"
```

PowerShell

Per collegare un ruolo IAM a un'istanza

Utilizza il cmdlet Register-EC2IamInstanceProfile.

```
Register-EC2IamInstanceProfile `
    -InstanceId i-1234567890abcdef0 `
    -IamInstanceProfile_Name TestRole-1
```

Per sostituire il ruolo IAM su un'istanza che ha già un ruolo IAM collegato, l'istanza deve essere in esecuzione. È possibile eseguire questa operazione se si desidera modificare il ruolo IAM per un'istanza senza scollegare prima quella esistente. Ad esempio, è possibile eseguire questa operazione per verificare che le operazioni API eseguite dalle applicazioni in esecuzione sull'istanza non siano interrotte.

Console

Per sostituire un ruolo IAM per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Nel menu Actions (Operazioni), scegliere Security (Sicurezza), Modify IAM role (Modifica ruolo IAM).
5. Per il ruolo IAM, seleziona il profilo dell'istanza IAM.
6. Scegli Aggiorna ruolo IAM.

AWS CLI

Per sostituire un ruolo IAM per un'istanza

1. Se necessario, utilizza il comando describe-iam-instance-profile-associations per recuperare l'ID associazione.

```
aws ec2 describe-iam-instance-profile-associations \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
```

```
    --query IamInstanceProfileAssociations.AssociationId
```

2. Utilizza il comando replace-iam-instance-profile-association. Specifica l'ID associazione per il profilo dell'istanza esistente e l'ARN o il nome del nuovo profilo dell'istanza.

```
aws ec2 replace-iam-instance-profile-association \
    --association-id iip-assoc-0044d817db6c0a4ba \
    --iam-instance-profile Name="TestRole-2"
```

PowerShell

Per sostituire un ruolo IAM per un'istanza

1. Se necessario, utilizza il Get-EC2IamInstanceProfileAssociation cmdlet per ottenere l'ID dell'associazione.

```
(Get-EC2IamInstanceProfileAssociation -Filter @{Name="instance-id";
 Values="i-0636508011d8e966a"}).AssociationId
```

2. Utilizza il cmdlet Set-EC2IamInstanceProfileAssociation. Specifica l'ID associazione per il profilo dell'istanza esistente e l'ARN o il nome del nuovo profilo dell'istanza.

```
Set-EC2IamInstanceProfileAssociation `
    -AssociationId iip-assoc-0044d817db6c0a4ba `
    -IamInstanceProfile_Name TestRole-2
```

Puoi scollegare un ruolo IAM da un'istanza in esecuzione o arrestata.

Console

Per scollegare un ruolo IAM da un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Nel menu Actions (Operazioni), scegliere Security (Sicurezza), Modify IAM role (Modifica ruolo IAM).
5. Per IAM role (Ruolo IAM), scegliere No IAM Role (Nessun ruolo IAM).

6. Scegli Aggiorna ruolo IAM.
7. Quando viene richiesta la conferma, inserisci Scollega, quindi scegli Scollega.

AWS CLI

Per scollegare un ruolo IAM da un'istanza

1. Se necessario, utilizza describe-iam-instance-profile-associations per ottenere l'ID di associazione del profilo istanza IAM da scollegare.

```
aws ec2 describe-iam-instance-profile-associations \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --query IamInstanceProfileAssociations.AssociationId
```

2. Utilizza il comando disassociate-iam-instance-profile.

```
aws ec2 disassociate-iam-instance-profile --association-id iip-
assoc-0044d817db6c0a4ba
```

PowerShell

Per scollegare un ruolo IAM da un'istanza

1. Se necessario, utilizzalo Get-EC2IamInstanceProfileAssociation per ottenere l'ID di associazione da cui scollegare il profilo dell'istanza IAM.

```
(Get-EC2IamInstanceProfileAssociation -Filter @{Name="instance-id";
 Values="i-0636508011d8e966a"}).AssociationId
```

2. Utilizza il cmdlet Unregister-EC2IamInstanceProfile.

```
Unregister-EC2IamInstanceProfile -AssociationId iip-assoc-0044d817db6c0a4ba
```

Ruoli di identità dell'istanza per le istanze Amazon EC2

Ogni istanza Amazon EC2 avviata dispone di un ruolo di identità dell'istanza che ne rappresenta l'identità. Un ruolo di identità di istanza è un tipo di ruolo IAM. AWS i servizi e le funzionalità integrati per utilizzare il ruolo di identità dell'istanza possono utilizzarlo per identificare l'istanza nel servizio.

Le credenziali del ruolo di identità dell'istanza sono accessibili dal servizio di metadati dell'istanza (IMDS) in `/identity-credentials/ec2/security-credentials/ec2-instance`. Le credenziali sono costituite da una coppia di chiavi di accesso AWS temporanee e da un token di sessione. Vengono utilizzate per firmare le richieste AWS Sigv4 ai AWS servizi che utilizzano il ruolo di identità dell'istanza. Le credenziali sono presenti nei metadati dell'istanza indipendentemente dal fatto che sull'istanza sia abilitato un servizio o una funzione che fa uso dei ruoli di identità dell'istanza.

I ruoli di identità dell'istanza vengono creati automaticamente all'avvio di un'istanza, non dispongono di alcun documento relativo alla policy di affidabilità ruolo e non sono soggetti a policy di identità o risorse.

Servizi supportati

I seguenti AWS servizi utilizzano il ruolo di identità dell'istanza:

- Amazon Bedrock AgentCore: le istanze AgentCore di runtime utilizzano il ruolo di identità dell'istanza per configurare le istanze durante il lancio.
- Amazon EC2: EC2 Instance Connect utilizza il ruolo di identità dell'istanza per aggiornare le chiavi host di un'istanza Linux.
- Amazon GuardDuty — GuardDuty Runtime Monitoring utilizza il ruolo di identità dell'istanza per consentire all'agente di runtime di inviare dati di telemetria di sicurezza all'endpoint VPC. GuardDuty
- AWS Lambda— Lambda Managed Instances utilizza il ruolo di identità dell'istanza per gli hook del ciclo di vita, la telemetria e la distribuzione degli artefatti.
- Servizio di token di sicurezza AWS (AWS STS) — Le credenziali del ruolo di identità dell'istanza possono essere utilizzate con l'azione. AWS STS `GetCallerIdentity`
- AWS Systems Manager— Quando si utilizza la configurazione predefinita di gestione dell'host, AWS Systems Manager utilizza l'identità fornita dal ruolo di identità dell'istanza per registrare le istanze EC2. Dopo aver identificato l'istanza, Systems Manager può passare il ruolo IAM `AWSSystemsManagerDefaultEC2InstanceManagementRole` all'istanza.

I ruoli di identità delle istanze non possono essere utilizzati con altri AWS servizi o funzionalità perché non hanno un'integrazione con i ruoli di identità dell'istanza.

ARN del ruolo di identità dell'istanza

L'ARN del ruolo di identità dell'istanza presenta il formato seguente:

```
arn:aws-partition:iam::account-number:assumed-role/aws:ec2-instance/instance-id
```

Ad esempio:

```
arn:aws:iam::0123456789012:assumed-role/aws:ec2-instance/i-1234567890abcdef0
```

Per maggiori informazioni sugli ARN, consulta Nomi della risorsa Amazon (ARN) nella Guida per l'utente di IAM.

Gestione degli aggiornamenti per le istanze Amazon EC2

Ti consigliamo di applicare patch, aggiornare e proteggere regolarmente il sistema operativo e le applicazioni sulle istanze EC2. Puoi utilizzare Gestione patch di AWS Systems Manager per automatizzare il processo di installazione degli aggiornamenti correlati alla sicurezza per il sistema operativo e le applicazioni.

Per le istanze EC2 in un gruppo con scalabilità automatica, puoi utilizzare il runbook AWS-PatchAsgInstance per evitare che le istanze sottoposte a patch vengano sostituite. In alternativa, puoi utilizzare qualsiasi servizio di aggiornamento automatico o processi consigliati per installare gli aggiornamenti che sono forniti dal fornitore dell'applicazione.

Resources

- AL2023: Aggiornamento di AL2023 nella Guida per l'utente di Amazon Linux 2023
- AL2: Gestisci il software sulla tua istanza Amazon Linux 2 nella Guida per l'utente di Amazon Linux 2
- Istanze Windows: the section called “Gestione degli aggiornamenti”

Procedure ottimali relative alla sicurezza delle istanze Windows

Si consiglia di seguire queste procedure ottimali relative alla sicurezza delle istanze Windows.

Indice

- High-level best practice in materia di sicurezza
- Gestione degli aggiornamenti
- Gestione della configurazione

- Gestione delle modifiche
- Audit e responsabilità istanze Windows Amazon EC2

High-level best practice in materia di sicurezza

Devi rispettare le seguenti procedure ottimali di sicurezza di alto livello per le tue istanze di Windows:

- Accesso minimo: viene concesso l'accesso solo a sistemi e percorsi attendibili e previsti. Questo vale per tutti i prodotti Microsoft, ad esempio Active Directory, server di produttività aziendale Microsoft e servizi infrastrutturali quali Servizi di desktop remoto, server proxy inverso, server Web IIS e altri. Usa AWS funzionalità come i gruppi di sicurezza delle istanze Amazon EC2, gli elenchi di controllo degli accessi alla rete (ACL) e le public/private sottoreti Amazon VPC per aumentare la sicurezza su più posizioni in un'architettura. All'interno di un'istanza di Windows, i clienti possono utilizzare Windows Firewall per sviluppare ulteriormente una strategia di difesa in profondità all'interno della distribuzione. Installare solo i componenti e le applicazioni del sistema operativo necessari per il funzionamento del sistema come progettato. Configurare i servizi infrastrutturali, ad esempio IIS, per l'esecuzione con account di servizio o per l'utilizzo di funzionalità quali le identità del pool di applicazioni per accedere alle risorse localmente e in remoto all'intera infrastruttura.
- Privilegio minimo: determina il set minimo di privilegi necessari alle istanze e agli account per svolgere le loro funzioni. Limita tali server e utenti in modo da consentire solo queste autorizzazioni definite. Utilizza tecniche quali i controlli di accesso basati sui ruoli per ridurre l'area di superficie degli account amministrativi e creare i ruoli più limitati per eseguire un'attività. Utilizza le funzionalità del sistema operativo, ad esempio Encrypting File System (EFS) all'interno di NTFS per crittografare i dati sensibili inattivi e controllare l'accesso dell'applicazione e dell'utente ad esso.
- Gestione della configurazione: crea una configurazione di base del server che includa patch di sicurezza aggiornate e suite di protezione basate su host che includono antivirus, antimalware, intrusione e monitoraggio dell'integrità dei file. detection/prevention Valuta ogni server rispetto alla linea di base registrata corrente per identificare e contrassegnare eventuali deviazioni. Assicura che ogni server sia configurato per generare e archiviare in modo sicuro i dati di log e di controllo appropriati.
- Gestione delle modifiche: crea processi per controllare le modifiche alle linee di base della configurazione del server e lavora verso processi di modifica completamente automatizzati. Inoltre, sfrutta Just Enough Administration (JEA) con Windows PowerShell DSC per limitare l'accesso amministrativo alle funzioni minime richieste.
- Gestione patch: implementa processi che applicano patch, aggiornano e proteggono regolarmente il sistema operativo e le applicazioni nelle istanze EC2.

- Log di controllo: controlla l'accesso e tutte le modifiche apportate alle istanze Amazon EC2 per verificare l'integrità del server e garantire che vengano apportate solo le modifiche autorizzate. Sfrutta funzionalità come Enhanced Logging for IIS per migliorare le funzionalità di registrazione predefinite. AWS funzionalità come VPC Flow Logs AWS CloudTrail sono disponibili anche per controllare l'accesso alla rete, comprese rispettivamente allowed/denied le richieste e le chiamate API.

Gestione degli aggiornamenti

Per garantire i migliori risultati quando esegui un server Windows su Amazon EC2, ti consigliamo di implementare le seguenti procedure ottimali:

- Configure Windows Update
- Update drivers
- Use the latest Windows AMIs
- Test performance before migration
- Update launch agents
- Riavvia un'istanza Windows dopo avere installato gli aggiornamenti. Per ulteriori informazioni, consulta Riavvio di un'istanza Amazon EC2.

Per informazioni su come aggiornare o migrare un'istanza Windows a una nuova versione di Windows Server, consultare Aggiornamento di un'istanza EC2 Windows a una versione più recente di Windows Server.

Configura Windows Update

Per impostazione predefinita, le istanze avviate dalle AMI di AWS Windows Server non ricevono aggiornamenti tramite Windows Update.

Aggiornamento dei driver Windows

Mantieni aggiornati i driver su tutte le istanze di Windows EC2 per accertarti che le correzioni più recenti e i miglioramenti di prestazioni siano applicati a tutta la tua serie di istanze. A seconda del tipo di istanza, è necessario aggiornare i driver AWS PV, Amazon ENA e AWS NVMe.

- Utilizza gli argomenti su SNS per ottenere gli aggiornamenti per le ultime versioni dei driver.

- Usa il runbook di AWS Systems Manager automazione per applicare facilmente gli aggiornamenti AWSSupport-UpgradeWindowsAWSDrivers alle tue istanze.

Avvio di istanze usando le AMI Windows più recenti

AWS rilascia ogni mese nuove AMI Windows, che contengono le patch, i driver e gli agenti di avvio del sistema operativo più recenti. Quando avvii nuove istanze o quando crei immagini personalizzate, devi utilizzare le AMI più recenti.

- Per visualizzare gli aggiornamenti di ogni versione delle AMI AWS Windows, consulta la cronologia delle versioni di AWS Windows AMI.
- Per compilare con le AMI più recenti disponibili, consulta Query per l'AMI Windows più recente tramite Systems Manager Parameter Store.
- Per ulteriori informazioni sulle AMI Windows specializzate che è possibile utilizzare per avviare istanze per il database e sui casi d'uso relativi all'hardening della conformità, vedere AMI Windows specializzate nei Riferimenti Windows AMI AWS .

Verifica system/application le prestazioni prima della migrazione

La migrazione delle applicazioni aziendali verso AWS può comportare molte variabili e configurazioni. È opportuno testare sempre le prestazioni della soluzione EC2 per assicurarsi di quanto segue:

- I tipi di istanza sono configurati correttamente, incluse la dimensione dell'istanza, le reti migliorate e la tenancy (condivisa o dedicata).
- La topologia dell'istanza è idonea per il carico di lavoro e, laddove necessario, impiega caratteristiche ad alte prestazioni (tenancy dedicata, gruppi di collocamento, volumi archivio dell'istanza, bare metal).

Installare la versione più recente di EC2Launch v2

Installa l'agente EC2Launch v2 più recente per assicurarti che le ultime correzioni vengano applicate a tutto il parco istanze. Per ulteriori informazioni, consulta Installare EC2Launch v2.

Se si utilizza un parco istanze misto o si desidera continuare a utilizzare gli agenti EC2Launch (Windows Server 2016 e 2019) o EC2 Config (solo sistemi operativi legacy), eseguire l'aggiornamento alle versioni più recenti dei rispettivi agenti.

Gli aggiornamenti automatici sono supportati nelle seguenti combinazioni di versioni di Windows Server e agenti di avvio. Puoi attivare gli aggiornamenti automatici nella console SSM Quick Setup Host Management in Agenti di avvio Amazon EC2.

Versione Windows	EC2Launch v1	EC2Launch v2
2016	✓	✓
2019	✓	✓
2022		✓

- Per ulteriori informazioni sull'aggiornamento a EC2Launch v2, consulta the section called "Installare EC2Launch v2".
- Per informazioni sull'aggiornamento manuale di EC2Config, consulta the section called "Installazione di EC2Config".
- Per informazioni sull'aggiornamento manuale di EC2Launch, consulta the section called "Installazione di EC2Launch".

Gestione della configurazione

Amazon Machine Images (AMI) fornisce una configurazione iniziale per un'istanza Amazon EC2, che include il sistema operativo Windows e personalizzazioni facoltative specifiche del cliente, come applicazioni e controlli di sicurezza. Crea un catalogo AMI contenente linee di base di configurazione di sicurezza personalizzate per garantire che tutte le istanze di Windows vengano avviate con controlli di sicurezza standard. Le linee di base di sicurezza possono essere inserite in un'AMI, avviate dinamicamente all'avvio di un'istanza EC2 o impacchettate come prodotto per una distribuzione uniforme attraverso i portafogli di Service Catalog. AWS Per ulteriori informazioni sulla protezione di un'AMI, consulta Best Practices for Building an AMI.

Ogni istanza Amazon EC2 deve rispettare gli standard di sicurezza organizzativa. Non installare ruoli e funzionalità di Windows che non sono necessari e installa software per la protezione da codice dannoso (antivirus, antimalware, attenuazione degli exploit), monitora l'integrità dell'host ed esegui il rilevamento delle intrusioni. Configura il software di sicurezza per monitorare e mantenere le impostazioni di sicurezza del sistema operativo, proteggere l'integrità dei file operativi critici e avvisare eventuali deviazioni dalla linea di base di sicurezza. Considera di implementare i benchmark

della configurazione di sicurezza pubblicati da Microsoft, dal Center for Internet Security (CIS) o dal National Institute of Standards and Technology (NIST). Prendi in considerazione l'utilizzo di altri strumenti Microsoft per server di applicazioni particolari, ad esempio il Best Practice Analyzer per SQL Server.

AWS i clienti possono anche eseguire valutazioni di Amazon Inspector per migliorare la sicurezza e la conformità delle applicazioni distribuite sulle istanze Amazon EC2. Amazon Inspector valuta automaticamente le applicazioni per individuare vulnerabilità o deviazioni dalle procedure consigliate e include una base di conoscenze di centinaia di regole mappate a standard di conformità di sicurezza comuni (ad esempio, PCI DSS) e definizioni di vulnerabilità. Esempi di regole incorporate includono la verifica se l'accesso remoto root è abilitato o se sono installate versioni software vulnerabili. Queste regole vengono aggiornate regolarmente dai ricercatori di sicurezza. AWS

Quando si proteggono le istanze di Windows, si consiglia di implementare Servizi di dominio Active Directory per abilitare un'infrastruttura scalabile, sicura e gestibile per i percorsi distribuiti. Inoltre, dopo aver avviato le istanze dalla console Amazon EC2 o utilizzando uno strumento di provisioning di Amazon EC2, ad esempio AWS CloudFormation, è buona norma utilizzare funzionalità native del sistema operativo, come Microsoft Windows PowerShell DSC, per mantenere lo stato della configurazione in caso di deviazione della configurazione.

Gestione delle modifiche

Dopo aver applicato le basi di sicurezza iniziali alle istanze Amazon EC2 all'avvio, controlla le modifiche in corso su Amazon EC2 per mantenere la sicurezza delle macchine virtuali. Stabilisci un processo di gestione delle modifiche per autorizzare e incorporare le modifiche alle AWS risorse (come gruppi di sicurezza, tabelle di routing e ACL di rete) e alle configurazioni del sistema operativo e delle applicazioni (come l'applicazione di patch per Windows o delle applicazioni, gli aggiornamenti del software o gli aggiornamenti dei file di configurazione).

AWS fornisce diversi strumenti per aiutare a gestire le modifiche alle AWS risorse, tra cui,, e AWS CloudTrail AWS Config CloudFormation AWS Elastic Beanstalk, e i pacchetti di gestione per Systems Center Operations Manager e System Center Virtual Machine Manager. Tieni presente che Microsoft rilascia le patch di Windows il secondo martedì di ogni mese (o se necessario) e AWS aggiorna tutte le AMI Windows gestite AWS entro cinque giorni dal rilascio di una patch da parte di Microsoft. Pertanto è importante applicare continuamente patch a tutte le AMI di base, aggiornare i CloudFormation modelli e le configurazioni dei gruppi Auto Scaling con gli ID AMI più recenti e implementare strumenti per automatizzare la gestione delle patch delle istanze in esecuzione.

Microsoft fornisce diverse opzioni per la gestione delle modifiche al sistema operativo Windows e alle applicazioni. SCCM, ad esempio, fornisce una copertura completa del ciclo di vita delle modifiche dell'ambiente. Seleziona gli strumenti che rispondono ai requisiti aziendali e controlla in che modo le modifiche influenzeranno i contratti di servizio delle applicazioni, la capacità, la sicurezza e le procedure di disaster recovery. Evita le modifiche manuali e sfrutta invece il software di gestione automatica della configurazione o gli strumenti da riga di comando come EC2 Run Command o Windows PowerShell per implementare processi di modifica ripetibili e basati su script. Per rispondere a questo requisito, utilizza bastion host con logging avanzato per tutte le interazioni con le istanze di Windows per garantire che tutti gli eventi e le attività vengano registrati automaticamente.

Audit e responsabilità istanze Windows Amazon EC2

AWS CloudTrail e Regole di AWS Config fornisci funzionalità di controllo e tracciamento delle modifiche per il controllo delle modifiche alle risorse. AWS Config AWS Configura i log di eventi di Windows per inviare file di log locali a un sistema centralizzato di gestione dei log per conservare i dati di log per l'analisi del comportamento operativo e di sicurezza. Microsoft System Center Operations Manager (SCOM) aggrega informazioni sulle applicazioni Microsoft distribuite nelle istanze Windows e applica set di regole preconfigurati e personalizzati in base ai ruoli e ai servizi dell'applicazione. I System Center Management Pack si basano su SCOM per fornire indicazioni sulla configurazione e monitoraggio specifiche delle applicazioni. Questi Management Pack supportano Windows Server Active Directory, SharePoint Server 2013, Exchange Server 2013, Lync Server 2013, SQL Server 2014 e molti altri server e tecnologie.

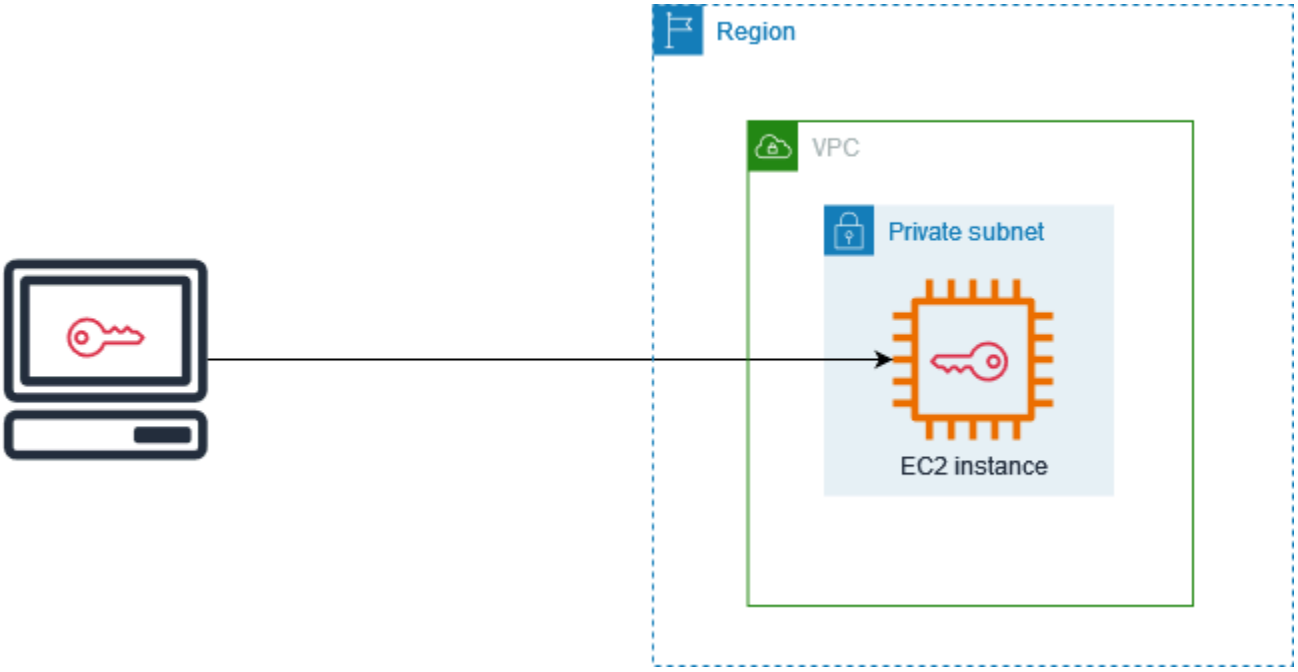
Oltre agli strumenti di gestione dei sistemi Microsoft, i clienti possono utilizzare Amazon CloudWatch per monitorare l'utilizzo della CPU delle istanze, le prestazioni del disco, la rete I/O ed eseguire controlli sullo stato di host e istanze. I servizi EC2Config, EC2Launch ed EC2Launch v2 launch forniscono accesso a funzionalità avanzate aggiuntive per le istanze di Windows. Ad esempio, possono esportare i log di sistema, sicurezza, applicazioni e Internet Information Services (IIS) di Windows in Logs che possono quindi essere integrati con le CloudWatch metriche e gli allarmi di Amazon. CloudWatch I clienti possono anche creare script per esportare i contatori delle prestazioni di Windows in metriche personalizzate di Amazon. CloudWatch

Coppie di chiavi Amazon EC2 e istanze Amazon EC2

Una coppia di chiavi, costituita da una chiave privata e una chiave pubblica, è un insieme di credenziali di sicurezza utilizzate per dimostrare l'identità durante la connessione a un'istanza Amazon EC2. Per le istanze Linux, la chiave privata ti consente di eseguire un SSH in modo sicuro

nella tua istanza. Per le istanze di Windows, la chiave privata è necessaria per decrittare la password dell'amministratore, che utilizzerai poi per connetterti alla tua istanza.

Amazon EC2 archivia solo la chiave pubblica nell'istanza mentre l'utente deve archiviare la chiave privata, come mostrato nel diagramma seguente. È importante archiviare la chiave privata in un luogo sicuro, in quanto chiunque possiede la chiave privata può connettersi alle istanze che utilizzano la coppia di chiavi.



Quando avvii un'istanza, puoi specificare una coppia di chiavi, in modo da poterti connettere all'istanza utilizzando un metodo che richiede una coppia di chiavi. A seconda di come gestisci la sicurezza, puoi specificare la stessa coppia di chiavi per tutte le istanze oppure puoi specificare coppie di chiavi diverse.

Per le istanze Linux, quando viene avviata per la prima volta, la chiave pubblica specificata all'avvio viene inserita nell'istanza Linux in una voce in `~/.ssh/authorized_keys`. Quando ti connetti all'istanza Linux usando SSH, per accedere devi specificare la chiave privata che corrisponde alla chiave pubblica.

Per ulteriori informazioni sulla connessione all'istanza EC2, consulta Connettiti all'istanza EC2.

> **Important**
>
> Poiché Amazon EC2 non conserva una copia della chiave privata, se si perde una chiave privata non è possibile recuperarla. Tuttavia, può ancora esserci un modo per connettersi a

istanze per cui hai perso la chiave privata. Per ulteriori informazioni, consulta Ho perso la mia chiave privata. Come posso connettermi alla mia istanza?

In alternativa alle coppie di chiavi, puoi utilizzare AWS Systems Manager Session Manager per connetterti alla tua istanza con una shell interattiva basata su browser o la AWS Command Line Interface ()AWS CLI.

Indice

- Creazione di una coppia di chiavi per l'istanza Amazon EC2
- Descrivere le tue coppie di chiavi
- Eliminazione della coppia di chiavi
- Aggiungi o sostituisci una chiave pubblica sull'istanza Linux
- Verifica dell'impronta digitale della coppia di chiavi

Creazione di una coppia di chiavi per l'istanza Amazon EC2

È possibile usare Amazon EC2 creare una coppia di chiavi, oppure è possibile utilizzare uno strumento di terzi per creare una coppia di chiavi e importarla in Amazon EC2.

Amazon EC2 supporta chiavi SSH-2 RSA a 2048 bit per istanze Linux e Windows. Amazon EC2 supporta anche le chiavi ED25519 su istanze Linux.

Per le istruzioni su come connettersi all'istanza dopo aver creato una coppia di chiavi, consulta the section called “Connessione a un’istanza Linux tramite SSH” e the section called “Connessione all’istanza Windows con il protocollo RDP”.

Indice

- Creazione di una coppia di chiavi utilizzando Amazon EC2
- Crea una coppia di chiavi usando AWS CloudFormation
- Creazione di una coppia di chiavi tramite uno strumento di terza parte e importazione della chiave pubblica in Amazon EC2

Creazione di una coppia di chiavi utilizzando Amazon EC2

Quando crei una coppia di chiavi utilizzando Amazon EC2, la chiave pubblica viene archiviata in Amazon EC2 e tu archivi la chiave privata.

Puoi creare fino a 5.000 coppie di chiavi per regione. Per richiedere un aumento, crea un caso di supporto. Per ulteriori informazioni, consulta Creazione di una richiesta di assistenza nella Guida per l'utente di Supporto .

Console

Come creare una coppia di chiavi utilizzando Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, sotto Network & Security (Rete e sicurezza), scegliere Key Pairs (Coppie di chiavi).
3. Scegliere Create key pair (Crea coppia di chiavi).
4. Per Name (Nome), immettere un nome descrittivo per la coppia di chiavi. Amazon EC2 associa la chiave pubblica con il nome specificato come nome della chiave. Il nome può includere fino a 255 caratteri ASCII. Non può includere spazi iniziali o finali.
5. Seleziona un tipo di coppia di chiavi appropriato per il tuo sistema operativo:

   (Istanze Linux) Per il tipo di coppia di chiavi, scegli RSA o ED25519.

   (Istanze Windows) Per il tipo di coppia di chiavi, scegli RSA. Le chiavi ED25519 non sono supportate per le istanze Windows.
6. Per Private key file format (Formato file chiave privata), scegliere il formato in cui salvare la chiave privata. Per salvare la chiave privata in un formato che può essere utilizzato con OpenSSH, scegliere pem. Per salvare la chiave privata in un formato che può essere utilizzato con PuTTY, scegliere ppk.
7. Per aggiungere un tag, scegli Add tag (Aggiungi tag) e immetti la chiave e il valore per il tag. Ripetere per ogni tag.
8. Scegliere Create key pair (Crea coppia di chiavi).
9. Il file della chiave privata viene automaticamente scaricato dal browser. Il nome del file di base è il nome specificato come nome della coppia di chiavi e l'estensione del nome del file è determinata dal formato di file scelto. Salvare il file della chiave privata in un luogo sicuro.

> **Important**
>
> Questo è l'unico momento in cui salvare il file della chiave privata.

10. Se prevedi di utilizzare un client SSH su un computer macOS o Linux per connetterti all'istanza Linux, utilizza il comando seguente per impostare le autorizzazioni del file della chiave privata per essere l'unico a poterlo leggere.

```
chmod 400 key-pair-name.pem
```

Se non imposti queste autorizzazioni, allora non puoi connetterti alle tue istanze usando questa coppia di chiavi. Per ulteriori informazioni, consulta Errore: Unprotected Private Key File (File della chiave privata non protetto).

AWS CLI

Come creare una coppia di chiavi utilizzando Amazon EC2

1. Utilizza il comando create-key-pair come segue per generare la coppia di chiavi e salvare la chiave privata in un file `.pem`. L'opzione `--query` stampa il materiale della chiave privata nell'output. L'opzione `--output` salva il materiale della chiave privata nel file specificato. L'estensione deve essere `.pem` o `.ppk`, a seconda del formato della chiave. Il nome della chiave privata può essere diverso da quello della chiave pubblica ma, per facilità d'uso, utilizza lo stesso nome.

```
aws ec2 create-key-pair \
    --key-name my-key-pair \
    --key-type rsa \
    --key-format pem \
    --query "KeyMaterial" \
    --output text > my-key-pair.pem
```

2. Se prevedi di utilizzare un client SSH su un computer macOS o Linux per connetterti all'istanza Linux, utilizza il comando seguente per impostare le autorizzazioni del file della chiave privata per essere l'unico a poterlo leggere.

```
chmod 400 key-pair-name.pem
```

Se non imposti queste autorizzazioni, allora non puoi connetterti alle tue istanze usando questa coppia di chiavi. Per ulteriori informazioni, consulta Errore: Unprotected Private Key File (File della chiave privata non protetto).

PowerShell

Come creare una coppia di chiavi utilizzando Amazon EC2

Utilizza il cmdlet New-EC2KeyPair come segue per generare la chiave e salvarla in un file `.pem` o `.ppk`. Il cmdlet Out-File salva il materiale della chiave privata in un file con estensione specificata. L'estensione deve essere `.pem` o `.ppk`, a seconda del formato della chiave. Il nome della chiave privata può essere diverso da quello della chiave pubblica ma, per facilità d'uso, utilizza lo stesso nome.

```
(New-EC2KeyPair `
    -KeyName "my-key-pair" `
    -KeyType "rsa" `
    -KeyFormat "pem").KeyMaterial | Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem
```

Crea una coppia di chiavi usando AWS CloudFormation

Quando si crea una nuova coppia di chiavi utilizzando CloudFormation, la chiave privata viene salvata in AWS Systems Manager Parameter Store. Il nome del parametro ha il formato seguente:

```
/ec2/keypair/key_pair_id
```

Per ulteriori informazioni, consulta Archivio dei parametri AWS Systems Manager nella Guida per l'utente di AWS Systems Manager .

Per creare una coppia di chiavi usando CloudFormation

1. Specifica la KeyPair risorsa AWS: :EC2:: nel tuo modello.

```
Resources:
  NewKeyPair:
    Type: 'AWS::EC2::KeyPair'
    Properties:
```

```
      KeyName: new-key-pair
```

2. Utilizza il comando describe-key-pairs come segue per ottenere l'ID della coppia di chiavi.

```
aws ec2 describe-key-pairs --filters Name=key-name,Values=new-key-pair --query
 KeyPairs[*].KeyPairId --output text
```

Di seguito è riportato un output di esempio.

```
key-05abb699beEXAMPLE
```

3. Utilizza il comando get-parameter come segue per ottenere il parametro per la tua chiave e salvare il materiale della chiave in un file `.pem`.

```
aws ssm get-parameter --name /ec2/keypair/key-05abb699beEXAMPLE --with-decryption
 --query Parameter.Value --output text > new-key-pair.pem
```

Autorizzazioni IAM richieste

CloudFormation Per consentire la gestione dei parametri di Parameter Store per tuo conto, il ruolo IAM assunto dall'utente CloudFormation o dall'utente deve disporre delle seguenti autorizzazioni:

- `ssm:PutParameter`: concede l'autorizzazione per creare un parametro per il materiale della chiave privata.
- `ssm:DeleteParameter`: concede l'autorizzazione a eliminare il parametro che ha archiviato il materiale della chiave privata. Questa autorizzazione è necessaria indipendentemente dal fatto che la coppia di chiavi sia stata importata o creata da CloudFormation.

Quando CloudFormation elimina una coppia di chiavi creata o importata da uno stack, esegue un controllo delle autorizzazioni per determinare se si dispone dell'autorizzazione per eliminare i parametri, anche se CloudFormation crea un parametro solo quando crea una coppia di chiavi, non quando importa una coppia di chiavi. CloudFormation verifica l'autorizzazione richiesta utilizzando un nome di parametro inventato che non corrisponde a nessun parametro dell'account. Pertanto, è possibile che nel messaggio di errore `AccessDeniedException` venga visualizzato un nome di parametro fittizio.

Creazione di una coppia di chiavi tramite uno strumento di terza parte e importazione della chiave pubblica in Amazon EC2

Invece di creare la coppia di chiavi tramite Amazon EC2, è possibile creare una coppia di chiavi RSA o ED25519 utilizzando uno strumento di terzi e importare la chiave pubblica in Amazon EC2.

Requisiti delle coppie di chiavi

- Tipi supportati:
  - (Linux e Windows) RSA
  - (Solo Linux) ED25519

    > **Note**
    >
    > Le chiavi ED25519 non sono supportate per le istanze Windows.

  - Amazon EC2 non accetta chiavi DSA.
- Formati supportati:
  - Il formato chiave pubblica di OpenSSH (per Linux, il formato in `~/.ssh/authorized_keys`)
  - (Solo Linux) Se effettui la connessione mediante SSH mentre stai utilizzando l'API EC2 Instance Connect, è supportato anche il formato SSH2.
  - Il formato del file della chiave privata SSH deve essere PEM o PPK
  - (Solo RSA) Il formato DER con codifica Base64
  - (Solo RSA) Il formato file della chiave pubblica SSH come specificato in RFC4716
- Lunghezze supportate:
  - 1024, 2048 e 4096.
  - (Solo Linux) Se effettui la connessione mediante SSH mentre stai utilizzando l'API EC2 Instance Connect, le lunghezze supportate sono 2048 e 4096.

Per creare una coppia di chiavi tramite uno strumento di terza parte

1. Generare una coppia di chiavi con lo strumento di terza parte preferito. Ad esempio, per creare una coppia di chiavi è possibile utilizzare ssh-keygen (uno strumento fornito con l'installazione standard di OpenSSH). In alternativa, Java, Ruby, Python e molti altri linguaggi di programmazione forniscono librerie standard che è possibile utilizzare per creare una coppia di chiavi.

> **Important**
>
> La chiave privata deve essere nel formato PEM o PPK. Ad esempio, utilizzare `ssh-keygen -m PEM` per generare la chiave OpenSSH nel formato PEM.

2. Salvare la chiave pubblica in un file locale. Ad esempio, `~/.ssh/my-key-pair.pub` (Linux, macOS) o `C:\keys\my-key-pair.pub` (Windows). L'estensione del nome del file non è importante.
3. Salvare la chiave privata in un file locale con estensione `.pem` o `.ppk`. Ad esempio, `~/.ssh/my-key-pair.pem` o `~/.ssh/my-key-pair.ppk` (Linux, macOS) o `C:\keys\my-key-pair.pem` o `C:\keys\my-key-pair.ppk` (Windows). L'estensione del file è importante perché, a seconda dello strumento che usi per connetterti all'istanza, avrai bisogno di un formato di file specifico. OpenSSH richiede un file `.pem`, mentre PuTTY richiede un file `.ppk`.

> **Important**
>
> Salvare il file della chiave privata in un luogo sicuro. Dovrai fornire il nome della chiave pubblica quando avvii un'istanza e la chiave privata corrispondente ogni volta che ti connetti all'istanza.

Dopo avere creato la coppia di chiavi, utilizzare uno dei seguenti metodi per importare la chiave pubblica in Amazon EC2.

Console

Come importare la chiave pubblica in Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Key Pairs (Coppie di chiavi).
3. Scegliere Import key pair (Importa coppia di chiavi).
4. Per Name (Nome), immettere un nome descrittivo per la chiave pubblica. Il nome può includere fino a 255 caratteri ASCII. Non può includere spazi iniziali o finali.

> **Note**
>
> Quando ci si connette all'istanza dalla console EC2, la console suggerisce questo nome per il nome file della chiave privata.

5. Scegliere Browse (Sfoglia) per navigare e selezionare la chiave pubblica oppure incollare il contenuto della chiave pubblica nel campo Public key contents (Contenuto chiave pubblica).
6. Scegliere Import key pair (Importa coppia di chiavi).
7. Verificare che la chiave pubblica importata venga visualizzata nell'elenco delle coppie di chiavi.

AWS CLI

Come importare la chiave pubblica in Amazon EC2

Utilizza il comando import-key-pair.

```
aws ec2 import-key-pair \
    --key-name my-key-pair \
    --public-key-material fileb://path/my-key-pair.pub
```

Per verificare che la coppia di chiavi sia stata importata correttamente

Utilizza il comando describe-key-pairs.

```
aws ec2 describe-key-pairs --key-names my-key-pair
```

PowerShell

Come importare la chiave pubblica in Amazon EC2

Utilizza il cmdlet Import-EC2KeyPair.

```
$publickey=[Io.File]::ReadAllText("C:\Users\TestUser\.ssh\id_rsa.pub")
Import-EC2KeyPair `
    -KeyName my-key-pair `
    -PublicKey $publickey
```

Per verificare che la coppia di chiavi sia stata importata correttamente

Utilizza il cmdlet Get-EC2KeyPair.

```
Get-EC2KeyPair -KeyName my-key-pair
```

Descrivere le tue coppie di chiavi

È possibile descrivere le coppie di chiavi archiviate in Amazon EC2. È inoltre possibile recuperare il materiale della chiave pubblica e identificare la chiave pubblica specificata all'avvio.

Processi

- Descrivere le tue coppie di chiavi
- Recupero del materiale delle chiavi pubbliche
- Identificazione della chiave pubblica specificata al momento dell'avvio

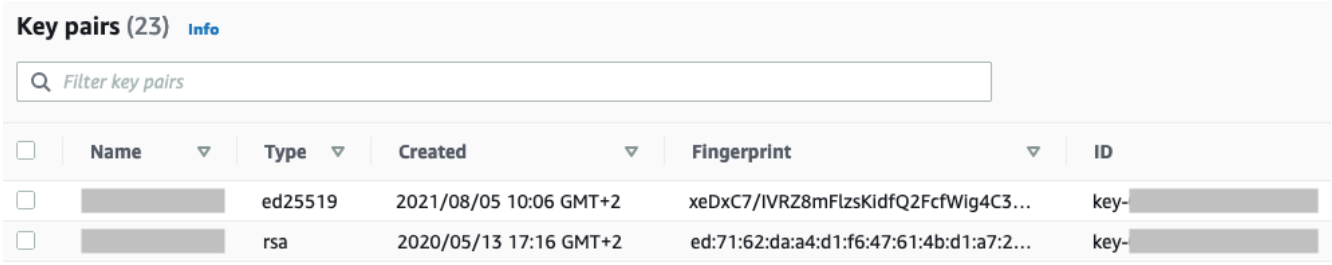
Descrivere le tue coppie di chiavi

È possibile visualizzare le seguenti informazioni sulle chiavi pubbliche archiviate in Amazon EC2: nome della chiave pubblica, ID, tipo di chiave, impronta digitale, materiale chiave pubblica, data e ora (nel fuso orario UTC) in cui la chiave è stata creata da Amazon EC2 (se la chiave è stata creata da uno strumento di terze parti, la data e l'ora si riferiscono al momento in cui la chiave è stata importata in Amazon EC2) e tutti i tag associati alla chiave pubblica.

Console

Per visualizzare le informazioni relative alle coppie di chiavi

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione sinistro, scegli Key Pairs (Coppie di chiavi).
3. È possibile visualizzare le informazioni su ciascuna chiave pubblica nella tabella Key pairs (Coppie di chiavi).



4. Per visualizzare i tag di una chiave pubblica, seleziona la casella di controllo accanto alla chiave e quindi scegli Actions (Operazioni), Manage tags (Gestisci tag).

AWS CLI

Per visualizzare le informazioni relative a una coppia di chiavi

Utilizza il comando describe-key-pairs.

```
aws ec2 describe-key-pairs --key-names key-pair-name
```

PowerShell

Per visualizzare le informazioni relative a una coppia di chiavi

Utilizza il cmdlet Get-EC2KeyPair.

```
Get-EC2KeyPair -KeyName key-pair-name
```

Recupero del materiale delle chiavi pubbliche

Puoi ottenere il materiale della chiave pubblica per le coppie di chiavi. Quello che segue è un esempio di chiave pubblica. Si noti che sono state aggiunte delle interruzioni di riga per facilitare la lettura.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Private key

Come recuperare il materiale della chiave pubblica utilizzando ssh-keygen (Linux)

Sul computer locale macOS, utilizza il comando ssh-keygen. Specificare il percorso in cui è stata scaricata la chiave privata (il file `.pem`).

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

Se questo ssh-keygen comando non funziona, esegui il seguente comando chmod per assicurarti che il file della chiave privata abbia i permessi richiesti

```
chmod 400 key-pair-name.pem
```

Per recuperare il materiale della chiave pubblica utilizzando PuTTYgen (Windows)

Avvia PuttyGen sul tuo computer Windows locale. Scegli Carica. Seleziona il file della chiave privata `.ppk` o `.pem`. PuTTYgen visualizza la chiave pubblica in Public key for pasting into OpenSSH authorized_keys file (Chiave pubblica da incollare nel file OpenSSH authorized_keys). È anche possibile visualizzare la chiave pubblica scegliendo Save public key (Salva chiave pubblica), specificando un nome del file, salvando il file e quindi aprendolo.

AWS CLI

Per recuperare il materiale della chiave pubblica

Utilizza il comando describe-key-pairs e specifica l'opzione `--include-public-key`.

```
aws ec2 describe-key-pairs \
    --key-names key-pair-name \
    --include-public-key \
    --query "KeyPairs[].PublicKey"
```

PowerShell

Per recuperare il materiale della chiave pubblica

Utilizza il cmdlet Get-EC2KeyPair.

```
(Get-EC2KeyPair -KeyName key-pair-name -IncludePublicKey $true).PublicKey
```

IMDSv2

Linux

Esegui i seguenti comandi dall'istanza Linux.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key
```

Windows

Esegui i seguenti cmdlet dall'istanza Windows.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri
 http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

Linux

Esegui il seguente comando dall'istanza Linux.

```
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Windows

Esegui il seguente cmdlet dall'istanza Windows.

```
Invoke-RestMethod -uri  http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

Identificazione della chiave pubblica specificata al momento dell'avvio

Se specifichi una chiave pubblica quando avvii un'istanza, il nome della chiave pubblica viene registrato dall'istanza. Il nome della chiave pubblica riportato per un'istanza non cambia, anche se si modifica la chiave pubblica sull'istanza o si aggiungono chiavi pubbliche.

Console

Per identificare la chiave pubblica specificata all'avvio dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.

4. Nella scheda Dettagli, in Dettagli dell'istanza, trova Coppia di chiavi assegnata all'avvio.

AWS CLI

Per identificare la chiave pubblica specificata all'avvio dell'istanza

Utilizza seguente il comando describe-instances:

```
aws ec2 describe-instances \
    --instance-id i-1234567890abcdef0 \
    --query "Reservations[].Instances[].KeyName" \
    --output text
```

Di seguito è riportato un output di esempio.

```
key-pair-name
```

PowerShell

Per identificare la chiave pubblica specificata all'avvio dell'istanza

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances | Select KeyName
```

Di seguito è riportato un output di esempio.

```
KeyName
-------
key-pair-name
```

Eliminazione della coppia di chiavi

È possibile eliminare una coppia di chiavi, il che rimuove la chiave pubblica archiviata in Amazon EC2. L'eliminazione di una coppia di chiavi non elimina la chiave privata corrispondente.

Quando elimini una chiave pubblica utilizzando i metodi seguenti, elimini la chiave pubblica archiviata in Amazon EC2 solo quando la coppia di chiavi è stata creata o importata. L'eliminazione di una chiave pubblica non rimuove la chiave pubblica dalle istanze a cui è stata aggiunta, né quando è

stata avviata l'istanza né successivamente. Inoltre, la chiave privata non viene eliminata dal computer locale. È possibile continuare a connettersi alle istanze avviate tramite una chiave pubblica che è stata eliminata da Amazon EC2, purché si disponga ancora del file della chiave privata (`.pem`).

> **Important**
>
> Se si sta utilizzando un gruppo Auto Scaling (ad esempio, in un ambiente Elastic Beanstalk), assicurarsi che la chiave pubblica che si sta cancellando non sia specificata in un modello di avvio o in una configurazione di avvio associati. Se Amazon EC2 Auto Scaling rileva un'istanza non integra, avvia un'istanza sostitutiva. Tuttavia, l'avvio dell'istanza non riesce se non è possibile trovare la chiave pubblica. Per ulteriori informazioni, consulta Modelli di avvio nella Guida per l'utente di Amazon EC2 Auto Scaling.

Console

Come eliminare la chiave pubblica su Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione scegli Coppie di chiavi.
3. Seleziona la coppia di chiavi da eliminare e scegli Actions (Operazioni), Delete (Elimina).
4. Nel campo di conferma immettere `Delete` e quindi scegliere Delete (Elimina).

AWS CLI

Come eliminare la chiave pubblica su Amazon EC2

Utilizza il comando delete-key-pair.

```
aws ec2 delete-key-pair --key-name my-key-pair
```

PowerShell

Come eliminare la chiave pubblica su Amazon EC2

Utilizza il cmdlet Remove-EC2KeyPair.

```
Remove-EC2KeyPair -KeyName my-key-pair
```

Aggiungi o sostituisci una chiave pubblica sull'istanza Linux

Description
Se si perde una chiave privata, si perde l'accesso a tutte le istanze che utilizzano la coppia di chiavi. Per ulteriori informazioni sulla connessione a un'istanza utilizzando una coppia di chiavi diversa da quella specificata all'avvio, vedi Ho perso la mia chiave privata.

Quando avvii un'istanza, puoi specificare una coppia di chiavi. Se si specifica una coppia di chiavi all'avvio, quando l'istanza viene avviata per la prima volta il materiale della chiave pubblica viene inserito nell'istanza Linux in una voce in `~/.ssh/authorized_keys`. Quando ti connetti per la prima volta alla tua istanza Linux tramite SSH, devi specificare l'utente predefinito e la chiave privata corrispondente alla chiave pubblica memorizzata sulla tua istanza Linux.

Dopo aver effettuato la connessione all'istanza, puoi modificare la coppia di chiavi utilizzata per accedere all'account di sistema predefinito dell'istanza aggiungendo una nuova chiave pubblica nell'istanza o sostituendo la chiave pubblica (eliminando la chiave pubblica esistente e aggiungendone una nuova) nell'istanza. È inoltre possibile rimuovere tutte le chiavi pubbliche da un'istanza.

È possibile aggiungere o sostituire una coppia di chiavi per i seguenti motivi:

- Se un utente dell'organizzazione richiede l'accesso all'utente di sistema utilizzando una coppia di chiavi separata, è possibile aggiungere tale coppia di chiavi all'istanza.
- Se si vuole impedire che qualcuno in possesso di una copia della chiave privata (file `.pem`) si colleghi alla propria istanza (ad esempio, se ha lasciato l'organizzazione), è possibile eliminare la chiave pubblica sull'istanza e sostituirla con una nuova.
- Se si crea un'AMI Linux da un'istanza, il materiale sulla chiave pubblica viene copiato dall'istanza all'AMI. Se si avvia un'istanza dall'AMI, la nuova istanza include la chiave pubblica dell'istanza originale. Per impedire a un utente che dispone della chiave privata di connettersi alla nuova istanza, è possibile rimuovere la chiave pubblica dall'istanza originale prima di creare l'AMI.

Usa queste procedure per modificare la coppia di chiavi dell'utente predefinito, ad esempio `ec2-user`. Per ulteriori informazioni sull'aggiunta di altri utenti all'istanza, consulta la documentazione per il sistema operativo dell'istanza.

Per aggiungere o sostituire una coppia di chiavi

1. Creare una nuova coppia di chiavi tramite la console Amazon EC2 o uno strumento di terze parti.
2. Recuperare la chiave pubblica da una nuova coppia di chiavi. Per ulteriori informazioni, consulta Recupero del materiale delle chiavi pubbliche.
3. Connettiti alla tua istanza.
4. Nell'istanza, utilizzando l'editor di testo che preferisci, apri il file `.ssh/authorized_keys`. Incolla le informazioni relative alla chiave pubblica della tua nuova coppia di chiavi sotto le informazioni relative alla chiave pubblica esistente, quindi salva il file.
5. Disconnettiti dall'istanza. Verifica di poterti connettere alla tua istanza utilizzando il file della chiave privata della nuova coppia di chiavi.
6. Se usi Auto Scaling, EC2 fleet o un modello di avvio per avviare le istanze, controlla se la coppia di chiavi che stai sostituendo è specificata nel modello o nella configurazione di avvio. Altrimenti, l'avvio dell'istanza avrà esito negativo.
7. (Facoltativo) Se si sostituisce una coppia di chiavi esistente, connettersi all'istanza ed eliminare le informazioni sulla chiave pubblica per la coppia di chiavi originale dal file `.ssh/authorized_keys`.

Come rimuovere una chiave pubblica da un'istanza

1. Connettiti alla tua istanza.
2. Utilizzare l'editor di testo preferito, aprire il file `.ssh/authorized_keys` nell'istanza. Eliminare le informazioni sulla chiave pubblica e quindi salvare il file.

> **Warning**
>
> Se rimuovi tutte le chiavi pubbliche da un'istanza e ti disconnetti da essa, non potrai ricollegarti all'istanza a meno che non abbia configurato un metodo alternativo per effettuare l'accesso.

Verifica dell'impronta digitale della coppia di chiavi

Per verificare l'impronta digitale della coppia di chiavi, confronta l'impronta digitale visualizzata nella pagina Coppie di chiavi della console Amazon EC2, o restituita dal comando describe-key-pairs, con

l'impronta digitale generata utilizzando la chiave privata sul computer locale. Queste impronte digitali devono corrispondere.

Quando Amazon EC2 calcola un'impronta digitale, potrebbe accodare un padding all'impronta digitale con caratteri =. Altri strumenti, ad esempio ssh-keygen, potrebbero omettere questo padding.

Se stai cercando di verificare l'impronta digitale dell'istanza EC2 Linux, non l'impronta digitale della coppia di chiavi, consulta Ottenimento dell'impronta dell'istanza.

Come vengono calcolate le impronte digitali

Amazon EC2 utilizza diverse funzioni hash per calcolare le impronte digitali per le coppie di chiavi RSA e ED25519. Inoltre, per le coppie di chiavi RSA, Amazon EC2 calcola le impronte digitali in modo diverso utilizzando diverse funzioni hash a seconda che la coppia di chiavi sia stata creata da Amazon EC2 o importata in Amazon EC2.

Nella tabella seguente sono elencate le funzioni hash utilizzate per calcolare le impronte digitali per le coppie di chiavi RSA e ED25519 create da Amazon EC2 e importate in Amazon EC2.

(Istanze Linux) Funzioni hash utilizzate per calcolare le impronte digitali

Fonte di coppia di chiavi	Coppie di chiavi RSA (Windows e Linux)	Coppie di chiavi ED25519 (Linux)
Create da Amazon EC2	SHA-1	SHA-256
Importate in Amazon EC2	MD5[1]	SHA-256

[1] Se importi una chiave RSA pubblica in Amazon EC2, l'impronta digitale viene calcolata utilizzando una funzione hash MD5. Ciò è vero indipendentemente da come è stata creata la coppia di chiavi, ad esempio utilizzando uno strumento di terze parti o generando una nuova chiave pubblica da una chiave privata esistente creata con Amazon EC2.

Utilizzare la stessa coppia di chiavi in diverse regioni

Se prevedi di utilizzare la stessa coppia di chiavi per connetterti a istanze in istanze diverse Regioni AWS, devi importare la chiave pubblica in tutte le regioni in cui la utilizzerai. Se utilizzi Amazon EC2 per creare la coppia di chiavi, puoi Recupero del materiale delle chiavi pubbliche in modo da poter importare la chiave pubblica nelle altre regioni.

Note

- Se si crea una coppia di chiavi RSA utilizzando Amazon EC2 e poi una chiave pubblica dalla chiave privata Amazon EC2, le chiavi pubbliche importate avranno un'impronta digitale diversa rispetto alla chiave pubblica originale. Questo perché l'impronta digitale della chiave RSA originale creata con Amazon EC2 viene calcolata utilizzando una funzione SHA-1 hash, mentre l'impronta digitale delle chiavi RSA importate viene calcolata utilizzando una funzione hash MD5.
- Per le coppie di chiavi ED25519, le impronte digitali saranno le stesse indipendentemente dal fatto che siano state create da Amazon EC2 o importate in Amazon EC2, poiché la stessa funzione hash viene utilizzata per calcolare l'impronta digitale. SHA-256

Creazione di un'impronta digitale dalla chiave privata

Utilizza uno dei seguenti comandi per generare un'impronta digitale dalla chiave privata sul computer locale.

Se si sta utilizzando un computer locale Windows, è possibile eseguire i comandi seguenti tramite Windows Subsystem per Linux (WSL). Installa il WSL e una distribuzione Linux seguendo le istruzioni riportate nella guida Come installare Linux in Windows con WSL. L'esempio riportato nelle istruzioni installa la distribuzione Ubuntu di Linux, ma si può installare qualunque distribuzione. Affinché vengano applicate le modifiche, ti verrà chiesto di riavviare il computer.

- Se la coppia di chiavi è stata creata tramite Amazon EC2

  Utilizza gli strumenti di OpenSSL per generare un'impronta digitale come riportato negli esempi seguenti.

  Per le coppie di chiavi RSA:

```
openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt |
 openssl sha1 -c
```

  (Istanze Linux) Per le coppie di chiavi ED25519:

```
ssh-keygen -l -f path_to_private_key
```

- (Solo coppie di chiavi RSA) Se hai importato la chiave pubblica in Amazon EC2

  Puoi seguire questa procedura indipendentemente dalla modalità con cui hai creato la coppia di chiavi, ad esempio utilizzando uno strumento di terzi o generando una nuova chiave pubblica da una chiave privata esistente creata utilizzando Amazon EC2

  Utilizza gli strumenti di OpenSSL per generare l'impronta digitale come riportato nell'esempio seguente.

  ```
  openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
  ```

- Se una coppia di chiavi OpenSSH è stata creata mediante OpenSSH 7.8 o versioni successive e la chiave pubblica è stata importata in Amazon EC2

  Utilizza ssh-keygen per generare un'impronta digitale come riportato negli esempi seguenti.

  Per le coppie di chiavi RSA:

  ```
  ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER
   | openssl md5 -c
  ```

  (Istanze Linux) Per le coppie di chiavi ED25519:

  ```
  ssh-keygen -l -f path_to_private_key
  ```

Gruppi di sicurezza Amazon EC2 per le istanze EC2

Un gruppo di sicurezza funge da firewall virtuale per le istanze EC2 per controllare il traffico in entrata e quello in uscita. Le regole in entrata controllano il traffico in entrata verso l'istanza e le regole in uscita controllano il traffico in uscita dall'istanza. Quando avvii un'istanza puoi specificare uno o più gruppi di sicurezza. Se non specifichi un gruppo di sicurezza, Amazon EC2 usa il gruppo di sicurezza predefinito per il VPC. Dopo l'avvio di un'istanza, è possibile modificare i relativi gruppi di sicurezza.

La sicurezza è una responsabilità condivisa AWS tra voi. Per ulteriori informazioni, vedereSicurezza in Amazon EC2. AWS fornisce i gruppi di sicurezza come uno degli strumenti per proteggere le istanze e devi configurarli per soddisfare le tue esigenze di sicurezza. Se i gruppi di sicurezza non soddisfano pienamente i requisiti, oltre a utilizzare i gruppi di sicurezza è possibile mantenere il firewall su tutte le istanze.

Prezzi

L'utilizzo di gruppi di sicurezza non comporta costi supplementari.

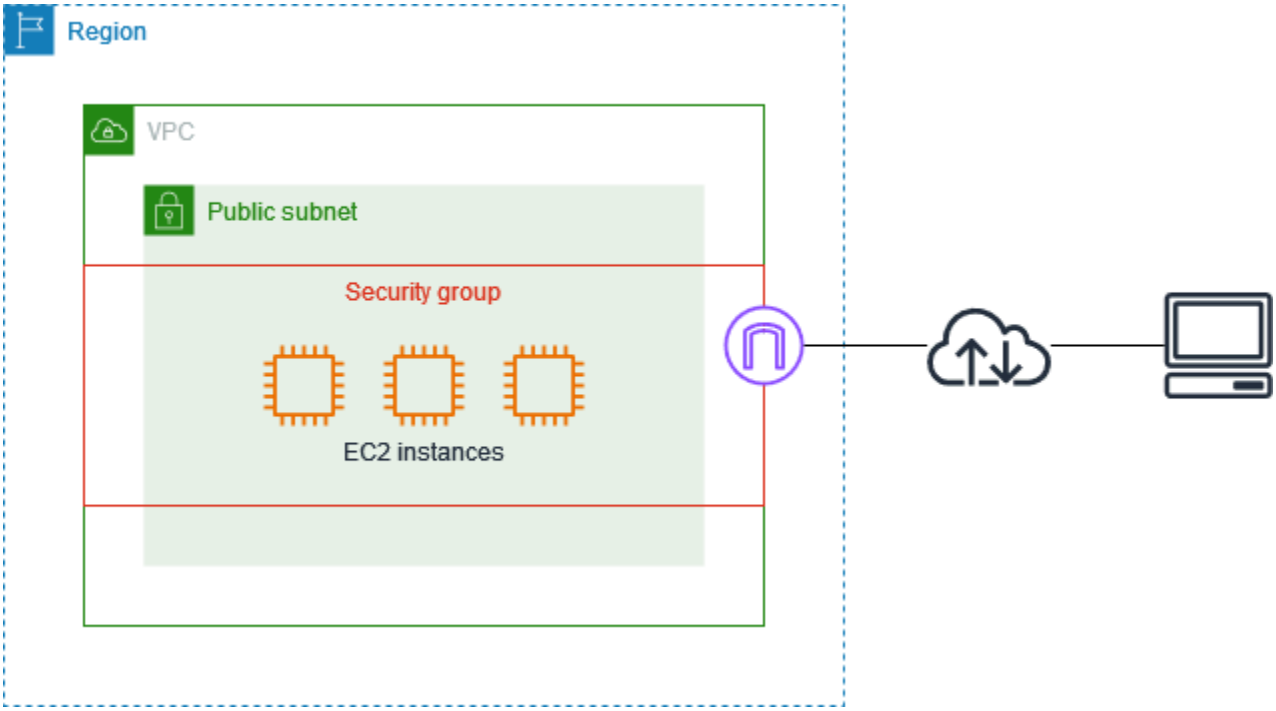
Indice

- Panoramica di
- Creare un gruppo di sicurezza per l'istanza Amazon EC2.
- Modifica i gruppi di sicurezza per l'istanza Amazon EC2.
- Eliminare un gruppo di sicurezza Amazon EC2
- Monitoraggio della connessione al gruppo di sicurezza Amazon EC2
- Regole del gruppo di sicurezza per diversi casi d'uso

Panoramica di

È possibile associare ogni istanza a più gruppi di sicurezza e associare ogni gruppo di sicurezza a più istanze. A ciascun gruppo di sicurezza si possono aggiungere regole che permettono il traffico da e verso le istanze a esso associate. Puoi modificare le regole di un gruppo di sicurezza in qualsiasi momento. Regole nuove e modificate vengono applicate automaticamente a tutte le istanze associate al gruppo di sicurezza. Quando Amazon EC2 decide se permettere al traffico di raggiungere un'istanza, valuta tutte le regole da tutti i gruppi di sicurezza associati all'istanza. Per ulteriori informazioni, consulta Regole del gruppo di sicurezza nella Guida per l'utente di Amazon VPC.

Il diagramma seguente mostra un VPC con una sottorete, un gateway Internet e un gruppo di sicurezza. La sottorete contiene delle istanze EC2. Il gruppo di sicurezza è associato alle istanze. L'unico traffico che raggiunge l'istanza è quello consentito dalle regole del gruppo di sicurezza. Ad esempio, se il gruppo di sicurezza contiene una regola che consente il traffico SSH dalla tua rete, allora puoi connetterti all'istanza dal tuo computer attraverso SSH. Se il gruppo di sicurezza contiene una regola che consente tutto il traffico proveniente dalle risorse a esso associate, ogni istanza può ricevere tutto il traffico inviato dalle altre istanze.



I gruppi di sicurezza sono stateful — Se invii una richiesta da un'istanza, il traffico in risposta alla richiesta è autorizzato a entrare, indipendentemente dalle regole dei gruppi di sicurezza in entrata. Inoltre, I risposte al traffico in entrata autorizzato possono uscire indipendentemente dalle regole in uscita. Per ulteriori informazioni, consulta Monitoraggio delle connessioni.

Creare un gruppo di sicurezza per l'istanza Amazon EC2.

I gruppi di sicurezza fungono da firewall per le istanze associate, controllando sia il traffico in entrata che in uscita a livello di istanza. È possibile aggiungere regole a un gruppo di sicurezza che consentono di connettersi all'istanza tramite SSH (istanze Linux) o RDP (istanze Windows). È inoltre possibile aggiungere regole che consentono il traffico client, ad esempio il traffico HTTP e HTTPS destinato a un server Web.

Puoi associare un gruppo di sicurezza a un'istanza quando la avvii. Quando aggiungi o rimuovi delle regole da dei gruppi di sicurezza associati, queste modifiche vengono applicate automaticamente a tutte le istanze a cui hai associato il gruppo di sicurezza.

Dopo l'avvio di un'istanza, puoi associare altri gruppi di sicurezza. Per ulteriori informazioni, consulta Modifica i gruppi di sicurezza per l'istanza Amazon EC2..

Puoi aggiungere regole del gruppo di sicurezza in entrata e in uscita durante la creazione di un gruppo di sicurezza oppure in un secondo momento. Per ulteriori informazioni, consulta

Configurazione delle regole per i gruppi di sicurezza. Per vedere esempi di regole che è possibile aggiungere a un gruppo di sicurezza, consulta Regole del gruppo di sicurezza per diversi casi d'uso.

Considerazioni

- I nuovi gruppi di sicurezza hanno solo una regola in uscita che autorizza tutto il traffico a lasciare la risorsa. Devi aggiungere le regole per autorizzare qualsiasi tipo di traffico in entrata o per limitare quello in uscita.
- Quando configuri un'origine per una regola che consente l'accesso SSH o RDP alle tue istanze, non consentire l'accesso da nessuna parte, perché in questo modo consentiresti l'accesso all'istanza da tutti gli indirizzi IP su Internet. Questo è accettabile per un breve periodo di tempo in un ambiente di test, ma non è sicuro per gli ambienti di produzione.
- Se esistono più regole per una determinata porta, Amazon EC2 applica la regola più permissiva. Ad esempio, se disponi di una regola che autorizza l'accesso alla porta TCP 22 (SSH) dall'indirizzo IP 203.0.113.1 e un'altra regola che autorizza l'accesso alla porta TCP 22 da ovunque, allora chiunque può accedere alla porta TCP 22.
- Puoi associare più gruppi di sicurezza a un'istanza. Pertanto, un'istanza può disporre di centinaia di regole valide. Questo può causare problemi nell'accesso all'istanza. È consigliabile comprimere le regole il più possibile.
- Quando specifichi un gruppo di sicurezza come l'origine o la destinazione di una regola, la regola influenza tutte le istanze associate al gruppo di sicurezza. Il traffico in entrata è autorizzato in base agli indirizzi IP privati delle istanze associate al gruppo di sicurezza di origine (e non in base agli indirizzi IP elastici o pubblici). Per ulteriori informazioni sugli indirizzi IP, consulta Indirizzamento IP per le istanze Amazon EC2.
- Per impostazione predefinita, Amazon EC2 blocca il traffico sulla porta 25. Per ulteriori informazioni, consulta Restrizione sull'e-mail inviata tramite la porta 25.

Console

Per creare un gruppo di sicurezza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fare clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
3. Scegliere Create Security Group (Crea gruppo di sicurezza).
4. Immettere un nome descrittivo e una breve descrizione del gruppo di sicurezza. Non è possibile modificare il nome e la descrizione di un gruppo di sicurezza dopo averlo creato.

5. Per VPC, scegli il VPC su cui eseguirai le tue istanze Amazon EC2.
6. (Facoltativo) Per aggiungere regole in entrata, scegli Regole in entrata. Per ogni regola, scegli Aggiungi regola e specifica il protocollo, la porta e l'origine. Ad esempio, per consentire il traffico SSH, scegli SSH per Tipo e specifica l'indirizzo IPv4 pubblico del tuo computer o della tua rete come Fonte.
7. (Facoltativo) Per aggiungere regole in uscita, scegli Regole in uscita. Per ogni regola, scegli Aggiungi regola e specifica il protocollo, la porta e la destinazione. Altrimenti, puoi mantenere la regola predefinita, che autorizza tutto il traffico in uscita.
8. (Facoltativo) Per aggiungere un tag, scegli Add new tag (Aggiungi nuovo tag) e immetti la chiave e il valore del tag.
9. Scegliere Create Security Group (Crea gruppo di sicurezza).

AWS CLI

Per creare un gruppo di sicurezza

Utilizza il seguente comando create-security-group.

```
aws ec2 create-security-group \
    --group-name my-security-group \
    --description "my security group" \
    --vpc-id vpc-1234567890abcdef0
```

Per esempi che aggiungono regole, consulta the section called "Configurazione delle regole per i gruppi di sicurezza".

PowerShell

Per creare un gruppo di sicurezza

Utilizza il cmdlet New-EC2SecurityGroup.

```
New-EC2SecurityGroup `
    -GroupName my-security-group `
    -Description "my security group" `
    -VpcId vpc-1234567890abcdef0
```

Per esempi che aggiungono regole, consulta the section called "Configurazione delle regole per i gruppi di sicurezza".

Modifica i gruppi di sicurezza per l'istanza Amazon EC2.

È possibile specificare i gruppi di sicurezza per le istanze Amazon EC2 durante l'avvio. Dopo l'avvio di un'istanza, è possibile aggiungere o rimuovere i gruppi di sicurezza. Puoi anche aggiungere, rimuovere o modificare le regole dei gruppi di sicurezza per i gruppi di sicurezza associati in qualsiasi momento.

I gruppi di sicurezza sono associati alle interfacce di rete. Quando si aggiungono o rimuovono gruppi di sicurezza, cambiano anche i gruppi di sicurezza associati all'interfaccia di rete primaria. Si possono modificare anche i gruppi di sicurezza associati a qualunque interfaccia di rete secondaria. Per ulteriori informazioni, consulta Modifica degli attributi dell'interfaccia di rete.

Processi

- Aggiungi o rimuovi gruppi di sicurezza
- Configurazione delle regole per i gruppi di sicurezza

Aggiungi o rimuovi gruppi di sicurezza

Dopo avere avviato un'istanza, puoi aggiungere o rimuovere gruppi di sicurezza dall'elenco dei gruppi di sicurezza associati. Se associ a un'istanza più gruppi di sicurezza, le regole di ciascun gruppo di sicurezza vengono aggregate efficacemente per creare un unico set di regole. Amazon EC2 utilizza questo set di regole per determinare se consentire il traffico o meno.

Requisiti

- L'istanza deve trovarsi nello stato `running` o `stopped`.

Console

Per modificare i gruppi di sicurezza per un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza, quindi scegliere Actions (Operazioni), Security (Sicurezza), Change security groups (Cambia gruppi di sicurezza).
4. Per Gruppi di sicurezza associati, selezionare un gruppo di sicurezza dall'elenco e scegliere Aggiungi gruppo di sicurezza.

Per rimuovere un gruppo di sicurezza già associato, scegliere Rimuovi per tale gruppo di sicurezza.

5. Scegli Save (Salva).

AWS CLI

Per modificare i gruppi di sicurezza per un'istanza

Utilizza il seguente comando modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --groups sg-1234567890abcdef0
```

PowerShell

Per modificare i gruppi di sicurezza per un'istanza

Utilizza il cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -Group sg-1234567890abcdef0
```

Configurazione delle regole per i gruppi di sicurezza

Dopo aver creato un gruppo di sicurezza, puoi aggiungere, aggiornare ed eliminare le relative regole. Quando aggiungi, aggiorni o elimini una regola, la modifica viene applicata automaticamente alle risorse associate al gruppo di sicurezza.

Per vedere esempi di regole che è possibile aggiungere a un gruppo di sicurezza, consulta Regole del gruppo di sicurezza per diversi casi d'uso.

Autorizzazioni richieste

Prima di iniziare, assicurati di disporre delle autorizzazioni richieste. Per ulteriori informazioni, consulta Esempio: utilizzo dei gruppi di sicurezza.

Protocolli e porte

- Con la console, quando selezioni un tipo predefinito, il protocollo e l'intervallo di porte vengono specificati automaticamente. Per inserire un intervallo di porte, dovrai selezionare uno dei seguenti tipi personalizzati: TCP personalizzato o UDP personalizzato.
- Con AWS CLI, puoi aggiungere una singola regola con una singola porta utilizzando le `--port` opzioni `--protocol` and. Per aggiungere più regole o una regola con un intervallo di porte, seleziona l'opzione `--ip-permissions`.

Origini e destinazioni

- Tramite la console potrai indicare i seguenti dati come origine per le regole in entrata o come destinazione per le regole in uscita:
  - Personalizzato: un intervallo CIDR IPv4, un intervallo CIDR IPv6, un gruppo di sicurezza o un elenco di prefissi.
  - Anywhere-IPv4— La 0.0.0. 0/0 Blocco CIDR IPv4.
  - Anywhere-IPv6— Il blocco CIDR: :/0 IPv6.
  - My IP: l'indirizzo IPv4 pubblico del computer locale.
- Con AWS CLI, è possibile specificare un blocco CIDR IPv4 utilizzando l'opzione o un gruppo di sicurezza utilizzando l'`--cidr`opzione. `--source-group` Per indicare un elenco di prefissi o un intervallo CIDR IPv6, utilizza l'opzione `--ip-permissions`.

> **Warning**
>
> Se aggiungi delle regole in entrata per le porte 22 (SSH) o 3389 (RDP), è consigliabile autorizzare l'accesso all'istanza solo l'indirizzo IP o l'intervallo di indirizzi specifico. Se lo desideri Anywhere-IPv4, consenti al traffico proveniente da tutti gli indirizzi IPv4 di accedere alle tue istanze utilizzando il protocollo specificato. Se lo desideri Anywhere-IPv6, consenti al traffico proveniente da tutti gli indirizzi IPv6 di accedere alle tue istanze utilizzando il protocollo specificato.

Console

Configurazione delle regole per i gruppi di sicurezza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.
3. Selezionare il gruppo di sicurezza.
4. Per modificare le regole in entrata, scegli Modifica regole in entrata dalla scheda Azioni o dalla scheda Regole in entrata.

   a. Per aggiungere una regola, scegli Aggiungi regola e immetti il tipo, il protocollo, la porta e l'origine della regola.

      Se il tipo è TCP o UDP, è necessario immettere l'intervallo di porte consentito. Se si sceglie un protocollo ICMP personalizzato, occorre scegliere il nome del tipo ICMP da Protocollo e, se applicabile, il nome del codice da Intervallo di porte. Se scegli qualsiasi altro tipo, il protocollo e l'intervallo di porte vengono configurati automaticamente.

   b. Per aggiornare una regola, modificane il protocollo, la descrizione e l'origine in base alle esigenze. Tuttavia, il tipo di origine non può essere modificato. Ad esempio, se l'origine è un blocco CIDR IPv4, non è possibile specificare un blocco CIDR IPv6, un elenco di prefissi o un gruppo di sicurezza.

   c. Per eliminare una regola, seleziona il pulsante Elimina corrispondente.

5. Per modificare le regole in uscita, scegli Modifica regole in uscita dalla scheda Azioni o dalla scheda Regole in uscita.

   a. Per aggiungere una regola, scegli Aggiungi regola e immetti il tipo, il protocollo, la porta e la destinazione della regola. Facoltativamente, è possibile inserire una descrizione.

      Se il tipo è TCP o UDP, è necessario immettere l'intervallo di porte consentito. Se si sceglie un protocollo ICMP personalizzato, occorre scegliere il nome del tipo ICMP da Protocollo e, se applicabile, il nome del codice da Intervallo di porte. Se scegli qualsiasi altro tipo, il protocollo e l'intervallo di porte vengono configurati automaticamente.

   b. Per aggiornare una regola, modificane il protocollo, la descrizione e l'origine in base alle esigenze. Tuttavia, il tipo di origine non può essere modificato. Ad esempio, se l'origine è un blocco CIDR IPv4, non è possibile specificare un blocco CIDR IPv6, un elenco di prefissi o un gruppo di sicurezza.

   c. Per eliminare una regola, seleziona il pulsante Elimina corrispondente.

6. Scegliere Salva regole.

AWS CLI

Per aggiungere regole del gruppo di sicurezza

Utilizza il comando authorize-security-group-ingress per aggiungere regole in entrata. Il seguente esempio consente il traffico SSH in entrata dai blocchi CIDR nell'elenco di prefissi specificato.

```
aws ec2 authorize-security-group-ingress \
    --group-id sg-1234567890abcdef0 \
    --ip-permissions
 'IpProtocol=tcp,FromPort=22,ToPort=22,PrefixListIds=[{PrefixListId=pl-
f8a6439156EXAMPLE}]'
```

Utilizza il comando authorize-security-group-egress per aggiungere regole in uscita. Il seguente esempio consente il traffico TCP in uscita sulla porta 80 alle istanze con il gruppo di sicurezza specificato.

```
aws ec2 authorize-security-group-egress \
    --group-id sg-1234567890abcdef0 \
    --ip-permissions
 'IpProtocol=tcp,FromPort=80,ToPort=80,UserIdGroupPairs=[{GroupId=sg-0aad1c26bb6EXAMPLE}]'
```

Per rimuovere le regole per del gruppo di sicurezza

Utilizza il comando revoke-security-group-ingress per rimuovere una regola in entrata.

```
aws ec2 revoke-security-group-egress \
    --group id sg-1234567890abcdef0 \
    --security-group-rule-ids sgr-09ed298024EXAMPLE
```

Utilizza il comando revoke-security-group-egress per rimuovere una regola in uscita.

```
aws ec2 revoke-security-group-ingress \
    --group id sg-1234567890abcdef0 \
    --security-group-rule-ids sgr-0352250c1aEXAMPLE
```

Per modificare le regole del gruppo di sicurezza

Utilizza il comando modify-security-group-rules. Il seguente esempio modifica l'intervallo CIDR IPv4 della regola del gruppo di sicurezza specificato.

```
aws ec2 modify-security-group-rules \
    --group id sg-1234567890abcdef0 \
    --security-group-rules
 'SecurityGroupRuleId=sgr-09ed298024EXAMPLE,SecurityGroupRule={IpProtocol=tcp,FromPort=80,To
```

PowerShell

Per aggiungere regole del gruppo di sicurezza

Usa il Grant-EC2SecurityGroupIngress cmdlet per aggiungere regole in entrata. Il seguente esempio consente il traffico SSH in entrata dai blocchi CIDR nell'elenco di prefissi specificato.

```
$plid = New-Object -TypeName Amazon.EC2.Model.PrefixListId
$plid.Id = "pl-f8a6439156EXAMPLE"
Grant-EC2SecurityGroupIngress `
    -GroupId sg-1234567890abcdef0 `
    -IpPermission @{IpProtocol="tcp"; FromPort=22; ToPort=22; PrefixListIds=$plid}
```

Utilizzare il Grant-EC2SecurityGroupEgress cmdlet per aggiungere regole in uscita. Il seguente esempio consente il traffico TCP in uscita sulla porta 80 alle istanze con il gruppo di sicurezza specificato.

```
$uigp = New-Object -TypeName Amazon.EC2.Model.UserIdGroupPair
$uigp.GroupId = "sg-0aad1c26bb6EXAMPLE"
Grant-EC2SecurityGroupEgress `
    -GroupId sg-1234567890abcdef0 `
    -IpPermission @{IpProtocol="tcp"; FromPort=80; ToPort=80; UserIdGroupPairs=
$uigp}
```

Per rimuovere le regole per del gruppo di sicurezza

Utilizzare il Revoke-EC2SecurityGroupIngress cmdlet per rimuovere le regole in entrata.

```
Revoke-EC2SecurityGroupIngress `
    -GroupId sg-1234567890abcdef0 `
    -SecurityGroupRuleId sgr-09ed298024EXAMPLE
```

Utilizzare il Revoke-EC2SecurityGroupEgress cmdlet per rimuovere le regole in uscita.

```
Revoke-EC2SecurityGroupEgress `
    -GroupId sg-1234567890abcdef0 `
    -SecurityGroupRuleId sgr-0352250c1aEXAMPLE
```

Per modificare le regole del gruppo di sicurezza

Utilizza il cmdlet Edit-EC2SecurityGroupRule. Il seguente esempio modifica l'intervallo CIDR IPv4 della regola del gruppo di sicurezza specificato.

```
$sgrr = New-Object -TypeName Amazon.EC2.Model.SecurityGroupRuleRequest
$sgrr.IpProtocol = "tcp"
$sgrr.FromPort = 80
$sgrr.ToPort = 80
$sgrr.CidrIpv4 = "0.0.0.0/0"
$sgr = New-Object -TypeName Amazon.EC2.Model.SecurityGroupRuleUpdate
$sgr.SecurityGroupRuleId = "sgr-09ed298024EXAMPLE"
$sgr.SecurityGroupRule = $sgrr
Edit-EC2SecurityGroupRule  `
    -GroupId sg-1234567890abcdef0 `
    -SecurityGroupRule $sgr
```

Eliminare un gruppo di sicurezza Amazon EC2

Quando non hai più bisogno di un gruppo di sicurezza che hai creato per le istanze Amazon EC2, puoi eliminarlo.

Requisiti

- Il gruppo di sicurezza non può essere associato a un'istanza o un'interfaccia di rete.
- Il gruppo di sicurezza non può essere utilizzato come riferimento da una regola di un altro gruppo di sicurezza.

Console

Per eliminare un gruppo di sicurezza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. (Facoltativo) Per verificare che il gruppo di sicurezza non sia associato a un'istanza, procedi come segue:

a. Fai clic su Gruppi di sicurezza nel riquadro di navigazione.
b. Copia l'ID del gruppo di sicurezza da eliminare.
c. Nel riquadro di navigazione, scegliere Instances (Istanze).
d. Nella barra di ricerca, aggiungi il filtro equivalente degli ID del gruppo di sicurezza e incolla l'ID del gruppo di sicurezza. Se non ci sono risultati, il gruppo di sicurezza non è associato a un'istanza. In caso contrario, è necessario disassociare il gruppo di sicurezza prima di poterlo eliminare.

3. Fai clic su Gruppi di sicurezza nel riquadro di navigazione.
4. Seleziona il gruppo di sicurezza e scegli Operazioni, Elimina gruppi di sicurezza.
5. Se hai selezionato più di un gruppo di sicurezza, ti verrà richiesta la conferma. Se alcuni gruppi di sicurezza non possono essere eliminati, viene visualizzato lo stato di ciascun gruppo di sicurezza, che indica se verrà eliminato. Per confermare l'eliminazione, immetti Elimina.
6. Scegli Elimina.

AWS CLI

Per eliminare un gruppo di sicurezza

Utilizza il seguente comando delete-security-group.

```
aws ec2 delete-security-group --group-id sg-1234567890abcdef0
```

PowerShell

Per eliminare un gruppo di sicurezza

Utilizza il cmdlet Remove-EC2SecurityGroup.

```
Remove-EC2SecurityGroup -GroupId sg-1234567890abcdef0
```

Monitoraggio della connessione al gruppo di sicurezza Amazon EC2

I gruppi di sicurezza utilizzano il monitoraggio delle connessioni per tracciare le informazioni sul traffico da e verso l'istanza. Le regole si applicano in base allo stato della connessione per stabilire se

il traffico è autorizzato o negato. Con questo approccio, i gruppi di sicurezza sono con stato. Ovvero, le risposte al traffico in entrata possono uscire dall'istanza a prescindere dalle regole del gruppo di sicurezza in uscita, e viceversa.

Ad esempio, supponiamo di avviare un comando come netcat o similare sulle istanze dal computer di casa e che le regole del gruppo di sicurezza in entrata consentano il traffico ICMP. Le informazioni sulla connessione (incluse le informazioni sulla porta) vengono monitorate. Il traffico in risposta dall'istanza per il comando non viene monitorato come nuova richiesta, ma come connessione stabilita e può uscire dall'istanza, anche se le regole del gruppo di sicurezza in uscita limitano il traffico ICMP in uscita.

Per i protocolli diversi da TCP, UDP o ICMP, vengono monitorati solo l'indirizzo IP e il numero di protocollo. Se l'istanza invia traffico a un altro host e l'host invia lo stesso tipo di traffico verso l'istanza entro 600 secondi, verrà accettato dal gruppo di sicurezza dell'istanza a prescindere dalle regole del gruppo di sicurezza in entrata. Il gruppo di sicurezza lo accetta perché considerato traffico di risposta al traffico originale.

Quando si modifica una regola del gruppo di sicurezza, le connessioni tracciate non vengono interrotte immediatamente. Il gruppo di sicurezza continua a consentire i pacchetti fino al timeout delle connessioni esistenti. Per avere la certezza che il traffico venga interrotto immediatamente o che tutto il traffico sia soggetto alle regole del firewall indipendentemente dallo stato di tracciamento, è possibile utilizzare una lista di controllo degli accessi di rete per la sottorete. Le liste di controllo degli accessi di rete sono stateless, pertanto non autorizzano automaticamente il traffico di risposta. L'aggiunta di una lista di controllo degli accessi di rete che blocca il traffico in entrambe le direzioni interrompe le connessioni esistenti. Per ulteriori informazioni, consulta la sezione relativa alle Liste di controllo degli accessi di rete nella Guida per l'utente di Amazon VPC.

> **Note**
>
> I gruppi di sicurezza non hanno alcun effetto sul traffico DNS da o verso il resolver Route 53, a volte indicato come «indirizzo IP VPC+2" (vedi Cos'è Amazon Route 53 Resolver? https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver.htmlnella Amazon Route 53 Developer Guide) o «AmazonProvidedDNS» (consulta i set di opzioni Work with DHCP nella Amazon Virtual Private Cloud User Guide). Se desideri filtrare le richieste DNS tramite il risolutore Route 53, puoi abilitare DNS Firewall per il risolutore Route 53 (consulta DNS Firewall per il risolutore Route 53 nella Guida per sviluppatori di Amazon Route 53).

Connessioni non tracciate

Non vengono monitorati tutti i flussi di traffico. Se una regola del gruppo di sicurezza consente flussi TCP o UDP per tutto il traffico (0.0.0). 0/0 o: :/0) e c'è una regola corrispondente nella direzione opposta che consente tutto il traffico di risposta (0.0.0. 0/0 o: :/0) per qualsiasi porta (0-65535), allora quel flusso di traffico non viene tracciato, a meno che non faccia parte di una connessione tracciata automaticamente. ??? Il traffico in risposta per un flusso non monitorato può scorrere in base alla regola in entrata o in uscita che autorizza il traffico in risposta, non in base alle informazioni di monitoraggio.

Un flusso di traffico non monitorato viene interrotto immediatamente se la regola che permette il flusso è rimossa o modificata. Ad esempio, se hai un file aperto (0.0.0. 0/0) regola in uscita e si rimuove una regola che consente tutto (0.0.0. 0/0) traffico SSH (porta TCP 22) in entrata verso l'istanza (o modificandolo in modo tale che la connessione non sia più consentita), le connessioni SSH esistenti all'istanza vengono immediatamente interrotte. Poiché la connessione non è stata in precedenza tracciata, la modifica interromperà la connessione. D'altra parte, se disponi di una regola in entrata più rigida che inizialmente consente una connessione SSH (ovvero la connessione è stata monitorata), ma modifichi la regola per non consentire più nuove connessioni dall'indirizzo del client SSH corrente, la connessione SSH esistente non verrà interrotta poiché è monitorata.

Connessioni monitorate automaticamente

Le connessioni effettuate tramite il seguente vengono monitorate automaticamente, anche se la configurazione del gruppo di sicurezza non lo richiede altrimenti:

- Egress-only gateway internet
- Acceleratori di Global Accelerator
- Gateway NAT
- Endpoint Firewall Network Firewall
- Network Load Balancers
- AWS PrivateLink (endpoint VPC di interfaccia)
- AWS Lambda (interfacce di rete elastiche Hyperplane)
- Endpoint gateway DynamoDB: ogni connessione a DynamoDB utilizza 2 voci conntrack.

Permessi di tracciamento delle connessioni

Amazon EC2 definisce il numero massimo di connessioni che possono essere monitorate per ogni istanza. Una volta raggiunto il massimo, tutti i pacchetti inviati o ricevuti vengono eliminati perché non è possibile stabilire una nuova connessione. In questo caso, le applicazioni che inviano e ricevono pacchetti non possono comunicare correttamente. Utilizza il parametro delle prestazioni di rete `conntrack_allowance_available` per determinare il numero di connessioni tracciate ancora disponibili per quel tipo di istanza.

Per determinare se i pacchetti sono stati eliminati perché il traffico di rete per l'istanza ha superato il numero massimo di connessioni che possono essere monitorate, utilizza il parametro delle prestazioni di rete `conntrack_allowance_exceeded`. Per ulteriori informazioni, consulta Monitoraggio delle prestazioni di rete per le impostazioni ENA dell'istanza EC2.

Con Elastic Load Balancing, se si supera il numero massimo di connessioni che è possibile monitorare per istanza, si consiglia di ridimensionare il numero di istanze registrate con il load balancer o la dimensione delle istanze registrate con il load balancer.

Best practice per il monitoraggio delle connessioni

Il routing asimmetrico, in cui il traffico entra in un'istanza attraverso un'interfaccia di rete ed esce da un'altra interfaccia di rete, può ridurre le prestazioni di picco che un'istanza può raggiungere se i flussi vengono tracciati.

Per mantenere le massime prestazioni e ottimizzare la gestione delle connessioni quando il monitoraggio delle connessioni è abilitato per i gruppi di sicurezza, consigliamo la seguente configurazione:

- Evita topologie di routing asimmetriche, se possibile.
- Invece di utilizzare i gruppi di sicurezza per il filtraggio, utilizza gli ACL di rete.
- Se devi utilizzare gruppi di sicurezza con il tracciamento delle connessioni, configura il timeout di tracciamento delle connessioni in modo che sia inattivo per il minor tempo possibile. Per ulteriori dettagli sul timeout del monitoraggio delle connessioni inattive, consulta la sezione seguente.
- Con i timeout predefiniti più brevi sulle istanze Nitrov6, le applicazioni con connessioni di lunga durata (come pool di connessioni al database, connessioni HTTP persistenti o carichi di lavoro in streaming) dovrebbero configurare un valore appropriato all'avvio dell'istanza. `TcpEstablishedTimeout`

- Per connessioni di lunga durata, configura TCP keep lives in modo che venga inviato a intervalli inferiori a 5 minuti per garantire che le connessioni rimangano aperte e mantengano il loro stato tracciato. Questo aiuta a prevenire l'interruzione delle connessioni a causa di un timeout di inattività e riduce il sovraccarico del ripristino della connessione.

Per ulteriori informazioni sull'ottimizzazione della performance sul sistema Nitro, consultare Considerazioni sul sistema Nitro per l'ottimizzazione delle prestazioni.

Timeout di tracciamento delle connessioni inattive

Il gruppo di sicurezza tiene traccia di ogni connessione stabilita per garantire che i pacchetti restituiti vengano consegnati come previsto. Per ciascuna istanza esiste un numero massimo di connessioni che possono essere monitorate. Le connessioni che rimangono inattive possono portare all'esaurimento del tracciamento delle connessioni, impedire il tracciamento delle connessioni ed eliminare i pacchetti. Ora puoi impostare il timeout in secondi per il tracciamento delle connessioni inattive su un'interfaccia di rete elastica.

> **Note**
>
> Questa funzionalità è disponibile solo con le istanze. Nitro-based Dovresti testare le tue applicazioni su istanze di generazione Nitrov6 con il `350` secondo timeout predefinito di tracciamento della connessione ridotto prima di implementarle in produzione.

Esistono tre timeout configurabili:

- Timeout TCP stabilito: il timeout (in secondi) per le connessioni TCP inattive in uno stato stabilito.
  - Minimo: `60` secondi
  - Massimo: `432000` secondi
  - Predefinito: `350` secondi per i tipi di istanze Nitro v6 (esclusi P6e-GB200); `432000` secondi per tutti gli altri tipi di istanza (inclusi). P6e-GB200
  - Consigliato: meno di `432000` secondi.
- Timeout UDP: il timeout (in secondi) per i flussi UDP inattivi che hanno registrato traffico solo in un'unica direzione o una singola transazione richiesta-risposta.
  - Minimo: `30` secondi
  - Massimo: `60` secondi

  - Impostazione predefinita: 30 secondi
- Timeout del flusso UDP: il timeout (in secondi) per i flussi UDP inattivi classificati come flussi che hanno registrato più di una transazione richiesta-risposta.
  - Minimo: 60 secondi
  - Massimo: 180 secondi
  - Impostazione predefinita: 180 secondi

Potresti voler modificare i timeout predefiniti per uno dei seguenti casi:

- Se stai monitorando le connessioni tracciate utilizzando i parametri delle prestazioni di rete di Amazon EC2, i parametri conntrack_allowance_exceeded e conntrack_allowance_available consentono di monitorare i pacchetti persi e tenere traccia dell'utilizzo della connessione per gestire in modo proattivo la capacità delle istanze EC2 con azioni di aumento o riduzione per contribuire a soddisfare la domanda di connessioni di rete prima di perdere i pacchetti. Se osservi cali di conntrack_allowance_exceeded sulle tue istanze EC2, potresti trarre vantaggio dall'impostazione di un timeout stabilito dal TCP inferiore per tenere conto delle sessioni obsolete dovute a client o middle box di rete non corretti. TCP/UDP
- In genere, i sistemi di bilanciamento del carico o i firewall hanno un timeout di inattività stabilito dal protocollo TCP compreso tra 60 e 90 minuti. Se utilizzi carichi di lavoro che dovrebbero gestire un numero molto elevato di connessioni (superiore a 100.000) da dispositivi come i firewall di rete, si consiglia di configurare un timeout simile su un'interfaccia di rete EC2.
- Se stai eseguendo un carico di lavoro che utilizza una topologia di routing asimmetrica, ti consigliamo di configurare un timeout di inattività TCP Established di 60 secondi.
- Se esegui carichi di lavoro con un numero elevato di connessioni come DNS, SIP, SNMP, Syslog, Radius e altri servizi che utilizzano principalmente UDP per soddisfare le richieste, l'impostazione del timeout '' su 60s consente di aumentare la capacità esistente e di prevenire guasti indesiderati. UDP-stream scale/performance
- Per le TCP/UDP connessioni tramite Network Load Balancer, tutte le connessioni vengono tracciate. Il valore di timeout di inattività per i flussi TCP è di 350 secondi e per i flussi UDP è di 120 secondi e varia a seconda dei valori di timeout a livello di interfaccia. Potresti voler configurare i timeout a livello di interfaccia di rete per consentire una maggiore flessibilità di timeout rispetto ai valori predefiniti per il bilanciatore del carico.

È possibile configurare i timeout di tracciamento della connessione quando si eseguono le seguenti operazioni:

- Creazione di un'interfaccia di rete
- Modifica degli attributi dell'interfaccia di rete
- Avvio di un'istanza EC2
- Creazione di un modello di avvio di un'istanza EC2

Esempio

Nell'esempio seguente, il gruppo di sicurezza ha regole in entrata specifiche che autorizzano il traffico TCP e ICMP e regole in uscita che autorizzano tutto il traffico in uscita.

In entrata

Tipo di protocollo	Numero della porta	Origine
TCP	22 (SSH)	203.0.113. 1/32
TCP	80 (HTTP)	0.0.0. 0/0
TCP	80 (HTTP)	::/0
ICMP	Tutti	0.0.0. 0/0

In uscita

Tipo di protocollo	Numero della porta	Destinazione
Tutti	Tutti	0.0.0. 0/0
Tutti	Tutti	::/0

Con una connessione di rete diretta all'istanza o all'interfaccia di rete, il comportamento di monitoraggio è il seguente:

- Il traffico TCP in entrata e in uscita sulla porta 22 (SSH) viene tracciato, poiché la regola in entrata consente il traffico da 203.0.113. 1/32 solo e non tutti gli indirizzi IP (0.0.0. 0/0).

- Il traffico TCP in entrata e in uscita sulla porta 80 (HTTP) non viene monitorato, perché le regole in entrata e in uscita autorizzano il traffico da tutti gli indirizzi IP.
- Il traffico ICMP viene sempre monitorato.

Se viene rimossa la regola in uscita per il traffico IPv4, viene monitorato tutto il traffico IPv4 in entrata e in uscita, incluso il traffico sulla porta 80 (HTTP). Lo stesso vale per il traffico IPv6 se si rimuove la regola in uscita per il traffico IPv6.

Regole del gruppo di sicurezza per diversi casi d'uso

Puoi creare un gruppo di sicurezza e aggiungere regole che rispecchiano il ruolo dell'istanza associata al gruppo di sicurezza. Ad esempio, un'istanza configurata come un server Web richiede regole del gruppo di sicurezza che consentano l'accesso HTTP e HTTPS in entrata. Allo stesso modo, un'istanza di database richiede regole che consentano l'accesso per il tipo di database, ad esempio l'accesso sulla porta 3306 per MySQL.

Di seguito sono illustrati esempi dei tipi di regole che è possibile aggiungere ai gruppi di sicurezza per tipi di accesso specifici.

Esempi

- Regole del server Web
- Regole del server di database
- Regole per la connessione alle istanze dal computer in uso
- Regole per la connessione alle istanze da un'istanza con lo stesso gruppo di sicurezza
- Regole per ping/ICMP
- Regole del server DNS
- Regole Amazon EFS
- Regole Elastic Load Balancing

Per istruzioni, consulta Creare un gruppo di sicurezza e the section called "Configurazione delle regole per i gruppi di sicurezza".

Regole del server Web

Le seguenti regole in entrata permettono l'accesso HTTP e HTTPS da qualunque indirizzo IP. Se il tuo VPC può supportare IPv6, puoi aggiungere regole per controllare il traffico HTTP e HTTPS dagli indirizzi IPv6.

Tipo di protocollo	Numero di protocollo	Porta	IP di origine	Note
TCP	6	80 (HTTP)	0.0.0. 0/0	Permette l'accesso HTTP in entrata da qualunque indirizzo IPv4
TCP	6	443 (HTTPS)	0.0.0. 0/0	Permette l'accesso HTTPS in entrata da qualunque indirizzo IPv4
TCP	6	80 (HTTP)	::/0	Permette l'accesso HTTP in entrata da qualunque indirizzo IPv6.
TCP	6	443 (HTTPS)	::/0	Permette l'accesso HTTPS in entrata da qualunque indirizzo IPv6.

Regole del server di database

Le seguenti regole in entrata sono esempi di regole che è possibile aggiungere per l'accesso al database a seconda del tipo di database in esecuzione sull'istanza. Per ulteriori informazioni sulle istanze Amazon RDS, consulta la Guida per l'utente di Amazon RDS.

Per l'IP di origine, specifica uno dei seguenti valori:

- Un indirizzo IP specifico o un intervallo di indirizzi IP (in notazione di blocco CIDR) nella rete locale
- Un ID del gruppo di sicurezza per un gruppo di istanze che accedono al database

Tipo di protocollo	Numero di protocollo	Porta	Note
TCP	6	1433 (MS SQL)	La porta predefinita di accesso al database di Microsoft SQL Server, ad esempio su un'istanza Amazon RDS
TCP	6	306 () MYSQL/ Aurora	La porta predefinita di accesso a un database MySQL o Aurora, ad esempio su un'istanza Amazon RDS
TCP	6	5439 (Redshift)	La porta predefinita per accedere a un database di cluster Amazon Redshift.
TCP	6	5432 (PostgreSQL)	La porta predefinita di accesso a un database PostgreSQL, ad esempio su un'istanza Amazon RDS
TCP	6	1521 (Oracle)	La porta predefinita di accesso a un database Oracle, ad esempio su un'istanza Amazon RDS

Facoltativamente, è possibile limitare il traffico in uscita dai server di database. Ad esempio, è possibile autorizzare l'accesso a Internet per gli aggiornamenti software, ma limitare tutti gli altri tipi di traffico. Occorre prima rimuovere la regola in uscita predefinita che autorizza tutto il traffico in uscita.

Tipo di protocollo	Numero di protocollo	Porta	IP di destinazione	Note
TCP	6	80 (HTTP)	0.0.0. 0/0	Permette l'accesso HTTP in uscita verso qualunque indirizzo IPv4
TCP	6	443 (HTTPS)	0.0.0. 0/0	Permette l'accesso HTTPS in uscita verso qualunque indirizzo IPv4

Tipo di protocollo	Numero di protocollo	Porta	IP di destinazione	Note
TCP	6	80 (HTTP)	::/0	(solo IPv6-enabled VPC) Consente l'accesso HTTP in uscita a qualsiasi indirizzo IPv6
TCP	6	443 (HTTPS)	::/0	(solo IPv6-enabled VPC) Consente l'accesso HTTPS in uscita a qualsiasi indirizzo IPv6

Regole per la connessione alle istanze dal computer in uso

Per stabilire la connessione all'istanza, il tuo gruppo di sicurezza deve avere regole in entrata che consentono l'accesso SSH (per le istanze Linux) o l'accesso RDP (per le istanze Windows).

Tipo di protocollo	Numero di protocollo	Porta	IP di origine
TCP	6	22 (SSH)	L'indirizzo IPv4 pubblico del tuo computer o un intervallo di indirizzi IP nella rete locale. Se il VPC può supportare IPv6 e la tua istanza ha un indirizzo IPv6, puoi inserire un indirizzo o un intervallo IPv6.
TCP	6	3389 (RDP)	L'indirizzo IPv4 pubblico del tuo computer o un intervallo di indirizzi IP nella rete locale. Se il VPC può supportare IPv6 e la tua istanza ha un indirizzo IPv6, puoi inserire un indirizzo o un intervallo IPv6.

Regole per la connessione alle istanze da un'istanza con lo stesso gruppo di sicurezza

Per consentire alle istanze associate allo stesso gruppo di sicurezza di comunicare tra loro, devi aggiungere esplicitamente regole apposite.

> **Note**
>
> Se le route vengono configurate per inoltrare il traffico tra due istanze in sottoreti diverse attraverso un'appliance middlebox, è necessario assicurarsi che i gruppi di sicurezza per entrambe le istanze consentano il flusso del traffico tra le istanze. Il gruppo di sicurezza per ogni istanza deve fare riferimento all'indirizzo IP privato dell'altra istanza o all'intervallo CIDR della sottorete che contiene l'altra istanza come origine. Se si fa riferimento al gruppo di sicurezza dell'altra istanza come origine, allora il flusso del traffico tra le istanze non sarà consentito.

La tabella seguente descrive la regola in entrata per un gruppo di sicurezza che permette alle istanze associate di comunicare tra loro. La regola autorizza tutti i tipi di traffico.

Tipo di protocollo	Numero di protocollo	Porte	IP di origine
-1 (Tutti)	-1 (Tutti)	-1 (Tutti)	L'ID del gruppo di sicurezza o l'intervallo CIDR della sottorete che contiene l'altra istanza (vedi nota).

Regole per ping/ICMP

Il comando ping è un tipo di traffico ICMP. Per effettuare il ping dell'istanza, devi aggiungere una delle seguenti regole ICMP in entrata.

Tipo	Protocollo	Origine		
ICMP personalizzato - IPv4	Richiesta echo	L'indirizzo IPv4 pubblico del tuo computer, un indirizzo IPv4		

Tipo	Protocollo	Origine		
		specifico o un indirizzo IPv4 o IPv6 di qualsiasi provenienza.		
Tutti ICMP - IPv4	ICMP IPv4 (1)	L'indirizzo IPv4 pubblico del tuo computer, un indirizzo IPv4 specifico o un indirizzo IPv4 o IPv6 di qualsiasi provenienza.		

Per utilizzare il comando ping6 per eseguire il ping degli indirizzi IPv6 della tua istanza, devi aggiungere la seguente regola ICMPv6 in entrata.

Tipo	Protocollo	Origine		
Tutto ICMP - IPv6	ICMP IPv6 (58)	L'indirizzo IPv6 del tuo computer, un indirizzo IPv4 specifico o un indirizzo IPv4 o IPv6 di qualsiasi provenienza.		

Regole del server DNS

Se hai configurato un'istanza EC2 come server DNS, devi verificare che il traffico TCP e UDP possa raggiungere il server DNS tramite la porta 53.

Per l'IP di origine, specifica uno dei seguenti valori:

- Un indirizzo IP o un intervallo di indirizzi IP (in notazione di blocco CIDR) in una rete
- L'ID di un gruppo di sicurezza per il set di istanze nella rete che richiedono l'accesso al server DNS

Tipo di protocollo	Numero di protocollo	Porta
TCP	6	53
UDP	17	53

Regole Amazon EFS

Se utilizzi un file system Amazon EFS con le istanze Amazon EC2 il gruppo di sicurezza che associ ai target di montaggio Amazon EFS deve autorizzare il traffico sul protocollo NFS.

Tipo di protocollo	Numero di protocollo	Porte	IP di origine	Note
TCP	6	2049 (NFS)	L'ID del gruppo di sicurezza	Permette l'accesso NFS in entrata dalle risorse (compreso l'obiettivo di montaggio) associate a questo gruppo di sicurezza.

Per montare un file system Amazon EFS su un'istanza Amazon EC2, devi connetterti all'istanza. Di conseguenza, il gruppo di sicurezza associato all'istanza deve avere regole che autorizzano il traffico SSH in entrata dal computer locale o dalla rete locale.

Tipo di protocollo	Numero di protocollo	Porte	IP di origine	Note
TCP	6	22 (SSH)	L'intervallo di indirizzi IP del computer locale o l'intervallo di indirizzi IP	Permette l'accesso SSH in entrata dal tuo computer locale.

Tipo di protocollo	Numero di protocollo	Porte	IP di origine	Note
			(in notazione di blocco CIDR) per la rete.	

Regole Elastic Load Balancing

Se registri le istanze EC2 in un bilanciatore del carico, il gruppo di sicurezza a esso associato deve permettere la comunicazione con le istanze. Per ulteriori informazioni, consulta la documentazione per il bilanciatore del carico elastico qui di seguito.

- Gruppi di sicurezza per l'Application Load Balancer
- Gruppi di sicurezza per il Network Load Balancer
- Configurazione dei gruppi di sicurezza per Classic Load Balancer

NitroTPM per istanze Amazon EC2

Nitro Trusted Platform Module (NitroTPM) è un dispositivo virtuale fornito da AWS Nitro System e conforme alle specifiche TPM 2.0. Archivia in modo sicuro gli artefatti (come password, certificati o chiavi di crittografia) utilizzati per autenticare l'istanza. NitroTPM può generare chiavi e utilizzarle per funzioni crittografiche (come hashing, firma, crittografia e decrittografia).

NitroTPM fornisce l'avvio misurato, un processo in cui il bootloader e il sistema operativo creano hash crittografici di ogni binario di avvio e li combinano con i valori precedenti nei PCR (Platform Configuration Registers) interni di NitroTPM. Con l'avvio misurato, è possibile ottenere valori PCR firmati da NitroTPM e utilizzarli per dimostrare alle entità remote l'integrità del software di avvio dell'istanza. Questo è noto come attestazione remota.

Con NitroTPM, è possibile taggare chiavi e segreti con un valore PCR specifico in modo da renderli sempre inaccessibili se il valore del PCR, e quindi l'integrità dell'istanza, cambia. Questa speciale forma di accesso condizionale è indicata come sealing e annullamento del sealing. Le tecnologie dei sistemi operativi, ad esempio BitLocker, possono utilizzare NitroTPM per sigillare una chiave di decrittografia dell'unità in modo che l'unità possa essere decrittografata solo quando il sistema operativo è stato avviato correttamente ed è in uno stato noto di buono stato.

Per utilizzare NitroTPM, devi selezionare un'Amazon Machine Image (AMI) configurata per il supporto di NitroTPM, quindi utilizzare l'AMI per avviare le istanze. Nitro-based È possibile selezionare una delle AMI predefinite di Amazon o crearne una direttamente.

Prezzi

L'utilizzo di NitroTPM non prevede costi aggiuntivi. È previsto un pagamento solo per le risorse sottostanti utilizzate.

Indice

- Requisiti per l'utilizzo di NitroTPM con istanze Amazon EC2
- Abilitazione di un'AMI Linux per NitroTPM
- Verifica che un'AMI sia abilitata per NitroTPM
- Abilitazione o interruzione dell'utilizzo di NitroTPM su un'istanza Amazon EC2
- Verifica che un'istanza Amazon EC2 sia abilitata per NitroTPM
- Recuperare la chiave di approvazione pubblica per un'istanza EC2

Requisiti per l'utilizzo di NitroTPM con istanze Amazon EC2

Per avviare un'istanza con NitroTPM abilitato, devi soddisfare i seguenti requisiti.

Argomenti

- AMI
- Tipi di istanza
- Considerazioni

AMI

L'AMI deve avere NitroTPM abilitato.

AMI di Linux

Non esistono AMI preconfigurate. Devi configurare la tua AMI. Per ulteriori informazioni, consulta Abilitazione di un'AMI Linux per NitroTPM.

AMI di Windows

Per trovare un'AMI AWS Windows preconfigurata per NitroTPM e UEFI Secure Boot con le chiavi Microsoft, consulta Trova le AMI di Windows Server configurate con NitroTPM e UEFI Secure Boot nella Guida alle AMI di Windows. AWS

> **Note**
>
> Sistema operativo: l'AMI deve includere un sistema operativo con driver Command Response Buffer (CRB) TPM 2.0. La maggior parte dei sistemi operativi attuali include un driver CRB TPM 2.0.
> Modalità di avvio UEFI: l'AMI deve essere configurata per la modalità di avvio UEFI. Per ulteriori informazioni, consulta UEFI Secure Boot per istanze Amazon EC2.

Tipi di istanza

Devi utilizzare uno dei seguenti tipi di istanza virtualizzate:

- Uso generale: M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6a, M6g, M6gd, M6i, M6id, M6idn, M6in, M7a, M7g, M7gd, M7i, M8a, M8aZn, M8g, M8gb, M8gd, M8gN, M8i M7i-flex, M8id, M8in, M8idn, M8ine, M8iN, M8ib, M8idb, M9g, M9gd, T3, T3a, M8i-flex T4g
- Ottimizzato per il calcolo: C5, C5a, C5ad, C5d, C5n, C6a, C6g, C6gd, C6gn, C6gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i C7i-flex,, C8a, C8g, C8gb, C8gd, C8gn, C8gn, C8i, C8id C8i-flex, C8in, C8ine, C8ib, C9g, C9gd
- Memoria ottimizzata: R5, R5a, R5ad, R5b, R5d, R5dn, R5n, R6a, R6g, R6gd, R6i, R6id, R6idn, R6in, R7a, R7g, R7gd, R7i, R7iZ, R8a, R8g, R8gb, R8gb, R8z Gd, R8gn, R8i, R8id,, R8in, R8idn, R8ib, R8idb, R9g R8i-flex, R9gd,,,,,,,,,, X2idn, X2iedn, X2ieZn, X8g U7i-6tb U7i-8tb U7i-12tb U7in-16tb, X8aedz U7in-24tb U7in-32tb, X8i, z1d
- Ottimizzate per l'archiviazione: D3, D3en, I3en, I4i, I7i, I7ie, I8g, I8ge, Im4gn
- Calcolo accelerato: F2, G4dn, G5, G6, G6e, G6f, Gr6, Gr6f, G7, G7e, Inf1, Inf1, Inf2, P5, P5e, P5en P6-B200, P6-B300, P6e-GB200,, Trn2, Trn2u
- High-performance calcolo: HPC6a, HPC6id, HPC8a

Considerazioni

Le seguenti considerazioni si applicano quando si utilizza NitroTPM:

- Dopo aver avviato un'istanza utilizzando un'AMI con NitroTPM abilitato, se desideri modificare il tipo di istanza, anche il nuovo tipo di istanza che scegli deve supportare NitroTPM.
- BitLocker i volumi crittografati con NitroTPM-based chiavi possono essere utilizzati solo sull'istanza originale.
- Lo stato di NitroTPM non viene visualizzato nella console Amazon EC2.
- Lo stato di NitroTPM non è incluso negli snapshot Amazon EBS.
- Lo stato NitroTPM non è incluso nelle immagini Import/Export VM.
- NitroTPM non è supportato su AWS Outposts., Zone locali o Zone di lunghezza d'onda.

Abilitazione di un'AMI Linux per NitroTPM

Per abilitare NitroTPM per un'istanza, è necessario avviare l'istanza utilizzando un'AMI con NitroTPM abilitato. Devi configurare l'AMI Linux per il supporto di NitroTPM quando la registri. Non è possibile configurare il supporto di NitroTPM in un secondo momento.

Per l'elenco delle AMI di Windows preconfigurate per il supporto di NitroTPM, consulta Requisiti per l'utilizzo di NitroTPM con istanze Amazon EC2.

È necessario creare un'AMI con NitroTPM configurato utilizzando l'API. RegisterImage Non puoi usare la console o la macchina virtuale Amazon EC2. Import/Export

Per abilitare un'AMI Linux per NitroTPM

1. Avvia un'istanza temporanea con l'AMI Linux richiesta. Annota l'ID del relativo volume principale, che puoi trovare nella console nella scheda Archiviazione dell'istanza.
2. Dopo che l'istanza ha raggiunto lo stato `running`, crea uno snapshot del volume root dell'istanza. Per ulteriori informazioni, consulta Create a snapshot of an EBS volume.
3. Registra lo snapshot che hai creato come AMI. Nella mappatura dei dispositivi a blocchi, specifica lo snapshot che hai creato per il volume principale.

   Di seguito è riportato un esempio di comando register-image. Per `--tpm-support`, specificare `v2.0`. Per `--boot-mode`, specificare `uefi`.

```
aws ec2 register-image \
    --name my-image \
    --boot-mode uefi \
    --architecture x86_64 \
    --root-device-name /dev/xvda \
```

```
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0abcdef1234567890} \
    --tpm-support v2.0
```

Di seguito è riportato un esempio del Register-EC2Image cmdlet.

```
$block = @{SnapshotId=snap-0abcdef1234567890}
Register-EC2Image `
    -Name my-image `
    -Architecture "x86_64" `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block} `
    -BootMode Uefi `
    -TpmSupport V20
```

4. Interruzione dell'istanza temporanea avviata nel passaggio 1.

Verifica che un'AMI sia abilitata per NitroTPM

Per abilitare NitroTPM per un'istanza, è necessario avviare l'istanza utilizzando un'AMI con NitroTPM abilitato. Puoi descrivere un'immagine per verificare che sia abilitata per NitroTPM. Se sei il proprietario dell'AMI, puoi descrivere l'attributo dell'immagine `tpmSupport`.

La console Amazon EC2 non visualizza `TpmSupport`.

AWS CLI

Per verificare che NitroTPM sia abilitato

Utilizzare il comando describe-images .

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[*].TpmSupport
```

Se NitroTPM è abilitato per l'AMI, viene visualizzato il seguente output. Se TPM non è abilitato, l'output è vuoto.

```
[
    "v2.0"
]
```

In alternativa, se sei il proprietario dell'AMI, puoi utilizzare il comando describe-image-attribute con l'attributo `tpmSupport`.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute tpmSupport
```

Di seguito è riportato un output di esempio.

```
{
    "ImageId": "ami-0abcdef1234567890",
    "TpmSupport": {
        "Value": "v2.0"
    }
}
```

Per trovare le AMI con NitroTPM abilitato

Il seguente esempio elenca gli ID delle AMI che possiedi con NitroTPM abilitato.

```
aws ec2 describe-images \
    --owners self \
    --filters Name=tpm-support,Values=v2.0 \
    --query Images[].ImageId
```

PowerShell

Per verificare che NitroTPM sia abilitato

Utilizza il cmdlet Get-EC2Image.

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | Select TpmSupport
```

Se NitroTPM è abilitato per l'AMI, viene visualizzato il seguente output. Se TPM non è abilitato, l'output è vuoto.

```
TpmSupport
----------
v2.0
```

In alternativa, se sei il proprietario dell'AMI, puoi utilizzare il Get-EC2ImageAttribute cmdlet con l'attributo. `tpmSupport`

```
Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute tpmSupport
```

Per trovare le AMI con NitroTPM abilitato

Il seguente esempio elenca gli ID delle AMI che possiedi con NitroTPM abilitato.

```
Get-EC2Image `
    -Owner self `
    -Filter @{Name="tpm-support; Values="v2.0"} | Select ImageId
```

Abilitazione o interruzione dell'utilizzo di NitroTPM su un'istanza Amazon EC2

Puoi abilitare un'istanza Amazon EC2 per NitroTPM solo all'avvio. Dopo aver abilitato un'istanza per NitroTPM, non è possibile disabilitarla. Se non si devono più utilizzare NitroTPM, è necessario configurare il sistema operativo per interrompere l'utilizzo di NitroTPM.

Argomenti

- Avvio di un'istanza con NitroTPM abilitato
- Interruzione dell'utilizzo di NitroTPM su un'istanza

Avvio di un'istanza con NitroTPM abilitato

Quando viene avviata un'istanza con i prerequisiti, NitroTPM viene abilitato automaticamente sull'istanza. È possibile abilitare NitroTPM su un'istanza all'avvio. Per ulteriori informazioni sull'avvio di un'istanza MySQL, consulta Avviare un'istanza Amazon EC2.

Interruzione dell'utilizzo di NitroTPM su un'istanza

Dopo aver avviato un'istanza con NitroTPM abilitato, non è possibile disabilitare NitroTPM per l'istanza. Tuttavia, puoi configurare il sistema operativo affinché interrompa l'utilizzo di NitroTPM disabilitando il driver del dispositivo TPM 2.0 sull'istanza utilizzando i seguenti strumenti:

- Per le istanze Linux, utilizza tpm-tools.
- Per le istanze Windows, utilizza la console di gestione TPM (tpm.msc).

Per ulteriori informazioni sulla disabilitazione del driver del dispositivo, consulta la documentazione per il sistema operativo in uso.

Verifica che un'istanza Amazon EC2 sia abilitata per NitroTPM

Puoi verificare se un'istanza Amazon EC2 è abilitata per NitroTPM. Se il supporto NitroTPM è abilitato sull'istanza, il comando restituisce `"v2.0"`. Altrimenti, il campo `TpmSupport` non è presente nell'output.

La console Amazon EC2 non visualizza il campo `TpmSupport`.

AWS CLI

Per verificare se un'istanza è abilitata per NitroTPM

Utilizzare il comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].TpmSupport
```

PowerShell

Per verificare se un'istanza è abilitata per NitroTPM

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.TpmSupport
```

Verifica l'accesso a NitroTPM sulla tua istanza di Windows

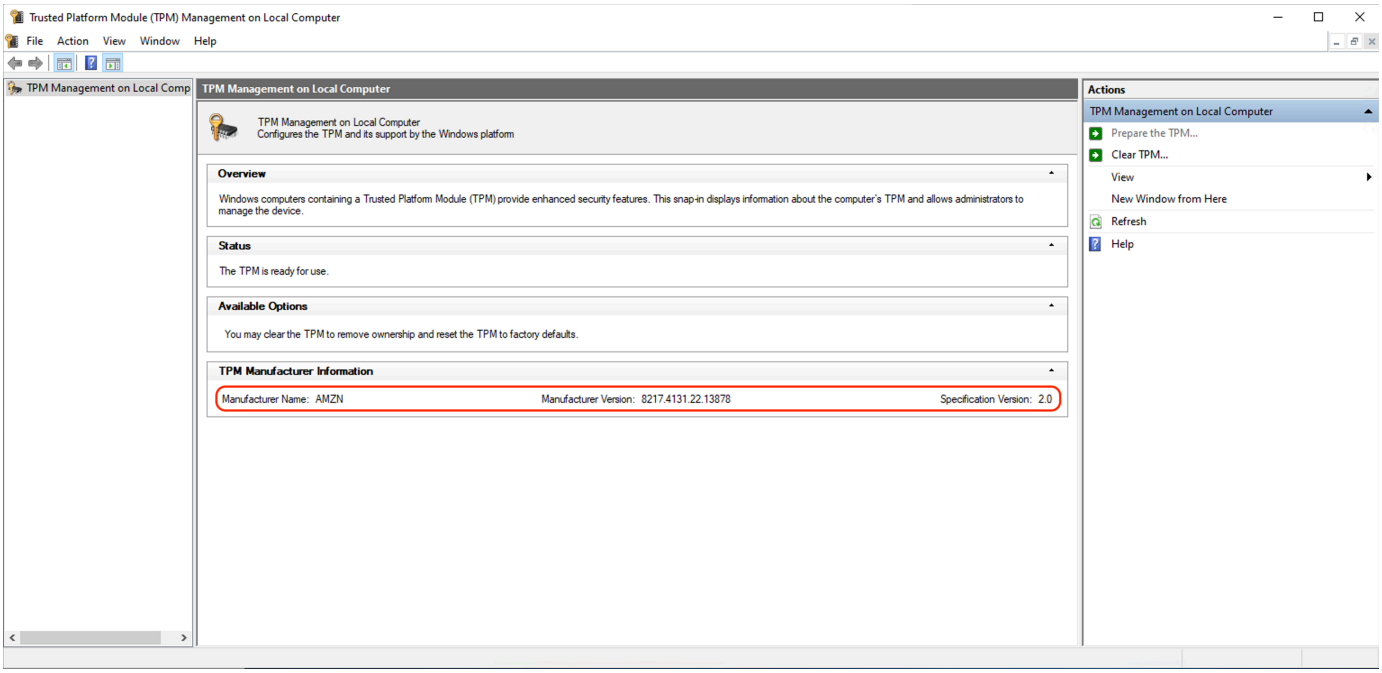
(Solo istanze Windows) Per verificare se NitroTPM è accessibile a Windows

1. Connettiti all'istanza EC2 Windows.

2. Nell'istanza, esegui il programma tpm.msc.

   Viene visualizzata la finestra TPM Management on Local Computer (Gestione TPM sul computer locale).

3. Seleziona il campo TPM Manufacturer Information (Informazioni sul produttore TPM). Contiene il nome del produttore e la versione di NitroTPM sull'istanza.



Recuperare la chiave di approvazione pubblica per un'istanza EC2

Puoi recuperare in modo sicuro la chiave di approvazione pubblica per un'istanza in qualsiasi momento.

AWS CLI

Come recuperare la chiave di approvazione pubblica per un'istanza

Utilizza il comando get-instance-tpm-ek-pub.

Esempio 1

L'esempio seguente ottiene la chiave di approvazione pubblica `rsa-2048`nel formato `tpmt` per l'istanza specificata.

```
aws ec2 get-instance-tpm-ek-pub \
```

```
    --instance-id i-1234567890abcdef0 \
    --key-format tpmt \
    --key-type rsa-2048
```

Di seguito è riportato l'output di esempio.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "tpmt",
    "KeyType": "rsa-2048",
    "KeyValue": "AAEACwADALIAIINxl2dEhLEXAMPLEUal1yT9UtduBlILZPKh2hszFGmqAAYAgABDA
    EXAMPLEAAABAOiRd7WmgtdGNoV1h/AxmW+CXExblG8pEUfNm0LOLiYnEXAMPLERqApiFa/UhvEYqN4
    Z7jKMD/usbhsQaAB1gKA5RmzuhSazHQkax7EXAMPLEzDthlS7HNGuYn5eG7qnJndRcakS+iNxT8Hvf
    0S1ZtNuItMs+Yp4SO6aU28MT/JZkOKsXIdMerY3GdWbNQz9AvYbMEXAMPLEPyHfzgVO0QTTJVGdDxh
    vxtXCOu9GYf0crbjEXAMPLEd4YTbWdDdgOKWF9fjzDytJSDhrLAOUctNzHPCd/92l5zEXAMPLEOIFA
    Ss50C0/802c17W2pMSVHvCCa9lYCiAfxH/vYKovAAE="
}
```

Esempio 2

L'esempio seguente ottiene la chiave di approvazione pubblica `rsa-2048`nel formato `der` per l'istanza specificata.

```
aws ec2 get-instance-tpm-ek-pub \
    --instance-id i-1234567890abcdef0 \
    --key-format der \
    --key-type rsa-2048
```

Di seguito è riportato l'output di esempio.

```
{
    "InstanceId": "i-1234567890abcdef0",
    "KeyFormat": "der",
    "KeyType": "rsa-2048",
    "KeyValue": "MIIBIjANBgEXAMPLEw0BAQEFAAOCAQ8AMIIBCgKCAQEA6JF3taEXAMPLEXWH8DGZb4
    JcTFuUbykRR82bQs4uJifaKSOv5NGoEXAMPLEG8Rio3hnuMowP+6xuGxBoAHWAoDlGbO6FJrMdEXAMP
    LEnYUHvMO2GVLsc0a5ifl4buqcmd1FxqRL6I3FPwe9/REXAMPLE0yz5inhI7ppTbwxP8lmQ4qxch0x6
    tjcZ1Zs1DP0EXAMPLERUYLQ/Id/OBU7RBNMlUZ0PGG/G1cI670Zh/RytuOdx9iEXAMPLEtZ0N2A4pYX
    1+PMPK0lIOGssA5Ry03Mc8J3/3aXnOD2/ASRQ4gUBKznQLT/zTZEXAMPLEJUe8IJr2VgKIB/Ef+9gqi
    8AAQIDAQAB"
}
```

PowerShell

Come recuperare la chiave di approvazione pubblica per un'istanza

Utilizza il cmdlet Get-EC2InstanceTpmEkPub.

Esempio 1

L'esempio seguente ottiene la chiave di approvazione pubblica `rsa-2048`nel formato `tpmt` per l'istanza specificata.

```
Get-EC2InstanceTpmEkPub `
    -InstanceId i-1234567890abcdef0 `
    -KeyFormat tpmt `
    -KeyType rsa-2048
```

Esempio 2

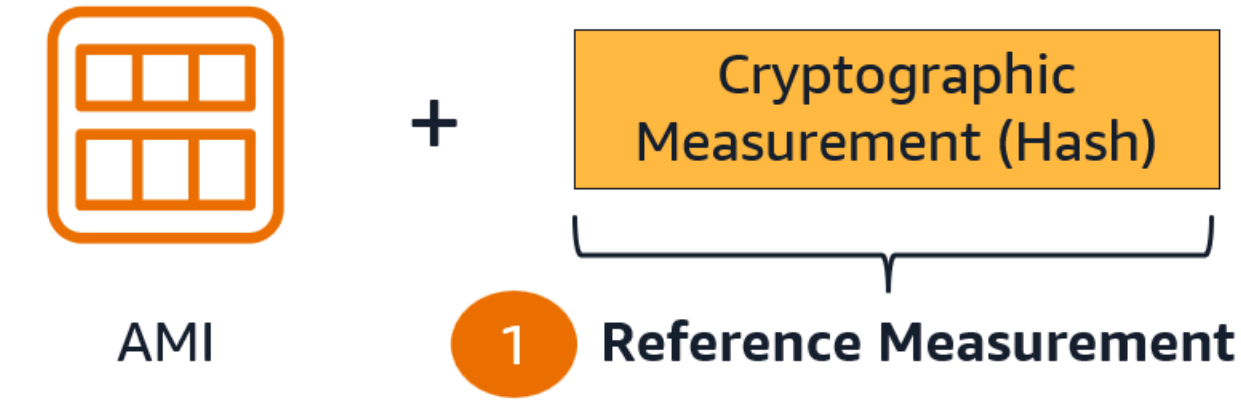
L'esempio seguente ottiene la chiave di approvazione pubblica `rsa-2048`nel formato `der` per l'istanza specificata.

```
Get-EC2InstanceTpmEkPub `
    -InstanceId i-1234567890abcdef0 `
    -KeyFormat der `
    -KeyType rsa-2048
```

Attestazione dell'istanza Amazon EC2

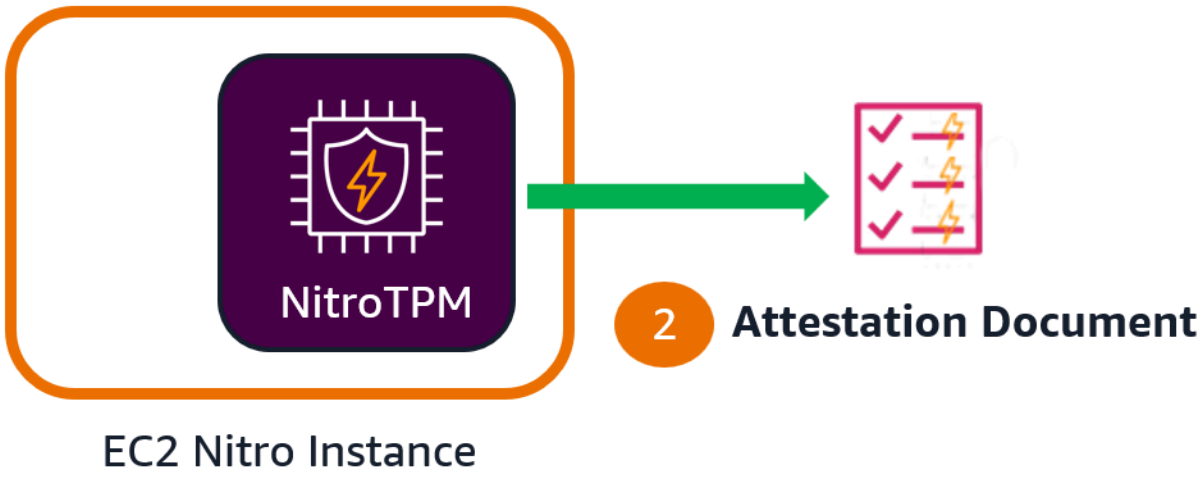
L'attestazione è un processo che permette di dimostrare crittograficamente a qualsiasi parte che su un'istanza Amazon EC2 sono in esecuzione solo software, driver e processi di avvio affidabili. L'attestazione dell'istanza Amazon EC2 è alimentata da Nitro Trusted Platform Module (NitroTPM) e dalle AMI attestabili.

Il primo passo per l'attestazione consiste nella creazione di un'AMI attestabile e nella determinazione delle misure di riferimento di tale AMI. Un'AMI attestabile è un'AMI creata da zero per l'attestazione. Le misurazioni di riferimento sono misurazioni di tutti i software e le configurazioni che hai incluso nella tua AMI. Per ulteriori informazioni su come ottenere le misurazioni di riferimento, consulta Crea la descrizione dell'immagine di esempio.



Il passaggio successivo consiste nell'avviare un'istanza EC2 Nitro-TPM abilitata con l'AMI Attestable. Dopo aver avviato l'istanza, puoi utilizzare gli strumenti NitroTPM per generare il documento di attestazione. Quindi puoi confrontare le misure effettive della tua istanza EC2 tratte dal Documento di attestazione con le misurazioni di riferimento per verificare se l'istanza dispone del software e delle configurazioni di cui ti fidi.

Confrontando le misurazioni di riferimento generate durante il processo di creazione dell'AMI attestabile con le misurazioni incluse nel documento di attestazione di un'istanza, puoi verificare che sull'istanza siano in esecuzione solo software e codice di cui ti fidi.



Integrazione con AWS KMS

Per semplificare il processo di confronto delle misurazioni, è possibile utilizzare AWS Key Management Service (AWS KMS) come verificatore per i documenti di attestazione. Con AWS KMS, è possibile creare politiche chiave KMS basate sull'attestazione che consentano operazioni specifiche con la chiave KMS solo se si fornisce un documento di attestazione con misurazioni che corrispondono alle misure di riferimento. A tale scopo, aggiungi chiavi di condizione specifiche alle policy della chiave KMS che utilizzano le misurazioni di riferimento come valori della chiave di condizione, quindi specifica quali operazioni KMS sono consentite se la chiave di condizione è soddisfatta.

Quando si eseguono operazioni KMS utilizzando la chiave KMS, è necessario allegare un documento di attestazione alla richiesta KMS. AWS KMS quindi convalida le misurazioni del documento di attestazione rispetto alle misure di riferimento nella politica chiave KMS e consente l'accesso con la chiave solo se le misurazioni corrispondono.

Inoltre, quando generi il documento di attestazione per un'istanza, è necessario specificare una chiave pubblica per una coppia di chiavi che ti appartengono. La chiave pubblica specificata è compresa nel documento di attestazione. Quando AWS KMS convalida il documento di attestazione e consente un'operazione di decrittografia, crittografa automaticamente la risposta con la chiave pubblica inclusa nel documento di attestazione prima che venga restituita. Ciò garantisce che la risposta possa essere decrittografata e utilizzata solo con la chiave privata corrispondente per la chiave pubblica compresa nel documento di attestazione.

Questo garantisce che solo le istanze che eseguono software e codici affidabili possano eseguire operazioni di crittografia utilizzando una chiave KMS.

Attestazione di ambienti di elaborazione isolati

In generale, puoi creare e configurare un'istanza EC2 in modo che diventi un ambiente di calcolo isolato, che non fornisce alcun accesso interattivo né alcun meccanismo che consenta agli amministratori e agli utenti di accedere ai dati elaborati nell'istanza EC2. Con l'attestazione dell'istanza EC2 puoi dimostrare a terzi o a un servizio che la tua istanza funziona come un ambiente di calcolo isolato. Per ulteriori informazioni, consulta Isola i dati dai tuoi operatori.

Per un esempio, consulta la descrizione dell'immagine di esempio di Amazon Linux 2023, che crea un ambiente di calcolo isolato. Puoi utilizzare questa descrizione dell'immagine di esempio come punto di partenza e personalizzarla per soddisfare le tue esigenze.

AWS Modello di responsabilità condivisa

Le AMI attestabile e NitroTPM sono elementi costitutivi che possono aiutarti a configurare e impostare l'attestazione sulle tue istanze EC2. L'utente è responsabile della configurazione dell'AMI per soddisfare il proprio caso d'uso. Per ulteriori informazioni, consulta AWS Shared Responsibility Model.

Argomenti

- AMI attestabili
- Preparazione AWS KMS per l'attestazione
- Ottieni il documento di attestazione NitroTPM
- Integrazione con AWS KMS
- Isola i dati dai tuoi operatori

AMI attestabili

Un'AMI attestabile è un'Amazon Machine Image (AMI) con un hash crittografico corrispondente che ne rappresenta tutto il contenuto. L'hash viene generato durante il processo di creazione dell'AMI e viene calcolato in base all'intero contenuto dell'AMI, incluse le applicazioni, il codice e il processo di avvio.

Mantenere uno stato attestabile

Le misurazioni di un'istanza si basano sul suo stato di avvio iniziale. Qualsiasi modifica al software o al codice apportata all'istanza dopo l'avvio e che persiste dopo il riavvio modificherà la misurazione dell'istanza dopo il riavvio. Se le misurazioni vengono alterate, si discostano dalle misurazioni di riferimento dell'AMI attestabile e l'istanza non sarà più in grado di AWS KMS attestarla con successo dopo il riavvio dell'istanza. Pertanto, affinché le AMI attestabile siano utili, le istanze devono tornare allo stato di avvio originale dopo il riavvio.

Il ritorno costante allo stato di avvio originale garantisce che un'istanza possa attestarsi correttamente dopo il riavvio. Le seguenti utilità possono essere utilizzate per assicurare che le istanze rimangano attestabili dopo il riavvio:

- `erofs`— Read-Only File system avanzato. Questa utilità garantisce che il filesystem root sia di sola lettura. Con questa utilità, le scritture sul filesystem, tra cui, e `/etc`, `/run` e `/var`, vengono

archiviate in memoria e perse al riavvio dell'istanza, lasciando il filesystem root nello stato di avvio originale. Per ulteriori informazioni, consulta la documentazione erofs.

- `dm-verity`: fornisce protezione dell'integrità per il filesystem root di sola lettura. L'utilità calcola un hash dei blocchi del filesystem e lo memorizza nella riga di comando del kernel. Ciò permette al kernel di verificare l'integrità del filesystem durante l'avvio. Per ulteriori informazioni, consulta la documentazione dm-verity.

Requisiti per la creazione di AMI attestabili

Le AMI attestabili hanno i seguenti requisiti:

- Sistema operativo di base: Amazon Linux 2023 e NixOS
- Architettura – architettura `x86_64` o `arm64`
- Supporto TPM: NitroTPM deve essere abilitato. Per ulteriori informazioni, consulta Requisiti per l'utilizzo di NitroTPM con istanze Amazon EC2.
- Modalità di avvio: la modalità di avvio UEFI deve essere abilitata.

Argomenti

- Creazione di AMI attestabili
- Crea la descrizione dell'immagine di esempio di Amazon Linux 2023
- Descrizione dell'immagine di esempio di Amazon Linux 2023
- Personalizza la descrizione delle immagini di esempio di Amazon Linux 2023 per il tuo carico di lavoro
- Calcola le misurazioni PCR per un'AMI personalizzata

Creazione di AMI attestabili

Per creare un'AMI attestabile, dovrai utilizzare Amazon Linux 2023 con KIWI Next Generation (KIWI NG). Amazon Linux 2023 fornisce tutto il software e le utilità necessari per creare un'AMI attestabile utilizzando KIWI NG.

KIWI NG è uno strumento open source per la creazione di immagini preconfigurate Linux-based . KIWI NG utilizza descrizioni di immagini XML che definiscono il contenuto di un'immagine. La descrizione dell'immagine specifica il sistema operativo di base, il software, la configurazione del kernel e gli script da eseguire per creare un'AMI pronta all'uso per un caso d'uso specifico.

Durante la fase di compilazione dell'AMI, devi utilizzare l'utilità `nitro-tpm-pcr-compute`per generare le misurazioni di riferimento basate sull'Unified Kernel Image (UKI) generata da KIWI NG. Per ulteriori informazioni sull'uso dell'utilità `nitro-tpm-pcr-compute`, consulta Calcola le misurazioni PCR per un'AMI personalizzata.

AWS fornisce un esempio di descrizione dell'immagine di Amazon Linux 2023 che include tutte le configurazioni necessarie per configurare un'istanza EC2 in un ambiente di calcolo isolato. Per ulteriori informazioni, consulta Crea la descrizione dell'immagine di esempio di Amazon Linux 2023.

Crea la descrizione dell'immagine di esempio di Amazon Linux 2023

AWS fornisce un esempio di descrizione dell'immagine di Amazon Linux 2023 che puoi utilizzare come punto di partenza per creare le tue AMI Attestable personalizzate per i tuoi carichi di lavoro. La descrizione dell'immagine di esempio include Amazon Linux 2023 come sistema operativo di base, configurazioni `dm-verity` ed `erofs` per l'immutabilità del file system e rimuove tutti gli accessi interattivi (come SSH, connessione all'istanza EC2 e console seriale) per creare un ambiente di calcolo isolato. Per ulteriori informazioni sulla descrizione dell'immagine di esempio, consulta il repository Github.

La descrizione dell'immagine di esempio installa automaticamente gli strumenti NitroTPM (`nitro-tpm-pcr-compute` e `nitro-tpm-attest`) nell'immagine creata nella directory `/usr/bin/`. Questo garantisce che gli strumenti siano preinstallati sulle istanze avviate dall'AMI.

La descrizione dell'immagine di esempio comprende uno script, `edit_boot_install.sh`, che include i comandi necessari per generare le misurazioni di riferimento. Lo script monta il file immagine disco raw (`.raw`) creato da KIWI NG su un dispositivo loopback, individua l'UKI, che ha l'estensione `.efi`, quindi esegue l'utilità `nitro-tpm-pcr-compute` per generare le misurazioni di riferimento per l'AMI. Lo script viene automaticamente eseguito da KIWI NG durante la compilazione.

Questo tutorial mostra come creare la descrizione dell'immagine di esempio per generare un'AMI attestabile.

Per ulteriori informazioni sulla creazione di descrizioni delle immagini, consulta la seguente documentazione di KIWI NG:

- Quick Start
- Descrizione delle immagini
- Descrizione dell'immagine di esempio di Amazon Linux 2023

Prerequisiti

La tua identità IAM deve avere le seguenti autorizzazioni per completare questo tutorial:

- `ebs:CompleteSnapshotebs:StartSnapshot`, e così via `ebs:PutSnapshotBlock arn:aws:ec2:*::snapshot/*`
- `ec2:RegisterImage`su tutte le risorse

Per creare la descrizione dell'immagine di esempio di Amazon Linux 2023 utilizzando KIWI NG

1. Avvia un'istanza Amazon EC2 utilizzando l'ultima AMI AL2023. Per assicurarti che l'istanza disponga di spazio di archiviazione sufficiente per creare l'AMI, verifica di fornire almeno 12 GB di spazio di archiviazione.
2. Installare le dipendenze richieste. Il seguente comando installa le seguenti utilità:
   - `kiwi-cli`
   - `veritysetup`
   - `erofs-utils`
   - `aws-nitro-tpm-tools`

   ```
   sudo dnf install -y kiwi-cli python3-kiwi kiwi-systemdeps-core python3-poetry-core
    qemu-img veritysetup erofs-utils git cargo aws-nitro-tpm-tools
   ```
3. Installa l'utilità `coldsnap`. Questa utilità consente di creare snapshot di Amazon EBS da dati di immagini non elaborati. Userai questa utilità per creare uno snapshot EBS dal file di immagine del disco non elaborato creato da KIWI NG.

   ```
   git clone https://github.com/awslabs/coldsnap.git
   cd coldsnap
   cargo install --locked coldsnap
   cd ..
   ```
4. Ottieni i file di descrizione dell'immagine di esempio.

   ```
   sudo dnf install kiwi-image-descriptions-examples
   ```

I file di descrizione dell'immagine di esempio vengono scaricati nella seguente directory: `/usr/share/kiwi-image-descriptions-examples/al2023/attestable-image-example`

5. Crea la descrizione dell'immagine di esempio utilizzando il comando `system build` KIWI NG. Il seguente comando crea un file di immagine non elaborato del disco nella directory `./image`.

```
sudo kiwi-ng \
--color-output \
--loglevel 0 \
system build \
--description /usr/share/kiwi-image-descriptions-examples/al2023/attestable-image-example \
--target-dir ./image
```

Per ulteriori informazioni, consulta la documentazione relativa alla compilazione del sistema kiwi-ng.

6. Ottieni le misure di riferimento per l'AMI. Le misurazioni vengono generate dall'utilità `nitro-tpm-pcr-compute`durante la creazione dell'immagine nel passaggio precedente. Puoi individuare le misurazioni di riferimento nel seguente file: `./image/pcr_measurements.json`.

Le misurazioni sono fornite nel seguente formato JSON:

```
{
  "Measurements": {
    "HashAlgorithm": "SHA384 { ... }",
    "PCR4": "PCR4_measurement",
    "PCR7": "PCR7_measurement",
    "PCR12": "PCR12_measurement"
  }
}
```

7. Utilizza l'utilità `coldsnap` per caricare l'immagine grezza del disco creata da KIWI NG su uno snapshot EBS. Questo comando restituisce l'ID dello snapshot. Prendi nota dell'ID, ti servirà per il passaggio successivo.

```
SNAPSHOT=$(.cargo/bin/coldsnap upload ./image/al2023*.raw)
echo "Created snapshot: $SNAPSHOT"
```

Per ulteriori informazioni sull'`coldsnap`utilità, consultate il repository coldsnap GitHub .

8. Registra un'AMI abilitata per TPM 2.0 con la modalità di avvio UEFI utilizzando lo snapshot del passaggio precedente. Per `--architecture`, specifica `x86_64` per Intel o `arm64` per Graviton.

```
aws ec2 register-image \
--name "attestable_isolated_al2023_ami" \
--virtualization-type hvm \
--boot-mode uefi \
--architecture x86_64|arm64 \
--root-device-name /dev/xvda \
--block-device-mappings DeviceName=/dev/xvda,Ebs={SnapshotId=${SNAPSHOT}} \
--tpm-support v2.0 \
--ena-support
```

Descrizione dell'immagine di esempio di Amazon Linux 2023

La descrizione dell'immagine di esempio di Amazon Linux 2023 presenta le seguenti caratteristiche:

1. Avvio con Unified Kernel Image (UKI): avvio utilizzando un unico file binario firmato che combina il kernel `initrd` e i parametri di avvio in un'unica immagine immutabile.
2. Read-only file system root: utilizzate Enhanced Read-Only File System (`erofs`) con protezione dm-verity per garantire che il filesystem root non possa essere modificato e mantenga la verifica dell'integrità crittografica.
3. Filesystem overlay temporaneo: crea un filesystem overlay temporaneo che consenta scritture temporanee su directory come `/etc`, `/run` e `/var`. Dato che questo filesystem overlay esiste solo in memoria, tutte le modifiche vengono automaticamente perse al riavvio dell'istanza, garantendo che il sistema torni allo stato attendibile originale.
4. Metodi di accesso remoto disabilitati: rimuovi i meccanismi di accesso remoto seguenti per impedire l'accesso remoto:

Metodo di accesso	Description	Implement azione della descrizione dell'immagine
SSH	Esclude il server OpenSSH. Rende l'istanza intrinsec amente incapace di gestire il traffico SSH.	Ignora il pacchetto

Metodo di accesso	Description	Implement azione della descrizione dell'immagine
		`openssh-server *`
User Data (Dati utente)	Rimuove. Cloud-init Elimina la possibilità per gli operatori di fornire dati utente alle istanze e di eseguire script all'avvio.	Ignora i pacchetti `cloud-init e cloud-init-cfg-ec2 *`
Chrony	Disabilita la porta di comando chrony. Impedisce agli operatori di eseguire comandi chrony sulle istanze in esecuzione.	Ignora il pacchetto `amazon-chrony-config *`
MOTD	Rimuove il pacchetto MOTD. Elimina la possibilità per gli operatori di modificare messaggi o funzionalità sulle istanze in esecuzione.	Ignora il pacchetto `update-motd *`
AWS SSM	Rimuove l'agente AWS SSM. Impedisce l'accesso remoto alle istanze in esecuzione tramite AWS SSM.	Ignora il pacchetto `amazon-ssm-agent *`
EC2 Instance Connect	Rimuove il pacchetto EC2 Instance Connect. Disattiva l'accesso SSH utilizzando questo strumento.	Ignora il pacchetto `ec2-instance-connect *`

Metodo di accesso	Description	Implement azione della descrizione dell'immagine
Console seriale	Disattiva la console seriale. Garantisce che l'accesso alla console non sia disponibile per le istanze in esecuzione e rimuove la possibilità per operatori di accedere alla console seriale.	Disabilitato tramite il parametro della riga di comando del kernel

* Per ulteriori informazioni, consulta Image Description Elements.

Personalizza la descrizione delle immagini di esempio di Amazon Linux 2023 per il tuo carico di lavoro

Puoi personalizzare la descrizione dell'immagine di esempio di Amazon Linux 2023 e includere pacchetti software, script e i file necessari per il tuo carico di lavoro specifico. Le personalizzazioni si ottengono aggiungendo o modificando vari elementi nella descrizione delle immagini KIWI NG.

Argomenti

- Gestione del repository
- Gestione dei pacchetti
- Aggiungi file e directory
- Aggiunta di script personalizzati

Gestione del repository

Per impostazione predefinita, la descrizione dell'immagine di esempio include un singolo elemento `<repository>` che punta a un endpoint mirror per i repository principali di Amazon Linux 2023. Se necessario, puoi aggiungere riferimenti ad altri repository da cui installare il software richiesto.

La descrizione dell'immagine di esempio utilizza il gestore di pacchetti `dnf`, come definito nell'elemento `<packagemanager>`.

Per ulteriori informazioni sull'aggiunta di repository, consulta Configurazione dei repository.

Gestione dei pacchetti

Per impostazione predefinita, la descrizione dell'immagine di esempio comprende tutti i pacchetti necessari per creare un'AMI attestabile di Amazon Linux 2023 per un ambiente di calcolo isolato con un file system `erofs` di sola lettura.

Puoi includere pacchetti software aggiuntivi nella descrizione dell'immagine aggiungendoli all'elemento `<packages>` nella descrizione dell'immagine. L'elemento `<packages>` definisce tutto il software che deve essere installato nell'AMI.

Puoi anche utilizzare l'elemento `<packages>` per disinstallare o eliminare pacchetti software specifici.

Per ulteriori informazioni sull'aggiunta o la rimozione di pacchetti nella descrizione dell'immagine, consulta Adding and Removing Packages.

Aggiungi file e directory

La descrizione dell'immagine di esempio include una directory ad albero sovrapposta (`/root/`). La directory ad albero sovrapposta è una directory che contiene file e directory che verranno copiati nell'immagine durante il processo di creazione dell'immagine. Tutti i file e le directory inseriti nella directory ad albero di overlay verranno copiati direttamente nel filesystem root dell'immagine durante il processo di creazione dell'immagine.

La directory ad albero sovrapposta viene copiata nell'immagine dopo che tutti i pacchetti sono stati installati. Vengono aggiunti nuovi file e vengono sovrascritti i file esistenti.

Aggiunta di script personalizzati

La descrizione dell'immagine di esempio comprende un singolo script personalizzato, `edit_boot_install.sh`. Questo script include i comandi necessari per eseguire l'utilità `nitro-tpm-pcr-compute`, che genera le misurazioni di riferimento in base al contenuto dell'immagine. Questo script viene chiamato subito dopo l'installazione del bootloader.

Se necessario, puoi includere script personalizzati nella descrizione dell'immagine per eseguire operazioni o configurazioni durante il processo di creazione dell'immagine o al primo avvio dell'immagine. L'uso degli script consente di personalizzare le immagini in modi che non possono essere ottenuti utilizzando la sola descrizione dell'immagine.

Per includere script personalizzati nella descrizione dell'immagine, devi denominarli correttamente in base al tipo di script e aggiungerli alla stessa directory del file `appliance.kiwi`. KIWI NG rileva ed esegue automaticamente gli script se sono denominati correttamente e collocati nella

posizione corretta, senza che sia necessario farvi riferimento esplicitamente nel file di descrizione dell'immagine.

Per maggiori informazioni sugli script supportati da KIWI NG, vedi Scripts. User-Defined

Calcola le misurazioni PCR per un'AMI personalizzata

L'utilità `nitro-tpm-pcr-compute` consente di generare le misurazioni di riferimento per un'AMI attestabile durante la fase di compilazione in base alla relativa Unified Kernel Image (UKI).

La descrizione dell'immagine di esempio di Amazon Linux 2023 installa automaticamente l'utilità nell'immagine incorporata nella directory `/usr/bin/`. La descrizione dell'immagine di esempio comprende anche uno script con i comandi necessari per eseguire l'utilità e generare le misurazioni di riferimento durante la creazione dell'immagine. Se stai utilizzando la descrizione dell'immagine di esempio, non è necessario installare l'utilità o eseguirla manualmente. Per ulteriori informazioni, consulta Crea la descrizione dell'immagine di esempio di Amazon Linux 2023.

Installa l'utilità nitro-tpm-pcr-compute

Se usi Amazon Linux 2023, puoi installare l'utilità `nitro-tpm-pcr-compute` dal repository Amazon Linux come segue.

```
sudo yum install aws-nitro-tpm-tools
```

Gli strumenti vengono installati nella directory `/usr/bin`.

Usa l'utilità nitro-tpm-pcr-compute

L'utilità fornisce un solo comando, `nitro-tpm-pcr-compute`, per generare le misurazioni di riferimento.

Quando esegui il comando, devi specificare quanto segue:

- Unified kernel image (`UKI.efi`): richiesta per l'avvio standard e UEFI.

Per generare le misurazioni di riferimento per un'AMI attestabile:

Utilizza il comando e i parametri seguenti:

```
/usr/bin/nitro-tpm-pcr-compute \
--image UKI.efi
```

L'utilità restituisce le misure di riferimento nel seguente formato JSON:

```
{
  "Measurements": {
    "HashAlgorithm": "SHA384 { ... }",
    "PCR4": "PCR4_measurement",
    "PCR7": "PCR7_measurement",
    "PCR12": "PCR12_measurement"
  }
}
```

Per un esempio pratico di uso dell'utilità `nitro-tpm-pcr-compute`, consulta lo script `edit_boot_install.sh` incluso nella descrizione dell'immagine di esempio di Amazon Linux 2023.

Preparazione AWS KMS per l'attestazione

> **Note**
>
> Se stai attestando un servizio di terze parti, devi creare i tuoi meccanismi personalizzati per ricevere, analizzare e convalidare i documenti di attestazione. Per ulteriori informazioni, consulta Convalida un documento di attestazione NitroTPM.

Dopo aver creato l'AMI Attestable, dovresti disporre di misure di riferimento da utilizzare per convalidare le richieste provenienti da un'istanza Amazon EC2. AWS KMS fornisce supporto integrato per l'attestazione con NitroTPM.

Per la AWS KMS chiave che hai usato per crittografare i tuoi dati segreti, aggiungi una policy chiave che consenta l'accesso alla chiave solo se le richieste API includono un documento di attestazione con misure che corrispondono alle misure di riferimento generate durante il processo di creazione dell'Attestable AMI. Utilizza le misurazioni PCR4 e PCR12 per l'avvio standard o le misurazioni PCR7 per l'avvio sicuro. Ciò garantisce che solo le richieste provenienti da istanze avviate utilizzando l'AMI Attestable possano eseguire operazioni crittografiche utilizzando la chiave. AWS KMS

AWS KMS fornisce `kms:RecipientAttestation:NitroTPMPCR4` `kms:RecipientAttestation:NitroTPMPCR7`, e chiavi di `kms:RecipientAttestation:NitroTPMPCR12` condizione che consentono di creare condizioni basate sull'attestazione per le policy chiave NitroTPM KMS. Per ulteriori informazioni, consulta Condition keys for NitroTPM.

Ad esempio, la seguente politica AWS KMS chiave consente l'accesso con chiave solo se la richiesta proviene da un'istanza con il profilo dell'istanza allegato e se la `MyEC2InstanceRole` richiesta include un documento di attestazione con valori specifici PCR 4 e PCR 12.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow requests from instances with attested AMI only",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyEC2InstanceRole"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateRandom"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {

 "kms:RecipientAttestation:NitroTPMPCR4":"EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde4

 "kms:RecipientAttestation:NitroTPMPCR12":"000000000000000000000000000000000000000000000000000000
        }
      }
    }
  ]
}
```

Ottieni il documento di attestazione NitroTPM

Il documento di attestazione è un componente chiave del processo di attestazione NitroTPM. Contiene una serie di misurazioni crittografiche che possono essere utilizzate per verificare l'identità dell'istanza e per dimostrare che sta eseguendo solo software affidabile. È possibile utilizzare l'Attestation Document with AWS KMS, che fornisce il supporto integrato per l'attestazione NitroTPM, o per creare meccanismi di attestazione crittografici personalizzati.

L'utilità `nitro-tpm-attest` consente di recuperare un documento di attestazione NitroTPM firmato per un'istanza Amazon EC2 durante il runtime.

La descrizione dell'immagine di esempio di Amazon Linux 2023 installa automaticamente l'utilità nell'immagine incorporata nella directory `/usr/bin/`. Questo garantisce che l'utilità sia preinstallata sulle istanze avviate utilizzando l'AMI. Non è necessario installare l'utilità manualmente. Per ulteriori informazioni, consulta Crea la descrizione dell'immagine di esempio di Amazon Linux 2023.

Argomenti

- Installa l'utilità nitro-tpm-attest
- Usa l'utilità nitro-tpm-attest
- Contenuto del documento di attestazione Nitro-PM
- Convalida un documento di attestazione NitroTPM

Installa l'utilità nitro-tpm-attest

Se usi Amazon Linux 2023, puoi installare l'utilità `nitro-tpm-attest` dal repository Amazon Linux come segue.

```
sudo yum install aws-nitro-tpm-tools
```

Usa l'**`utilità nitro-tpm-attest`**

L'utilità fornisce un solo comando, `nitro-tpm-attest`, per recuperare il documento di attestazione. Il comando restituisce il documento di attestazione codificato in Concise Binary Object Representation (CBOR) e firmato utilizzando CBOR Object Signing and Encryption (COSE).

Quando esegui il comando, puoi specificare i seguenti parametri facoltativi:

- `public-key`— Una chiave pubblica che può essere utilizzata da AWS KMS o da un servizio esterno per crittografare i dati di risposta prima che vengano restituiti. Questo garantisce che solo il destinatario previsto, in possesso della chiave privata, possa decrittografare i dati. Ad esempio, se si attesta con AWS KMS, il servizio crittografa i dati in chiaro con la chiave pubblica contenuta nel documento di attestazione e restituisce il testo cifrato risultante nel campo della risposta. `CiphertextForRecipient` Sono supportate solo le chiavi RSA.
- `user-data`: i dati utente possono essere utilizzati per fornire eventuali dati firmati aggiuntivi a un servizio esterno. Questi dati utente possono essere utilizzati per completare un protocollo concordato tra l'istanza richiedente e il servizio esterno. AWS KMS Non utilizzato per l'attestazione con.

- `nonce`: il nonce può essere utilizzato per configurare l'autenticazione challenge-response tra l'istanza e il servizio esterno per aiutare a prevenire attacchi di impersonificazione. L'uso di un nonce consente al servizio esterno di verificare che stia interagendo con un'istanza live e non con un imitatore che riutilizza un vecchio documento di attestazione. Non utilizzato per l'attestazione con. AWS KMS

Per recuperare il documento di attestazione

Utilizza il comando e i seguenti parametri facoltativi:

```
/usr/bin/nitro-tpm-attest \
--public-key rsa_public_key \
--user-data user_data \
--nonce nonce
```

Per un esempio completo che mostra come generare una coppia di chiavi RSA e come richiedere un'attestazione con la chiave pubblica, consultate il repository nitro-tpm-attest. GitHub

Contenuto del documento di attestazione Nitro-PM

Un documento di attestazione viene generato dal NitroTPM ed è firmato dall'hypervisor Nitro. Comprende una serie di valori dei registri di configurazione della piattaforma (PCR) relativi a un'istanza Amazon EC2. Le seguenti PCR sono comprese nel documento di attestazione:

> **Important**
>
> PCR0 e PCR1 vengono generalmente utilizzati per misurare il codice di avvio iniziale, controllato da AWS. Per consentire aggiornamenti sicuri del codice di avvio iniziale, questi PCR conterranno sempre valori costanti.

- `PCR0`: codice eseguibile del firmware del sistema principale
- `PCR1`: dati del firmware del sistema principale
- `PCR2`: codice eseguibile esteso o collegabile
- `PCR3`: dati firmware estesi o collegabili
- `PCR4`: codice di Boot Manager
- `PCR5`: configurazione del codice di Boot Manager e tabella dei dati e delle partizioni GPT

- PCR6: specifiche del produttore della piattaforma host
- PCR7: policy di avvio sicuro
- PCR8 – 15: definito per l'uso da parte del sistema operativo statico
- PCR16: debug
- PCR23: supporto per le applicazioni

PCR4, PCR7 e PCR12 vengono utilizzati specificamente per convalidare che un'istanza è stata avviata utilizzando un'AMI Attestable. PCR4 e PCR12 possono essere utilizzati per la convalida con l'avvio standard e PCR7 può essere utilizzato per la convalida con Secure Boot.

- PCR4 (Boot Manager Code): all'avvio di un'istanza, NitroTPM crea hash crittografici di tutti i file binari eseguiti dal suo ambiente UEFI. Con le AMI attestabili, questi file binari di avvio incorporano hash che impediscono il caricamento futuro di file binari che non hanno hash corrispondenti. In questo modo, l'hash binario ad avvio singolo può descrivere esattamente quale codice verrà eseguito da un'istanza.
- PCR7 (Secure Boot Policy): i file binari di avvio UEFI possono essere firmati con una chiave di firma UEFI Secure Boot. Quando UEFI Secure Boot è abilitato, UEFI impedirà l'esecuzione di file binari di avvio UEFI che non corrispondono alla policy configurata. PCR7 contiene un hash della policy UEFI Secure Boot dell'istanza.

  Se devi mantenere un'unica policy KMS che persista tra gli aggiornamenti delle istanze, puoi creare una policy che convalidi rispetto a PCR7 per convalidare un certificato UEFI Secure Boot. Durante la creazione di un'AMI Attestable, puoi quindi firmare il binario di avvio con il tuo certificato e installarlo come unico certificato consentito nelle AMI. UEFI-data Ricorda che questo modello richiede di generare comunque un nuovo certificato, installarlo nella tua policy e aggiornare le AMI se vuoi evitare che le istanze avviate da vecchie AMI (non attendibili) superino la tua policy KMS.
- PCR12: contiene l'hash della riga di comando passata al binario di avvio UEFI. Richiesto in combinazione con PCR4 per l'avvio standard per convalidare la riga di comando non è stato modificato.

Convalida un documento di attestazione NitroTPM

> **Note**
>
> Questo argomento è destinato agli utenti che utilizzano un servizio di gestione delle chiavi di terze parti e devono creare i propri meccanismi di convalida dei documenti di attestazione.

Questo argomento fornisce una panoramica dettagliata dell'intero flusso di attestazione NitroTPM. Descrive inoltre cosa viene generato dal sistema AWS Nitro quando viene richiesto un documento di attestazione e spiega come un servizio di gestione delle chiavi dovrebbe elaborare un documento di attestazione.

Argomenti

- Il documento di attestazione
- Convalida del documento di attestazione

Lo scopo dell'attestazione è dimostrare che un'istanza è un'entità affidabile, in base al codice e alla configurazione che sta eseguendo. La base della fiducia per l'istanza risiede nel sistema AWS Nitro, che fornisce i documenti di attestazione.

I documenti di attestazione sono firmati dalla AWS Nitro Attestation Public Key Infrastructure (PKI), che include un'autorità di certificazione pubblicata che può essere incorporata in qualsiasi servizio.

Il documento di attestazione

I documenti di attestazione sono codificati in Concise Binary Object Representation (CBOR) e firmati utilizzando CBOR Object Signing and Encryption (COSE).

Per ulteriori informazioni su CBOR, consulta RFC 8949: Concise Binary Object Representation (CBOR).

Specifiche del documento di attestazione

Il seguente esempio illustra la struttura di un documento di attestazione.

```
AttestationDocument = {
    module_id: text,                    ; issuing Nitro hypervisor module ID
    timestamp: uint .size 8,            ; UTC time when document was created, in
                                        ; milliseconds since UNIX epoch
```

```
    digest: digest,                     ; the digest function used for calculating the
                                        ; register values
    nitrotpm_pcrs: { + index => pcr },  ; map of PCRs at the moment the Attestation
 Document was generated
    certificate: cert,                  ; the public key certificate for the public
 key
                                        ; that was used to sign the Attestation
 Document
    cabundle: [* cert],                 ; issuing CA bundle for infrastructure
 certificate
    ? public_key: user_data,            ; an optional DER-encoded key the attestation
                                        ; consumer can use to encrypt data with
    ? user_data: user_data,             ; additional signed user data, defined by
 protocol
    ? nonce: user_data,                 ; an optional cryptographic nonce provided by
 the
                                        ; attestation consumer as a proof of
 authenticity
}

cert = bytes .size (1..1024)       ; DER encoded certificate
user_data = bytes .size (0..1024)
pcr = bytes .size (32/48/64)       ; PCR content
index = 0..31
digest = "SHA384"
```

I parametri facoltativi nel documento di attestazione (`public_key`,`user_data`, e `nonce`) possono essere utilizzati per stabilire un protocollo di convalida personalizzato tra un'istanza di attestazione e il servizio esterno.

Convalida del documento di attestazione

Quando richiedi un documento di attestazione dall'hypervisor Nitro, ricevi un blob binario che contiene il documento di attestazione firmato. Il documento di attestazione firmato è un CBOR-encoded oggetto COSE-signed (che utilizza la struttura di firma COSE_sign1). Il processo di convalida complessivo comprende le seguenti fasi:

1. Decodifica l'oggetto CBOR e mappalo su una struttura COSE_Sign1.
2. Estrai il documento di attestazione dalla struttura COSE_sign1.
3. Verifica la catena del certificato.
4. Controlla che il documento di attestazione sia firmato correttamente.

I documenti di attestazione sono firmati dalla AWS Nitro Attestation PKI, che include un certificato principale per le partizioni commerciali. AWS Il certificato root può essere scaricato da https://aws-nitro-enclaves.amazonaws.com/AWS_NitroEnclaves_Root-G1.zip e può essere verificato utilizzando la seguente impronta digitale.

```
64:1A:03:21:A3:E2:44:EF:E4:56:46:31:95:D6:06:31:7E:D7:CD:CC:3C:17:56:E0:98:93:F3:C6:8F:79:BB:5B
```

Il certificato principale si basa su una chiave AWS Certificate Manager privata Private Certificate Authority (AWS Private CA) e ha una durata di 30 anni. L'oggetto del PCA ha il seguente formato.

```
CN=aws.nitro-enclaves, C=US, O=Amazon, OU=AWS
```

Argomenti

- COSE e CBOR
- Validità semantica
- Validità dei certificati
- Validità della catena di certificati

COSE e CBOR

Di solito, la struttura della firma COSE_Sign1 viene utilizzata quando viene inserita una sola firma su un messaggio. I parametri relativi al contenuto e alla firma vengono inseriti nell'intestazione protetta invece di avere la separazione di COSE_Sign. La struttura può essere codificata come etichettata o senza tag, a seconda del contesto in cui verrà utilizzata. Una struttura COSE_Sign1 con tag è identificata dal tag CBOR 18.

L'oggetto CBOR che contiene il corpo, la firma e le informazioni sul corpo e sulla firma è chiamato struttura COSE_Sign1. La struttura COSE_Sign1 è un array CBOR. L'array include i seguenti campi.

```
[
  protected:   Header,
  unprotected: Header,
  payload:     This field contains the serialized content to be signed,
  signature:   This field contains the computed signature value.
]
```

Nel contesto di un documento di attestazione, l'array include quanto segue.

```
18(/* COSE_Sign1 CBOR tag is 18 */
    {1: -35}, /* This is equivalent with {algorithm: ECDS 384} */
    {}, /* We have nothing in unprotected */
    $ATTESTATION_DOCUMENT_CONTENT /* Attestation Document */,
    signature /* This is the signature */
)
```

Per ulteriori informazioni su CBOR, consulta RFC 8949: Concise Binary Object Representation (CBOR).

Validità semantica

Un documento di attestazione avrà sempre il relativo pacchetto CA nel seguente ordine.

```
[ ROOT_CERT - INTERM_1 - INTERM_2 .... - INTERM_N]
      0          1          2             N - 1
```

Tieni presente questo ordine, poiché alcuni strumenti esistenti, come quello di Java tratto CertPath dalla Java PKI API Programmer's Guide, potrebbero richiedere che vengano ordinati diversamente.

Per convalidare i certificati, inizia dal pacchetto Attestation Document CA e genera la catena richiesta, dove `TARGET_CERT` è il certificato nel documento di attestazione.

```
[TARGET_CERT, INTERM_N, ..... , INTERM_2, INTERM_1, ROOT_CERT]
```

Validità dei certificati

Per tutti i certificati della catena, devi assicurarti che la data corrente rientri nel periodo di validità specificato nel certificato.

Validità della catena di certificati

In generale, potrebbe servire una catena di più certificati, comprendente un certificato del proprietario della chiave pubblica firmato da una CA e zero o più certificati aggiuntivi di CA firmati da altre CA. Queste catene, chiamate percorsi di certificazione, sono necessarie perché un utente con chiave pubblica viene inizializzato solo con un numero limitato di chiavi pubbliche CA garantite. Le procedure di convalida del percorso di certificazione per la PKI Internet si basano sull'algoritmo fornito in. X.509 L'elaborazione del percorso di certificazione verifica l'associazione tra il nome distinto del soggetto, il nome alternativo del and/or soggetto e la chiave pubblica del soggetto. L'associazione è limitata dai vincoli specificati nei certificati che comprendono il percorso e gli input specificati dalla parte

affidante. I vincoli di base e le estensioni dei vincoli delle policy permettono alla logica di elaborazione del percorso di certificazione di automatizzare il processo decisionale.

> **Note**
>
> Il CRL deve essere disabilitato durante la convalida.

Utilizzando Java, a partire dal percorso principale e dalla catena di certificati generata, la convalida della catena è la seguente.

```
validateCertsPath(certChain, rootCertficate) {
    /* The trust anchor is the root CA to trust */
    trustAnchors.add(rootCertificate);

    /* We need PKIX parameters to specify the trust anchors
     * and disable the CRL validation
     */
    validationParameters = new PKIXParameters(trustAnchors);
    certPathValidator = CertPathValidator.getInstance(PKIX);
    validationParameters.setRevocationEnabled(false);

    /* We are ensuring that certificates are chained correctly */
    certPathValidator.validate(certPath, validationParameters);
}
```

Integrazione con AWS KMS

La tua istanza dovrebbe avere un'applicazione in grado di effettuare richieste AWS KMS API con il documento di attestazione recuperato da NitroTPM. Quando si effettua una richiesta con un documento di attestazione, AWS KMS convalida le misurazioni contenute nel documento di attestazione fornito rispetto alle misure di riferimento nella politica chiave del KMS. Le richieste sono consentite solo se le misurazioni nel Documento di Attestazione corrispondono alle misurazioni di riferimento nella policy della chiave KMS.

Quando si chiamano le operazioni Decrypt,, DeriveSharedSecret GenerateDataKey GenerateDataKeyPair, o GenerateRandom API con un documento di attestazione, queste API crittografano il testo in chiaro della risposta con la chiave pubblica del documento di attestazione e restituiscono testo cifrato anziché testo in chiaro. Questo testo criptato può essere decrittografato solo utilizzando la chiave privata corrispondente generata nell'istanza.

Per ulteriori informazioni, consulta Cryptographic attestation for NitroTPM nella Guida per gli sviluppatori AWS Key Management Service .

> **Note**
>
> Se stai attestando un servizio di terze parti, devi creare i tuoi meccanismi personalizzati per ricevere, analizzare e convalidare i documenti di attestazione. Per ulteriori informazioni, consulta Convalida un documento di attestazione NitroTPM.

Isola i dati dai tuoi operatori

Il sistema Nitro non ha alcun accesso da parte dell'operatore. AWS Non esiste alcun meccanismo per consentire a nessun AWS sistema o persona di accedere agli host Amazon EC2 Nitro, accedere alla memoria delle istanze EC2 o accedere ai dati dei clienti archiviati su uno storage di istanze crittografato locale o su volumi Amazon EBS crittografati remoti.

Durante l'elaborazione di dati altamente sensibili, potresti prendere in considerazione la possibilità di limitare l'accesso a tali dati impedendo anche ai tuoi operatori di accedere all'istanza EC2.

Puoi creare AMI Attestabili personalizzate configurate per offrire un ambiente di calcolo isolato. La configurazione AMI dipende dal carico di lavoro e dai requisiti dell'applicazione. Prendi in considerazione queste best practice quando crei la tua AMI per creare un ambiente di calcolo isolato.

- Rimuovi tutti gli accessi interattivi per impedire agli operatori o agli utenti di accedere all'istanza.
- Assicurati che nell'AMI siano inclusi solo software e codice affidabili.
- Configura un firewall di rete all'interno dell'istanza per bloccare l'accesso.
- Garantisci stati di sola lettura e immutabili per tutti gli archivi e i file system.
- Limita l'accesso delle istanze alle chiamate API autenticate, autorizzate e registrate.

Aggiornamento delle AMI attestabili che non hanno un accesso interattivo

Dopo aver avviato un'istanza utilizzando un ambiente di calcolo isolato (AMI), nessun utente o operatore può connettersi all'istanza. Ciò significa che non è possibile installare o aggiornare alcun software sull'istanza dopo l'avvio.

Se serve un nuovo software o un aggiornamento software, bisogna creare una nuova AMI attestabile che includa il software o gli aggiornamenti software richiesti. Quindi, utilizza quell'AMI per avviare una

nuova istanza o eseguire una sostituzione del volume root sull'istanza originale. Qualsiasi modifica software apportata all'AMI comporterà la generazione di un nuovo hash.

Le seguenti azioni comporteranno una modifica alle misurazioni di riferimento nel documento di attestazione NitroTPM:

- Arresto e avvio di un'istanza avviata con un'AMI attestabile
- Esecuzione di una sostituzione del volume root con un'AMI diversa

Se esegui una di queste azioni, devi aggiornare il servizio di attestazione con le nuove misurazioni di riferimento. Ad esempio, è necessario aggiornare la politica chiave del KMS in base alle nuove misurazioni di riferimento se la si utilizza AWS KMS per l'attestazione.

Un'istanza conserva il materiale chiave NitroTPM per l'intero ciclo di vita dell'istanza e persiste durante le operazioni di sostituzione del volume principale e durante le operazioni di sostituzione del volume principale. stop/starts

Credential Guard per istanze Windows

Il sistema AWS Nitro supporta Credential Guard per le istanze Windows di Amazon Elastic Compute Cloud (Amazon EC2). Credential Guard è una funzionalità di sicurezza basata sulla virtualizzazione di Windows (VBS) che consente la creazione di ambienti isolati per proteggere le risorse di sicurezza, come le credenziali utente di Windows e l'applicazione dell'integrità del codice, oltre alle protezioni del kernel di Windows. Quando esegui istanze EC2 Windows, Credential Guard utilizza il sistema AWS Nitro per proteggere le credenziali di accesso di Windows dall'estrazione dalla memoria del sistema operativo.

Indice

- Prerequisiti
- Avviare un'istanza supportata
- Disattivare l'integrità della memoria
- Attivare Credential Guard
- Verificare se Credential Guard è in esecuzione

Prerequisiti

L'istanza Windows deve soddisfare i seguenti prerequisiti per utilizzare Credential Guard.

Amazon Machine Images (AMI)

L'AMI deve essere preconfigurata per abilitare NitroTPM e UEFI Secure Boot. Per ulteriori informazioni sulle AMI supportate, consulta the section called "Requisiti".

Integrità della memoria

L'integrità della memoria, nota anche come Hypervisor-protected Code Integrity (HVCI) o Hypervisor enforced Code Integrity, non è supportata. Prima di attivare Credential Guard, devi assicurarti che questa funzionalità sia disattivata. Per ulteriori informazioni, consulta Disattivare l'integrità della memoria.

Tipi di istanza

I seguenti tipi di istanza supportano Credential Guard per tutte le dimensioni se non diversamente indicato: `C5`, `C5d`, `C5n`, `C6i`, `C6id`, `C6in`, `C7i`, `C7i-flex`, `M5`, `M5d`, `M5dn`, `M5n`, `M5zn`, `M6i`, `M6id`, `M6idn`, `M6in`, `M7i`, `M7i-flex`, `R5`, `R5b`, `R5d`, `R5dn`, `R5n`, `R6i`, `R6id`, `R6idn`, `R6in`, `R7i`, `R7iz`, `T3`.

> **Note**
>
> - Sebbene NitroTPM abbia in comune alcuni tipi di istanza obbligatori, il tipo di istanza deve essere uno dei precedenti per supportare Credential Guard.
> - Credential Guard non è supportato per:
>   - Istanze Bare Metal.
>   - I seguenti tipi di istanza: `C7i.48xlarge`, `M7i.48xlarge` e `R7i.48xlarge`.

Per ulteriori informazioni sui tipi di istanza, consulta Guida a tipi di istanza di Amazon EC2.

Avviare un'istanza supportata

Puoi utilizzare la console Amazon EC2 o AWS Command Line Interface (AWS CLI) per avviare un'istanza in grado di supportare Credential Guard. Avrai bisogno di un ID AMI compatibile per avviare l'istanza, che sia unico per ciascuna Regione AWS.

> **Tip**
>
> Puoi utilizzare il seguente link per scoprire e avviare istanze con AMI compatibili fornite da Amazon nella console Amazon EC2:

https://console.aws.amazon.com/ec2/v2/home?#Images:visibility=public-images;v=3;search=:TPM-Windows_Server;ownerAlias=amazon

Console

Per avviare un'istanza

Segui la procedura avviare di un'istanza specificando un tipo di istanza supportato e un'AMI Windows preconfigurata.

AWS CLI

Per avviare un'istanza

Utilizza il comando run-instances per avviare un'istanza utilizzando un tipo di istanza supportato e un'AMI Windows preconfigurata.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base \
    --instance-type c6i.large \
    --region us-east-1 \
    --subnet-id subnet-0abcdef1234567890
    --key-name key-name
```

PowerShell

Per avviare un'istanza

Utilizza il comando New-EC2Instance per avviare un'istanza utilizzando un tipo di istanza supportato e un'AMI Windows preconfigurata.

```
New-EC2Instance `
    -ImageId resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base `
    -InstanceType c6i.large `
    -Region us-east-1 `
    -SubnetId subnet-0abcdef1234567890 `
    -KeyName key-name
```

Disattivare l'integrità della memoria

È possibile utilizzare l'Editor Criteri di gruppo locali per disabilitare l'integrità della memoria negli scenari supportati. Le seguenti linee guida possono essere applicate per ciascuna impostazione di configurazione in Protezione basata su virtualizzazione dell'integrità del codice:

- Abilitata senza blocco: modifica l'impostazione impostandola su Disabilitato per disabilitare l'integrità della memoria.
- Abilitato con blocco UEFI: l'integrità della memoria è stata abilitata con il blocco UEFI. L'integrità della memoria non può essere disabilitata dopo che è stata abilitata con il blocco UEFI. Ti consigliamo di creare una nuova istanza con l'integrità della memoria disabilitata e di terminare l'istanza non supportata se non è in uso.

Per disabilitare l'integrità della memoria con l'Editor Criteri di gruppo locali

1. Connettiti alla tua istanza come account utente con privilegi di amministrazione utilizzando il protocollo RDP (Remote Desktop Protocol). Per ulteriori informazioni, consulta the section called "Connettiti utilizzando un client RDP".
2. Apri il menu Start e cerca **`cmd`** per avviare un prompt dei comandi.
3. Esegui i comandi seguenti per aprire l'Editor Criteri di gruppo locali: `gpedit.msc`
4. Nell'Editor Criteri di gruppo locali, scegli Configurazione computer, Modelli amministrativi, Sistema, Protezione dispositivi.
5. Seleziona Attiva la sicurezza basata sulla virtualizzazione, quindi seleziona Modifica impostazione delle policy.
6. Apri il menu a discesa delle impostazioni per Protezione basata su virtualizzazione dell'integrità del codice, scegli Disabilitata, quindi scegli Applica.
7. Riavvia l'istanza per applicare le modifiche.

Attivare Credential Guard

Dopo aver avviato un'istanza Windows con un tipo di istanza supportato e un'AMI compatibile e aver confermato che l'integrità della memoria è disabilitata, puoi attivare Credential Guard.

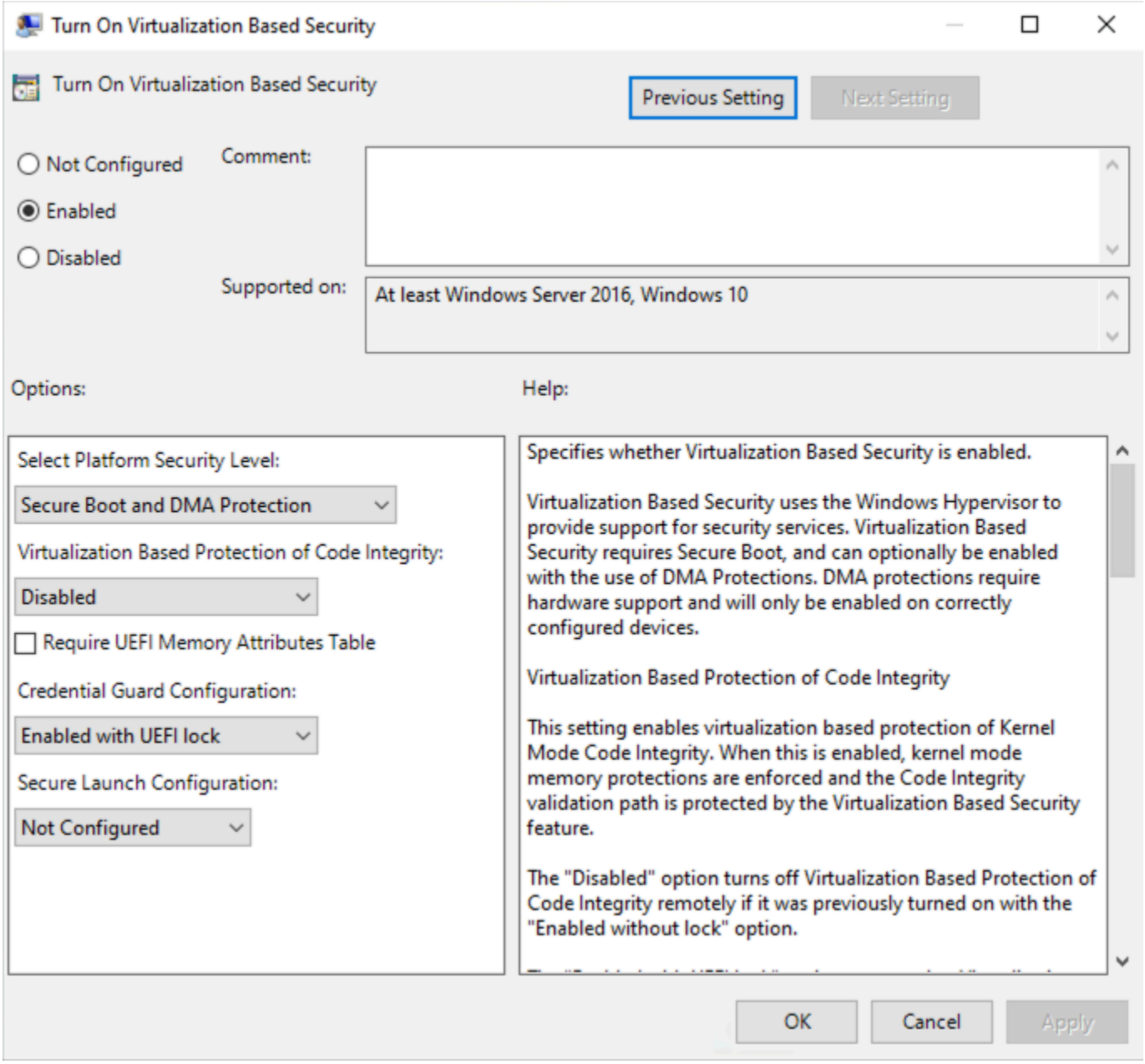
> **Important**
>
> Per eseguire i seguenti passaggi di attivazione di Credential Guard sono necessari i seguenti privilegi di amministratore.

Per attivare Credential Guard

1. Connettiti alla tua istanza come account utente con privilegi di amministrazione utilizzando il protocollo RDP (Remote Desktop Protocol). Per ulteriori informazioni, consulta the section called "Connettiti utilizzando un client RDP".
2. Apri il menu Start e cerca **`cmd`** per avviare un prompt dei comandi.
3. Esegui i comandi seguenti per aprire l'Editor Criteri di gruppo locali: `gpedit.msc`
4. Nell'Editor Criteri di gruppo locali, scegli Configurazione computer, Modelli amministrativi, Sistema, Protezione dispositivi.
5. Seleziona Attiva la sicurezza basata sulla virtualizzazione, quindi seleziona Modifica impostazione delle policy.
6. Scegli Abilitata nel menu Attiva la sicurezza basata sulla virtualizzazione.
7. Per Seleziona livello di sicurezza della piattaforma, scegli Secure Boot e protezione DMA.
8. Per Configurazione di Credential Guard, scegli Abilitato con blocco UEFI.

   > **Note**
   >
   > Le restanti impostazioni delle policy non sono necessarie per abilitare Credential Guard e possono essere lasciate come Non configurate.

   L'immagine seguente mostra le impostazioni VBS configurate come descritto in precedenza:



9. Riavvia l'istanza per applicare le impostazioni.

Verificare se Credential Guard è in esecuzione

Puoi utilizzare lo strumento Microsoft System Information (`Msinfo32.exe`) per confermare che Credential Guard è in esecuzione.

> **Important**
>
> È necessario innanzitutto riavviare l'istanza per completare l'applicazione delle impostazioni delle policy richieste per abilitare Credential Guard.

Per verificare se Credential Guard è in esecuzione

1. Connettiti all'istanza utilizzando il protocollo RDP (Remote Desktop Protocol). Per ulteriori informazioni, consulta the section called "Connettiti utilizzando un client RDP".
2. All'interno della sessione RDP dell'istanza, apri il menu Start e cerca **`cmd`** per avviare un prompt dei comandi.
3. Apri Informazioni sul sistema eseguendo il comando seguente: `msinfo32.exe`
4. Lo strumento Microsoft System Information elenca i dettagli per la configurazione VBS. Accanto a Servizi Virtualization-based di sicurezza, conferma che Credential Guard sia visualizzato come In esecuzione.

   L'immagine seguente mostra che VBS è in esecuzione come descritto in precedenza:

Virtualization-based security	Running
Virtualization-based security Required Security Properties	Base Virtualization Support, Secure Boot, DMA Protection
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Readonly, Mode Based Execution Control
Virtualization-based security Services Configured	Credential Guard
Virtualization-based security Services Running	Credential Guard

Accesso ad Amazon EC2 utilizzando un endpoint VPC di interfaccia

Puoi migliorare la sicurezza della tua VPC creando una connessione privata tra le risorse nella tua VPC e l'API Amazon EC2. Puoi accedere all'API Amazon EC2 come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. Direct Connect Le istanze EC2 presenti nel VPC non richiedono indirizzi IP pubblici per accedere all'API Amazon EC2.

Per ulteriori informazioni, consulta Access Servizi AWS through AWS PrivateLink nella Guida. AWS PrivateLink

Indice

- Creazione di un endpoint VPC dell'interfaccia

- Creazione di una policy di endpoint

Creazione di un endpoint VPC dell'interfaccia

Crea un endpoint di interfaccia per Amazon EC2 utilizzando uno dei seguenti nomi di servizi:

- com.amazonaws. ***region***.ec2 — Crea un endpoint per le azioni dell'API Amazon EC2.

Per ulteriori informazioni, consulta Accedere a un endpoint VPC Servizio AWS utilizzando un'interfaccia nella Guida. AWS PrivateLink

Creazione di una policy di endpoint

Una policy di endpoint è una risorsa IAM che è possibile allegare all'endpoint di interfaccia. La policy di endpoint di default permette l'accesso completo all'API Amazon EC2 tramite l'endpoint di interfaccia. Per controllare l'accesso consentito all'API Amazon EC2 dal VPC, allegare una policy di endpoint personalizzata all'endpoint di interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali che possono eseguire operazioni.
- Le operazioni che possono essere eseguite.
- La risorsa su cui è possibile eseguire le operazioni.

> **Important**
>
> Quando viene applicata una policy non predefinita a un endpoint VPC di interfaccia per Amazon EC2, alcune richieste API non riuscite, come quelle provenienti da`RequestLimitExceeded`, potrebbero non essere registrate su Amazon. AWS CloudTrail CloudWatch

Per ulteriori informazioni, consulta la sezione Controllo dell'accesso ai servizi con policy di endpoint nella Guida di AWS PrivateLink .

Nell'esempio seguente viene illustrata una policy endpoint VPC che nega l'autorizzazione per creare volumi non crittografati o per lanciare istanze con volumi non crittografati. Inoltre, la policy di esempio concede a chiunque l'autorizzazione per eseguire tutte le altre operazioni Amazon EC2.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Action": [
            "ec2:CreateVolume"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    },
    {
        "Action": [
            "ec2:RunInstances"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    }]
}
```

Opzioni di archiviazione per le istanze Amazon EC2

Amazon EC2 offre opzioni di archiviazione dei dati flessibili, convenienti e di facile utilizzo per le proprie istanze. Ogni opzione è associata a un'esclusiva combinazione di prestazioni e durabilità. Queste opzioni di archiviazione possono essere utilizzate in modo indipendente oppure combinate, per adattarsi alle proprie esigenze.

Storage a blocchi

- Amazon EBS: Amazon EBS fornisce volumi di archiviazione a blocchi durevoli che possono essere collegati e scollegati dalle istanze. È possibile collegare più volumi EBS a una singola istanza. Un volume EBS persiste indipendentemente dalla vita di esecuzione dell'istanza associata. Puoi crittografare i tuoi volumi EBS. Per conservare una copia di backup dei dati, è possibile creare snapshot dai volumi EBS. Gli snapshot vengono archiviati in Amazon S3. È possibile creare un volume EBS da uno snapshot.
- Archivio dell'istanza archiviazione a blocchi temporanea per le istanze EC2: l'archivio istanza offre un'archiviazione a blocchi temporanea per le istanze. Il numero, la dimensione e il tipo di volumi dell'archivio dell'istanza sono determinati dal tipo e dalla dimensione dell'istanza. I dati contenuti in un volume di archivio istanze sono persistenti solo per la durata dell'istanza associata; se arresti, iberni o termini un'istanza, i dati nei volumi dell'archivio istanze andranno perduti.

Archiviazione di oggetti

- Simple Storage Service (Amazon S3): Amazon S3 fornisce l'accesso a un'infrastruttura di archiviazione di dati affidabile e conveniente. È progettata per semplificare le operazioni di calcolo a livello di Web, permettendoti di archiviare e recuperare una quantità qualsiasi di dati, in qualsiasi momento, dall'interno di Amazon EC2 o da qualsiasi posizione sul Web. Ad esempio, puoi usare Amazon S3 per archiviare le copie di backup dei dati e delle applicazioni. Amazon EC2 utilizza Amazon S3 per archiviare snapshot EBS e Amazon AMI. S3-backed

Archiviazione dei file

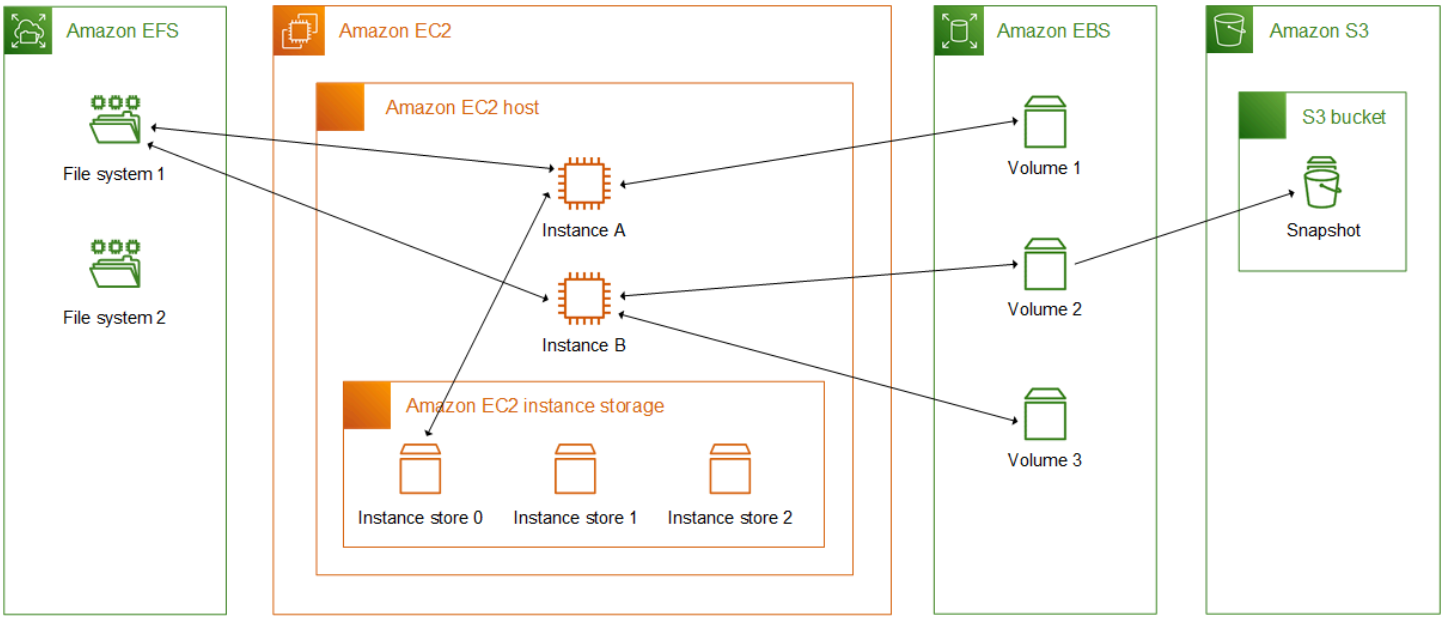
- Amazon EFS (Solo istanze Linux): Amazon EFS fornisce l'archiviazione di file scalabile da utilizzare con Amazon EC2. Puoi creare un file system EFS e configurare le istanze per montare il file system. Puoi utilizzare un file system EFS come origine dati comune per carichi di lavoro e applicazioni in esecuzione su più istanze.
- Amazon FSx: con Amazon FSx, puoi avviare, eseguire e scalare file system ricchi di funzionalità e ad alte prestazioni nel cloud. Amazon FSx è un servizio completamente gestito

che supporta un'ampia gamma di carichi di lavoro. Puoi scegliere tra questi file system ampiamente utilizzati: Lustre, ONTAP, NetApp OpenZFS e Windows File Server.

Memorizzazione nella cache dei file

- Usa Amazon File Cache con le EC2 istanze Amazon— Amazon File Cache fornisce una cache temporanea ad alte prestazioni AWS per l'elaborazione dei dati dei file. La cache fornisce l'accesso ai dati di lettura e scrittura ai carichi di lavoro di calcolo su Amazon EC2 con latenze inferiori al millisecondo, fino a centinaia di throughput e fino a milioni GB/s di IOPS.

L'illustrazione seguente mostra la relazione tra queste opzioni di archiviazione e la tua istanza.



AWS Prezzi dello archiviazione

Apri AWS Prezzi, scorri fino a Prezzi dei AWS prodotti e seleziona Storage. Scegli il prodotto di archiviazione per aprirne la pagina dei prezzi.

Storage a blocchi persistente Amazon EBS per istanze Amazon EC2

Amazon Elastic Block Store (Amazon EBS) fornisce risorse di archiviazione a blocchi scalabili e ad alte prestazioni che possono essere utilizzate con le istanze Amazon EC2. Con Amazon EBS, è possibile creare e gestire le seguenti risorse di archiviazione a blocchi:

- Volumi Amazon EBS: si tratta di volumi di archiviazione che è possibile collare alle istanze Amazon EC2. Dopo aver collegato un volume a un'istanza, è possibile utilizzarlo nello stesso modo in cui si utilizza l'archiviazione a blocchi. L'istanza può interagire con il volume proprio come farebbe con un'unità locale.
- Snapshot di Amazon EBS: si tratta di backup point-in-time di volumi Amazon EBS che persistono indipendentemente dal volume stesso. È possibile creare snapshot per eseguire il backup dei dati nei volumi Amazon EBS. È quindi possibile ripristinare nuovi volumi da tali snapshot in qualsiasi momento.

È possibile creare e collegare volumi EBS a un'istanza durante e in qualsiasi momento dopo l'avvio. È possibile anche aumentare le dimensioni o le prestazioni dei volumi EBS senza scollegare il volume o riavviare l'istanza.

È possibile creare snapshot EBS da un volume EBS in qualsiasi momento dopo la creazione. È possibile utilizzare gli snapshot EBS per eseguire il backup dei dati archiviati nei volumi. È quindi possibile utilizzare queste istantanee per ripristinare istantaneamente i volumi o per migrare i dati tra Account AWS AWS regioni o zone di disponibilità. Puoi utilizzare Amazon Data Lifecycle Manager o AWS Backup automatizzare la creazione, la conservazione e l'eliminazione degli snapshot EBS.

Un volume EBS gestito è gestito da un fornitore di servizi, come Amazon EKS Auto Mode. Non è possibile modificare direttamente le impostazioni di un volume EBS gestito. I volumi EBS gestiti sono identificati dal valore vero nel campo Gestito. Per ulteriori informazioni, consulta Istanze gestite di Amazon EC2.

Per ulteriori informazioni sull'utilizzo di volumi e snapshot, consulta la Guida per l'utente di Amazon EBS.

Limiti di volume di Amazon EBS per le istanze Amazon EC2

Il numero massimo di volumi Amazon EBS che puoi collegare a un'istanza dipende dal tipo e dalle dimensioni dell'istanza. Se si supera il limite di volume degli allegati per un'istanza, la richiesta di allegati ha esito negativo e viene visualizzato l'errore `AttachmentLimitExceeded`.

Quando consideri quanti volumi collegare alla tua istanza, dovresti considerare se hai bisogno di una maggiore larghezza di banda o di una maggiore I/O capacità di archiviazione.

Larghezza di banda e capacità

Per casi d'uso coerenti e prevedibili della larghezza di banda, utilizza EBS-optimized le istanze Amazon con volumi SSD General Purpose o volumi SSD IOPS con provisioning. Per ottimizzare le prestazioni, segui le linee guida riportate nella sezione per individuare la corrispondenza corretta tra l'IOPS per il quale hai eseguito il provisioning per i volumi in uso e la larghezza di banda delle istanze.

Per le configurazioni RAID, è possibile che gli array di dimensioni superiori a 8 volumi abbiano rendimenti prestazionali ridotti a causa dell'aumento del sovraccarico. I/O Esegui il test delle prestazioni di un'applicazione specifica e apporta le modifiche richieste, se necessario.

Indice

- Limiti di volume per le istanze basate sul sistema Nitro
  - Limite di volume EBS dedicato
  - Limite di volume EBS condiviso
- Limiti Xen-based di volume per le istanze
  - Istanze Linux
  - Istanze Windows

Limiti di volume per le istanze basate sul sistema Nitro

I limiti di volume per le istanze create sul sistema Nitro dipendono dal tipo di istanza. Alcuni tipi di istanze Nitro hanno un limite di volume EBS dedicato, mentre la maggior parte ha un limite di volume condiviso. Per visualizzare i limiti degli allegati al volume per ogni tipo di istanza, consulta quanto segue:

- Specifiche di Amazon EBS: uso generale
- Specifiche di Amazon EBS: calcolo ottimizzato
- Specifiche di Amazon EBS: memoria ottimizzata
- Specifiche di Amazon EBS: archiviazione ottimizzata
- Specifiche di Amazon EBS: calcolo accelerato
- Specifiche di Amazon EBS: elaborazione High-performance
- Specifiche di Amazon EBS: generazione precedente

Limite di volume EBS dedicato

I seguenti tipi di istanze Nitro hanno un limite di volume Amazon EBS dedicato fino che varia a seconda delle dimensioni dell'istanza. Il limite non è condiviso con altri allegati del dispositivo. In altre parole, puoi collegare un numero qualsiasi di volumi EBS fino al limite di allegati al volume, indipendentemente dal numero di dispositivi collegati, come i volumi dell'archivio dell'istanza NVMe e le interfacce di rete.

- Uso generale: M7a | M7i | | M8a | M8azn | M8g M7i-flex | M8gb | M8gd | M8gn | M8i | M8id | | M8in | M8idn | M8ine | M8ib | M8iB | M8idb | M9g | M9gd M8i-flex
- Ottimizzato per il calcolo: C7a | C7i C7i-flex | | C8a | C8g | C8gb | C8gd | C8gn | C8i | C8id C8i-flex | | C8in | C8ine | C8ib | C9g | C9gd
- Memoria ottimizzata: R7a | R7i | R7iZ | R8a | R8g | R8gb | R8gd | R8gn | R8i | R8id | | | R8in R8i-flex | R8iN | R8ib | R8idb | R9g | | | | | | | | X8g U7i-6tb U7i-8tb U7i-12tb | X8aedz U7in-16tb U7in-24tb U7in-32tb U7inh-32tb | X8i
- Archiviazione ottimizzata: I7i | I7ie | I8g | I8ge
- Calcolo accelerato: F2 | G6 | G6e | G6f | Gr6 | Gr6f | G7 | G7e | P4d | P4de | P5 | P5e | P5en P6-B200 | P6-B300 | P6e-GB200 | Trn2 | Trn2u
- Calcolo ad alte prestazioni: HPC7a | HPC8a

Limite di volume EBS condiviso

Tutti gli altri tipi di istanze Nitro (non elencate in Limite di volume EBS dedicato) hanno un limite di allegati ai volumi condiviso tra i volumi Amazon EBS, le interfacce di rete e i volumi di archiviazione delle istanze NVMe. Puoi collegare un numero qualsiasi di volumi Amazon EBS fino a quel limite, meno il numero di interfacce di rete collegate e i volumi di archiviazione delle istanze NVMe. Tieni presente che ogni istanza deve avere almeno un'interfaccia di rete e che i volumi di archiviazione delle istanze NVMe vengono collegati automaticamente all'avvio.

La maggior parte delle istanze Nitro supporta un massimo di 28 allegati. Negli esempi seguenti viene illustrato come calcolare il numero di volumi EBS che è possibile collegare.

Esempi

- Con un'istanza `m5.xlarge` con solo l'interfaccia di rete principale, è possibile collegare 27 volumi EBS.

  28 volumi - 1 interfaccia di rete = 27

- Con un'istanza `m5.xlarge` con due interfacce di rete aggiuntive, è possibile collegare 25 volumi EBS.

  28 volumi - 3 interfacce di rete = 25
- Con un'istanza `m5d.xlarge` con due interfacce di rete aggiuntive, è possibile collegare 24 volumi EBS.

  28 volumi - 3 interfacce di rete - 1 volume di archivio dell'istanza NVMe = 24

Limiti Xen-based di volume per le istanze

I limiti di volume per Xen-based le istanze, come T2, dipendono dal sistema operativo.

Per ulteriori informazioni, consulta Xen-based Istanze.

Istanze Linux

Il collegamento di più di 40 volumi a un'istanza Xen-based Linux può causare errori di avvio. Questo numero include il volume root, qualsiasi volume di archivio dell'istanza collegato e i volumi Amazon EBS.

Se si verificano problemi di avvio su un'istanza con un numero elevato di volumi, arresta l'istanza, scollega i volumi non importanti per il processo di avvio, quindi ricollega i volumi quando l'istanza è in esecuzione.

> **Important**
>
> Il collegamento di più di 40 volumi a un'istanza Xen-based Linux è supportato solo nel migliore dei modi e non è garantito.

Istanze Windows

La tabella seguente mostra i limiti di volume per le istanze Xen-based Windows in base al driver utilizzato. Questi numeri includono il volume root, qualsiasi volume di archivio dell'istanza collegato e i volumi Amazon EBS.

Driver	Limite di volumi
AWS PV	26

Driver	Limite di volumi
Citrix PV	26
Red Hat PV	17

Si consiglia di non collegare più di 26 volumi a un'istanza Xen-based Windows con driver AWS PV o Citrix PV, poiché è probabile che ciò causi problemi di prestazioni. Per determinare i driver PV utilizzati dall'istanza o per aggiornare l'istanza Windows dai driver Red Hat ai driver Citrix PV, consulta the section called "Aggiornamento dei driver PV".

> **Important**
>
> Il collegamento di più del seguente numero di volumi a un'istanza Xen-based Windows è supportato solo se necessario e non è garantito.

Per ulteriori informazioni su come i nomi dei dispositivi sono correlati ai volumi, vedereCome vengono collegati e mappati i volumi per le istanze Windows di Amazon EC2.

Schede EBS

La maggior parte dei tipi di istanza supporta una scheda EBS. I tipi di istanza che supportano più schede EBS offrono EBS-optimized prestazioni più elevate, sia in termini di throughput EBS che di IOPS. Le prestazioni massime della tua istanza Amazon EC2 sono distribuite equamente su ciascuna scheda EBS. Ad esempio, su un'istanza EC2 che supporta IOPS `1,000,000` totali con 2 schede EBS, ciascuna scheda EBS può supportare fino a IOPS. `500,000` Per informazioni sulle prestazioni Amazon EBS supportate della tua istanza Amazon EC2, consulta. Tipi di istanze Amazon EBS-optimized

Quando colleghi un volume Amazon EBS a un'istanza che supporta più schede EBS, puoi selezionare la scheda EBS per il volume specificando l'indice della scheda EBS. Il volume principale deve essere collegato all'indice della scheda EBS 0.

Tipi di istanza con più schede EBS

I seguenti tipi di istanza supportano più schede EBS. Per informazioni sul numero di volumi Amazon EBS supportati da un tipo di istanza, consulta. Limiti di volume di Amazon EBS per le istanze Amazon EC2

Tipo di istanza	Numero di schede EBS
Uso generale	
8 gb. 48 x large	2
8 gb. in metallo - 48xl	2
m8gn.48x grande	2
m8gn.metallo-48xl	2
m 8 pollici 96 x grande	2
metallo da 8 pollici - 96xl	2
m8idn.96xlarge	2
m8idn.metallo-96xl	2
m8ib.96x grande	2
m8ib.metallo-96xl	2
m8idb.96xlarge	2
m8idb.metallo-96xl	2
Ottimizzazione per il calcolo	
c8 gb.48x grande	2
c8gb.metallo-48xl	2
c8gn.48xlarge	2

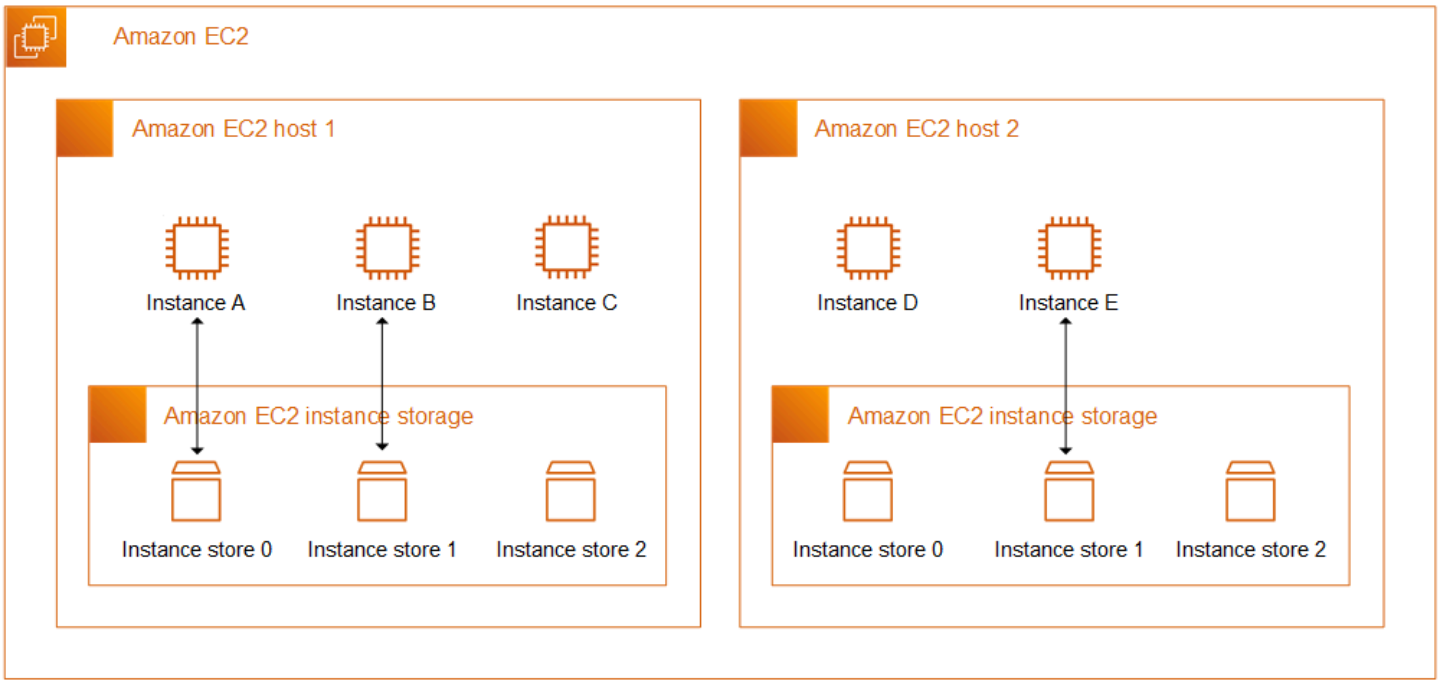
Tipo di istanza	Numero di schede EBS
c8gn.metal-48xl	2
c8in.96x grande	2
Metallo da 8 pollici - 96xl	2
c8ib.96x grande	2
c8ib.metallo-96xl	2
Ottimizzazione per la memoria	
r8gb.48x large	2
r8gb.metal-48xl	2
r8gn.48xlarge	2
r8gn.metal-48xl	2
R8in.96x grande	2
R8 pollici in metallo - 96xl	2
r8idn.96xlarge	2
r8idn.metallo-96xl	2
r8ib.96x grande	2
r8ib.metallo-96xl	2
r8idb.96xlarge	2
r8idb.metallo-96xl	2
Calcolo accelerato	
g 7.48x grande	2

Archivio dell'istanza archiviazione a blocchi temporanea per le istanze EC2

Un archivio dell'istanza fornisce un'archiviazione a blocchi temporanea per l'istanza EC2. Questo storage è fornito da dei dischi fisicamente collegati al computer host. L'archivio dell'istanza è ideale per l'archiviazione temporanea di informazioni che cambiano frequentemente, quali buffer, cache, dati Scratch e altri contenuti temporanei. Inoltre, è possibile utilizzarlo per l'archiviazione di dati temporanei che vengono replicati in un parco istanze, come il pool per il sistema di bilanciamento del carico dei server Web.

Un instance store consta di uno o più volumi di instance store esposti come dispositivi a blocchi. La dimensione di un archivio dell'istanza e il numero dei dispositivi disponibili variano a seconda del tipo di istanza. Ad esempio, non tutti i tipi di istanza forniscono i volumi dell'archivio dell'istanza. Per ulteriori informazioni, consulta Limiti di volume di archivio dell'istanza per le istanze EC2.

Ai dispositivi virtuali per i volumi dell'archivio dell'istanza vengono assegnati dei nomi da `ephemeral0` a `ephemeral23`. Ad esempio, con un tipo di istanza che supporta un volume dell'archivio dell'istanza, il nome del dispositivo virtuale del volume è `ephemeral0`. Con un tipo di istanza che supporta quattro volumi dell'archivio dell'istanza, i nomi dei dispositivi virtuali dei quattro volumi sono i seguenti: `ephemeral0`, `ephemeral1`, `ephemeral2` e `ephemeral3`.



Prezzi dell'archivio dell'istanza

Non sono previsti costi aggiuntivi per l'utilizzo dei volumi di archivio dell'istanza forniti per l'istanza. I volumi di archivio dell'istanza sono inclusi nel costo dell'utilizzo dell'istanza.

Indice

- Persistenza dei dati per i volumi di archivio dell'istanza Amazon EC2
- Limiti di volume di archivio dell'istanza per le istanze EC2
- Volumi di archivio dell'istanza SSD per istanze EC2
- Aggiunta di volumi di archivio dell'istanza a un'istanza EC2
- Abilita il volume di swap dell'archivio dell'istanza per le istanze EC2 M1 e C1
- Inizializza i volumi dell'archivio dell'istanza sulle istanze EC2
- Statistiche dettagliate delle prestazioni per i volumi di archivio dell'istanza Amazon EC2

Persistenza dei dati per i volumi di archivio dell'istanza Amazon EC2

I volumi dell'archivio dell'istanza vengono collegati solo all'avvio dell'istanza. Non puoi collegare un volume dell'archivio dell'istanza dopo l'avvio. Non puoi scollegare un volume dell'archivio dell'istanza da un'istanza e collegarlo a un'altra.

Un volume dell'archivio dell'istanza esiste solo durante la durata dell'istanza a cui è collegato. Non puoi configurare un volume dell'archivio dell'istanza in modo che persista oltre la durata dell'istanza associata.

I dati presenti in un volume dell'archivio dell'istanza persistono anche se l'istanza viene riavviata. Tuttavia, i dati non persistono se l'istanza viene arrestata, ibernata o terminata. Quando l'istanza viene arrestata, ibernata o terminata, ogni blocco del volume dell'archivio dell'istanza viene cancellato crittograficamente.

Pertanto, è consigliabile non fare affidamento sui volumi dell'archivio dell'istanza per dati preziosi e a lungo termine. Se devi mantenere i dati archiviati su un volume dell'archivio dell'istanza oltre la durata dell'istanza, devi copiarli manualmente su un'archiviazione più persistente, come un volume Amazon EBS, un bucket Amazon S3 o un file system Amazon EFS.

Alcuni eventi possono far sì che i dati non persistano per tutta la durata dell'istanza. La tabella seguente indica se i dati sui volumi dell'archivio dell'istanza vengono mantenuti durante eventi specifici, sia per le istanze virtualizzate che per quelle bare metal.

Event	Cosa succede ai tuoi dati?
User-initiated eventi del ciclo di vita delle istanze	
L'istanza viene riavviata	I dati persistono
L'istanza viene interrotta	I dati non persistono
L'istanza è ibernata	I dati non persistono
L'istanza è terminata	I dati non persistono
Il tipo di istanza è cambiato	I dati non persistono *
Dall' EBS-backed istanza viene creata un'AMI	I dati non rimangono nell'AMI creata **
Un'Amazon S3-backed AMI viene creata dall'istanza (istanze Linux)	I dati persistono nel pacchetto AMI caricato su Amazon S3 ***
User-initiated Eventi del sistema operativo	
Viene avviato un arresto	I dati non persistono †
Viene avviato un riavvio	I dati persistono
AWS eventi programmati	
Interruzione dell'istanza	I dati non persistono
Riavvio dell'istanza	I dati persistono
Riavvio del sistema	I dati persistono
Ipotesi di pensionamento	I dati non persistono
Eventi non pianificati	
Ripristino automatico semplificato	I dati non persistono
CloudWatch ripristino basato sull'azione	I dati non persistono
Il disco sottostante non funziona	I dati sul disco guasto non persistono

Event	Cosa succede ai tuoi dati?
Interruzione dell'alimentazione	I dati persistono al riavvio

* Se il nuovo tipo di istanza supporta l'archivio dell'istanza, l'istanza ottiene il numero di volumi di quest'ultimo supportati dal nuovo tipo di istanza, ma i dati non vengono trasferiti all'istanza nuova. Se il nuovo tipo di istanza non supporta l'archivio dell'istanze, l'istanza non ottiene i volumi di quest'ultimo.

** I dati non sono inclusi nell' EBS-backed AMI e non sono inclusi nei volumi degli store di istanze collegati alle istanze avviate da tale AMI.

*** I dati sono inclusi nel bundle AMI che viene caricato su Amazon S3. Quando avvii un'istanza da tale AMI, l'istanza ottiene i volumi dell'archivio dell'istanza raggruppati nell'AMI con i dati che contenevano al momento della creazione di quest'ultima.

† La protezione dalla terminazione e dall'arresto delle istanze non le protegge dagli arresti o dalle terminazioni dovute alle interruzioni avviate tramite il sistema operativo dell'istanza. I dati archiviati nei volumi dell'archivio dell'istanza non persistono sia negli eventi di arresto che in quelli di terminazione dell'istanza.

Limiti di volume di archivio dell'istanza per le istanze EC2

Il numero, la dimensione e il tipo di volumi dell'archivio dell'istanza sono determinati dal tipo dell'istanza. Alcuni tipi di istanza, come C8i, M8i e R8i, non supportano i volumi di archiviazione delle istanze, mentre altri tipi di istanza, come C8id, M8id e R8id, supportano i volumi di archiviazione delle istanze. Non puoi collegare più volumi dell'archivio dell'istanza a un'istanza di quelli supportati dal tipo di istanza. Per i tipi di istanze che supportano i volumi dell'archivio dell'istanza, il numero e le dimensioni di questi ultimi variano in base alla dimensione dell'istanza. Ad esempio, `r8id.large` supporta 1 volume di archiviazione delle istanze da 118 GB, mentre supporta 2 volumi di archiviazione delle istanze da 3800 GB. `r8id.32xlarge`

Per i tipi di istanze con volumi dell'archivio dell'istanza NVMe, tutti i volumi dell'archivio dell'istanza supportati vengono automaticamente collegati all'istanza all'avvio. Per i tipi di istanze con volumi dell'archivio dell'istanza non NVMe, come C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 e X1e, devi specificare manualmente le mappature dei dispositivi a blocchi per i volumi dell'archivio dell'istanza che desideri collegare all'avvio. Quindi, dopo l'avvio dell'istanza, devi formattare e montare i volumi

dell'archivio dell'istanza collegati prima di poterli utilizzare. Non puoi collegare un volume dell'archivio dell'istanza dopo l'avvio dell'istanza.

Alcuni tipi di istanze utilizzano NVMe o unità a stato SATA-based solido (SSD), mentre altri utilizzano unità disco SATA-based rigido (HDD). Gli SSD offrono I/O prestazioni casuali elevate con una latenza molto bassa, ma non è necessario che i dati persistano quando l'istanza termina o si possono sfruttare le architetture con tolleranza ai guasti. Per ulteriori informazioni, consulta Volumi di archivio dell'istanza SSD per istanze EC2.

I dati sui volumi dell'archivio istanza NVMe e alcuni volumi dell'archivio istanza HDD sono crittografati a riposo. Per ulteriori informazioni, consulta Protezione dei dati in Amazon EC2.

Volumi di archivio dell'istanza disponibili

La Guida ai tipi di istanza di Amazon EC2 mostra la quantità, le dimensioni, il tipo e le ottimizzazioni delle prestazioni per i volumi di archivio dell'istanza disponibili su ogni tipo di istanza supportata. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Specifiche dell'archivio dell'istanza: uso generale
- Specifiche dell'archivio dell'istanza: calcolo ottimizzato
- Specifiche dell'archivio dell'istanza: memoria ottimizzata
- Specifiche dell'archivio dell'istanza: archiviazione ottimizzata
- Specifiche dell'archivio dell'istanza: elaborazione accelerata
- High-performance Specifiche dell'Instance Store: elaborazione
- Specifiche dell'archivio dell'istanza: generazione precedente

Console

Recuperare le informazioni sul volume dell'archivio dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instance Types (Tipi di istanza).
3. Aggiungi il filtro Local instance storage = true. La colonna Storage indica la dimensione totale dell'archivio dell'istanza per il tipo di istanza.
4. (Facoltativo) Scegli l'icona Preferenze, quindi attiva il numero di dischi di archiviazione. Questa colonna indica il numero di volumi di archivio dell'istanza.
5. (Facoltativo) Aggiungi filtri per approfondire l'ambito di specifici tipi di istanze di interesse.

AWS CLI

Recuperare le informazioni sul volume dell'archivio dell'istanza

Utilizza il comando describe-instance-types. L'esempio seguente mostra la dimensione totale dello spazio di archiviazione delle istanze per ogni tipo di istanza nelle famiglie di istanze R8i con volumi di archiviazione delle istanze.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r8i*" "Name=instance-storage-
supported,Values=true" \
    --query 'sort_by(InstanceTypes, &InstanceStorageInfo.TotalSizeInGB)[].
{InstanceType:InstanceType,TotalSizeInGB:InstanceStorageInfo.TotalSizeInGB}' \
    --output table
```

Di seguito è riportato un output di esempio.

```
-------------------------------------
|        DescribeInstanceTypes       |
+------------------+-----------------+
|   InstanceType   |  TotalSizeInGB  |
+------------------+-----------------+
|  r8id.large      |  118            |
|  r8id.xlarge     |  237            |
|  r8id.2xlarge    |  474            |
|  r8id.4xlarge    |  950            |
|  r8id.8xlarge    |  1900           |
|  r8id.12xlarge   |  2850           |
|  r8id.16xlarge   |  3800           |
|  r8id.24xlarge   |  5700           |
|  r8id.32xlarge   |  7600           |
|  r8id.48xlarge   |  11400          |
|  r8id.metal-48xl |  11400          |
|  r8id.96xlarge   |  22800          |
|  r8id.metal-96xl |  22800          |
+------------------+-----------------+
```

Per ottenere dettagli completi sull'archiviazione dell'istanza per un tipo di istanza

Utilizza il comando describe-instance-types.

```
aws ec2 describe-instance-types \
```

```
    --filters "Name=instance-type,Values=r8id.32xlarge" \
    --query 'InstanceTypes[0].InstanceStorageInfo' \
    --output json
```

L'output di esempio mostra che questo tipo di istanza ha due volumi SSD NVMe da 3800 GB, per un totale di 7600 GB di storage di istanze.

```
{
    "TotalSizeInGB": 7600,
    "Disks": [
        {
            "SizeInGB": 3800,
            "Count": 2,
            "Type": "ssd"
        }
    ],
    "NvmeSupport": "required",
    "EncryptionSupport": "required"
}
```

PowerShell

Recuperare le informazioni sul volume dell'archivio dell'istanza

Utilizza il cmdlet Get-EC2InstanceType. L'esempio seguente visualizza la dimensione totale dello spazio di archiviazione delle istanze per ogni tipo di istanza nelle famiglie di istanze R8i con volumi di archiviazione delle istanze.

```
(Get-EC2InstanceType -Filter `
    @{Name="instance-type"; Values="r8i*"},
    @{Name="instance-storage-supported"; Values="true"}) |
    Sort-Object {$_.InstanceStorageInfo.TotalSizeInGB} |
    Format-Table InstanceType,

 @{Name="Disks.SizeInGB";Expression={$_.InstanceStorageInfo.Disks[0].SizeInGB}},
        @{Name="Disks.Count";Expression={$_.InstanceStorageInfo.Disks[0].Count}},
        @{Name="TotalSizeInGB";Expression={$_.InstanceStorageInfo.TotalSizeInGB}}
```

Di seguito è riportato un output di esempio.

```
InstanceType    Disks.SizeInGB Disks.Count TotalSizeInGB
```

```
------------    -------------- ----------- -------------
r8id.large                118           1           118
r8id.xlarge               237           1           237
r8id.2xlarge              474           1           474
r8id.4xlarge              950           1           950
r8id.8xlarge             1900           1          1900
r8id.12xlarge            2850           1          2850
r8id.16xlarge            3800           1          3800
r8id.24xlarge            2850           2          5700
r8id.32xlarge            3800           2          7600
r8id.48xlarge            3800           3         11400
r8id.metal-48xl          3800           3         11400
r8id.96xlarge            3800           6         22800
r8id.metal-96xl          3800           6         22800
```

Per ottenere dettagli completi sull'archiviazione dell'istanza per un tipo di istanza

Utilizza il cmdlet Get-EC2InstanceType.

```
(Get-EC2InstanceType `
    -Filter @{Name="instance-type"; Values="r8id.32xlarge"}).InstanceStorageInfo |
    Format-List *,
        @{Name="Disks.Count";Expression={$_.Disks[0].Count}},
        @{Name="Disks.SizeInGB";Expression={$_.Disks[0].SizeInGB}},
        @{Name="Disks.Type";Expression={$_.Disks[0].Type.Value}}
```

L'output di esempio mostra che questo tipo di istanza ha due volumi SSD NVMe da 3800 GB, per un totale di 7600 GB di storage di istanze.

```
Disks             : {Amazon.EC2.Model.DiskInfo}
EncryptionSupport : required
NvmeSupport       : required
TotalSizeInGB     : 7600
Disks.Count       : 2
Disks.SizeInGB    : 3800
Disks.Type        : ssd
```

Volumi di archivio dell'istanza SSD per istanze EC2

Come avviene per gli altri volumi di instance store, è necessario eseguire la mappatura dei volumi di instance store dell'istanza all'avvio di essa. I dati su un volume di instance di un SSF persistono solo

durante la vita dell'istanza associata. Per ulteriori informazioni, consulta Aggiunta di volumi di archivio dell'istanza a un'istanza EC2.

Volumi SSD NVMe

Alcune istanze offrono volumi di instance store SSD di tipo NVMe (Non-Volatile Memory Express). Per ulteriori informazioni sul tipo di volume di instance store supportato da ciascun tipo di istanza, consulta Limiti di volume di archivio dell'istanza per le istanze EC2.

I dati sullo storage delle istanze NVMe sono crittografati utilizzando un codice a XTS-AES-256 blocchi implementato in un modulo hardware sull'istanza. Le chiavi crittografiche sono generate utilizzando il modulo hardware e sono univoche per ciascun dispositivo di archivio NVMe. Quando l'istanza viene arrestata o terminata, tutte le chiavi crittografiche vengono distrutte e non possono essere ripristinate. Non è possibile disattivare questa cifratura e non è possibile fornire una propria chiave crittografica.

Istanze Linux

Per accedere ai volumi NVMe, è necessario installare i driver NVMe. Le seguenti AMI soddisfano questo requisito:

- AL2023
- Amazon Linux 2
- AMI Amazon Linux 2018.03 e versioni successive
- Ubuntu 14.04 o versioni successive con kernel `linux-aws`

> **Note**
>
> AWS Graviton-based i tipi di istanza richiedono Ubuntu 18.04 o versioni successive con kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 o versioni successive
- SUSE Linux Enterprise Server 12 SP2 o versioni successive
- CentOS 7.4.1708 o versioni successive
- FreeBSD 11.1 o versioni successive
- Debian 9 o versioni successive GNU/Linux

- Bottlerocket

Dopo avere effettuato la connessione all'istanza, è possibile elencare i dispositivi NVMe utilizzando il comando lspci. Quello elencato di seguito è l'output di esempio di un'istanza `i3.8xlarge` che supporta quattro dispositivi NVMe.

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

Se si sta utilizzando un sistema operativo supportato, ma non compaiono i dispositivi NVME, verifica che il modulo NVMe sia caricato utilizzando il seguente comando.

- Amazon Linux, Amazon Linux 2, Ubuntu, Red Hat Enterprise Linux 14/16, SUSE Linux Enterprise Server, CentOS 7

  ```
  $ lsmod | grep nvme
  nvme           48813  0
  ```

- Ubuntu 18

  ```
  $ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
  s/nvme/host/nvme-core.ko
  kernel/drivers/nvme/host/nvme.ko
  kernel/drivers/nvmem/nvmem_core.ko
  ```

I volumi NVMe sono in linea con le specificazioni NVMe 1.0e. È possibile utilizzare i comandi NVMe con i volumi NVMe. Con Amazon Linux, è possibile installare il pacchetto `nvme-cli` dal repository utilizzando il comando yum install. Con altre versioni supportate di Linux, è possibile scaricare il pacchetto `nvme-cli`, se non è disponibile nell'immagine.

Istanze Windows

Le AMI AWS Windows più recenti per i seguenti sistemi operativi contengono i driver AWS NVMe utilizzati per interagire con i volumi di storage di istanze SSD esposti come dispositivi a blocchi NVMe per prestazioni migliori:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Ad avvenuta connessione all'istanza, è possibile verificare la visualizzazione dei volumi NVMe da Gestione Disco. Nella barra delle applicazioni, aprire il menu contestuale (pulsante destro del mouse) per il logo Windows e scegliere Disk Management (Gestione disco).

Le AMI AWS Windows fornite da Amazon includono il driver NVMe. AWS Se non utilizzi le AMI AWS Windows più recenti, puoi installare il driver NVMe corrente. AWS

Non-NVMe Volumi SSD

Le seguenti istanze supportano volumi di storage di istanze che utilizzano SSD non NVMe per offrire I/O prestazioni casuali elevate: C3, I2, M3, R3 e X1. Per ulteriori informazioni sui volumi di instance store supportati da ogni tipo di istanza, consulta Limiti di volume di archivio dell'istanza per le istanze EC2.

SSD-based prestazioni del volume dell'archivio di istanze I/O

Man mano che si riempiono i volumi dell'archivio di SSD-based istanze per l'istanza, il numero di IOPS in scrittura che è possibile ottenere diminuisce. Questa riduzione è dovuta al lavoro aggiuntivo che il controller SSD deve svolgere per individuare spazio disponibile, riscrivere i dati esistenti e cancellare lo spazio inutilizzato in modo che possa essere riscritto. Questo processo di garbage collection produce un'amplificazione della scrittura interna dell'SSD, espressa come il rapporto delle operazioni di scrittura dell'SSD e le operazioni di scrittura dell'utente. La riduzione delle prestazioni è ancora maggiore se le operazioni di scrittura non sono in multipli di 4.096 byte o non sono allineate con il limite di 4.096 byte. Se scrivi una quantità inferiore di byte o di byte non allineati, il controller SSD deve leggere i dati circostanti e archiviare il risultato in una nuova posizione. Questo schema

comporta un aumento significativo dell'amplificazione di scrittura, una maggiore latenza e una drastica riduzione delle prestazioni. I/O

I controller SSD possono utilizzare svariate strategie per ridurre l'impatto dell'amplificazione della scrittura. Una di queste strategie è di riservare spazio nell'archiviazione dell'istanza SSD in modo che il controller possa gestire più efficacemente lo spazio disponibile per le operazioni di scrittura. Si tratta dell'over-provisioning. I volumi dell' SSD-based Instance Store forniti a un'istanza non dispongono di spazio riservato per l'overprovisioning. Per ridurre l'amplificazione della scrittura, consigliamo di lasciare il 10% del volume non partizionato in modo che il controller SSD possa utilizzarlo per l'eccesso di provisioning. In questo modo, l'archiviazione che si può utilizzare diminuisce, ma aumentano le prestazioni anche se il disco è prossimo alla capacità completa.

Per i volumi dell'archivio dell'istanza che supportano TRIM, è possibile usare il comando TRIM per notificare al controller SSD che i dati scritti non sono più necessari. Il controller avrà così più spazio libero, l'amplificazione della scrittura potrà ridursi e le prestazioni aumentare. Per ulteriori informazioni, consulta Supporto TRIM per i volumi di instance store.

Supporto TRIM per i volumi di instance store

Alcuni tipi di istanza supportano i volumi SSD con TRIM. Per ulteriori informazioni, consulta Limiti di volume di archivio dell'istanza per le istanze EC2.

> **Note**
>
> (Solo istanze Windows) Le istanze che eseguono Windows Server 2012 R2 supportano TRIM a partire dalla versione 7.3.0 di AWS PV Driver. Le istanze che eseguono versioni precedenti di Windows Server non supportano il TRIM.

Volumi di instance store che supportano TRIM vengono tagliati prima di essere allocati per l'istanza. Questi volumi non sono formattati con un file system in cui un'istanza viene avviata; pertanto è necessario formattarli prima che essi possano essere montati e utilizzati. Per accedere più rapidamente a questi volumi. è consigliabile saltare l'operazione TRIM al momento della formattazione.

Per disabilitare temporaneamente il supporto TRIM durante la formattazione iniziale, utilizzare il comando `fsutil behavior set DisableDeleteNotify 1` (istanze Windows). Al termine della formattazione, riattivare il supporto TRIM utilizzando `fsutil behavior set DisableDeleteNotify 0`.

Con i volumi di instance store che supportano TRIM, è possibile usare il comando TRIM per notificare al controller SSD che i dati scritti non sono più necessari. Il controller avrà così più spazio libero, l'amplificazione della scrittura potrà ridursi e le prestazioni aumentare. Su istanze Linux, utilizza il comando `fstrim` per abilitare il TRIM periodico. Sulle istanze Windows, utilizzare il comando `fsutil behavior set DisableDeleteNotify 0` per assicurarsi che il supporto TRIM sia abilitato durante il normale funzionamento.

Aggiunta di volumi di archivio dell'istanza a un'istanza EC2

Per i tipi di istanze con volumi dell'archivio dell'istanza NVMe, tutti i volumi dell'archivio dell'istanza supportati vengono automaticamente collegati all'istanza all'avvio. Questi volumi vengono enumerati automaticamente e viene assegnato loro un nome di dispositivo all'avvio dell'istanza.

Per i tipi di istanze con volumi dell'archivio dell'istanza non NVMe, come C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 e X1e, devi specificare manualmente le mappature dei dispositivi a blocchi per i volumi dell'archivio dell'istanza che desideri collegare all'avvio. Le mappature dei dispositivi a blocchi possono essere specificate nella richiesta di avvio dell'istanza o nell'AMI utilizzata per avviare l'istanza. La mappatura dei dispositivi a blocchi comprende il nome del dispositivo e il volume sul quale si esegue la mappatura. Per ulteriori informazioni, consulta Mappature dei dispositivi a blocchi per i volumi sulle istanze Amazon EC2

> **Important**
>
> I volumi dell'archivio dell'istanza possono essere collegati a un'istanza solo al momento dell'avvio della stessa. Non è collegare un volume di instance store dopo averlo avviato.

Dopo aver avviato l'istanza, è necessario assicurarsi che i volumi instance store per l'istanza siano stati formattati e montati, prima di poterla utilizzare. Il volume root dell'archivio dell'istanza viene montato automaticamente.

Considerazione dei volumi root

Una mappatura dei dispositivi a blocchi specifica sempre il volume root per l'istanza. Il volume root viene sempre montato automaticamente.

Istanze Linux: il volume root è un volume Amazon EBS oppure un volume di archivio dell'istanza. Per le istanze con un volume di instance store per il volume root, la dimensione di questo volume varia a seconda dell'AMI, ma la dimensione massima è di 10 GB. Per ulteriori informazioni, consulta Tipo di volume root.

Istanze di Windows: il volume root deve essere un volume Amazon EBS. L'archivio dell'istanza non è supportato per il volume root.

Indice

- Aggiunta di volumi di archivio dell'istanza a un'AMI Amazon EC2
- Aggiunta di volumi dell'archivio dell'istanza a un'istanza EC2 durante l'avvio
- Rendere i volumi dell'archivio dell'istanza disponibili per l'utilizzo su un'istanza EC2

Aggiunta di volumi di archivio dell'istanza a un'AMI Amazon EC2

È possibile creare un'AMI con una mappatura dei dispositivi a blocchi che include volumi di instance store.

Se avvii un'istanza con un tipo di istanza che supporta i volumi dell'archivio dell'istanza non NVMe utilizzando un'AMI che specifica questi ultimi nelle proprie mappature dei dispositivi a blocchi, l'istanza include tali volumi dell'archivio dell'istanza. Se il numero di mappature dei dispositivi a blocchi del volume dell'archivio dell'istanza nell'AMI supera il numero disponibile di volumi dell'archivio dell'istanza per un'istanza, le mappature aggiuntive vengono ignorate.

Se avvii un'istanza che supporta i volumi dell'archivio dell'istanza NVMe utilizzando un'AMI che specifica le mappature dei dispositivi a blocchi del volume dell'archivio dell'istanza, tali mappature vengono ignorate. Le istanze che supportano i volumi dell'archivio dell'istanza NVMe ottengono tutti i volumi dell'archivio dell'istanza supportati, indipendentemente dalle mappature dei dispositivi a blocchi specificate nella richiesta di avvio dell'istanza e nell'AMI. La mappatura del dispositivo per questi volumi dipende dall'ordine secondo cui il sistema operativo enumera i volumi.

Considerazioni

- Il numero di volumi di instance store disponibili dipende dal tipo di istanza. Per ulteriori informazioni, consulta the section called "Volumi di archivio dell'istanza disponibili".
- Devi specificare un nome di dispositivo per ogni dispositivo a blocchi. Per ulteriori informazioni, consulta Nomi dei dispositivi per i volumi sulle EC2 istanze Amazon.
- All'avvio di un'istanza è possibile omettere i volumi instance store non-NVMe specificati nella mappatura dei dispositivi a blocchi AMI e i volumi instance store.
- Per le istanze M3, specificare i volumi di archivio istanze nella mappatura dei dispositivi a blocchi dell'istanza, non nell'AMI. Amazon EC2 può ignorare le mappature dei dispositivi a blocchi del volume dell'archivio dell'istanza nell'AMI.

Console

Per aggiungere volumi di storage di istanze a un'AMI Amazon EBS-backed

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza.
3. Scegliere Actions (Operazioni), Image and templates (Immagine e modelli), Create image (Crea immagine).
4. Nella pagina Create image (Crea immagine), immettere un nome e una descrizione significativi per l'immagine.
5. Per ogni volume di instance store da aggiungere, selezionare Add volume (Aggiungi nuovo volume), selezionare un volume di instance store in Volume type (Tipo di volume) e selezionare il nome del dispositivo in Device (Dispositivo).
6. Scegliere Create Image (Crea immagine).

AWS CLI

Per aggiungere volumi di archivio dell'istanza a un'AMI

Utilizza il comando create-image con l'`--block-device-mappings`opzione per specificare una mappatura dei dispositivi a blocchi per un'AMI. EBS-backed Usa il comando register-image con l'`--block-device-mappings`opzione per specificare una mappatura dei dispositivi a blocchi per un'AMI iAmazon. S3-backed

```
--block-device-mappings file://mapping.json
```

La mappatura dei dispositivi a blocchi seguente aggiunge due volumi di archivio dell'istanza.

```
[
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral0"
    },
    {
        "DeviceName": "/dev/sdd",
        "VirtualName": "ephemeral1"
    }
]
```

PowerShell

Per aggiungere volumi di archivio dell'istanza a un'AMI

Utilizza il New-EC2Image cmdlet con il `-BlockDeviceMapping` parametro per specificare una mappatura dei dispositivi a blocchi per un'AMI. EBS-backed Utilizza il Register-EC2Image cmdlet con il `-BlockDeviceMapping` parametro per specificare una mappatura dei dispositivi a blocchi per un'AMI Amazon. S3-backed

```
-BlockDeviceMapping $bdm
```

La mappatura dei dispositivi a blocchi seguente aggiunge due volumi di archivio dell'istanza.

```
$bdm = @()

$sdc = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdc.DeviceName = "/dev/sdc"
$sdc.VirtualName = "ephemeral0"
$bdm += $sdc

$sdd = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdd.DeviceName = "/dev/sdd"
$sdd.VirtualName = "ephemeral1"
$bdm += $sdd
```

Aggiunta di volumi dell'archivio dell'istanza a un'istanza EC2 durante l'avvio

Quando si avvia un tipo di istanza con volumi dell'archivio dell'istanza non NVMe, come C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 e X1e, devi specificare manualmente le mappature dei dispositivi a blocchi per i volumi dell'archivio dell'istanza che desideri collegare all'avvio. Le mappature dei dispositivi a blocchi devono essere specificate nella richiesta di avvio dell'istanza o nell'AMI utilizzata per avviare l'istanza.

Se l'AMI include mappature dei dispositivi a blocchi per i volumi dell'archivio dell'istanza, non devi specificare le mappature dei dispositivi a blocchi nella richiesta di avvio dell'istanza, a meno che non siano necessari più volumi dell'archivio dell'istanza rispetto a quelli inclusi nell'AMI.

Se l'AMI non include le mappature dei dispositivi a blocchi per i volumi dell'archivio dell'istanza, devi specificare le mappature dei dispositivi a blocchi nella richiesta di avvio dell'istanza.

Per i tipi di istanze con volumi dell'archivio dell'istanza NVMe, tutti i volumi dell'archivio dell'istanza supportati vengono automaticamente collegati all'istanza all'avvio.

Considerazioni

- Il numero di volumi di instance store disponibili dipende dal tipo di istanza. Per ulteriori informazioni, consulta the section called "Volumi di archivio dell'istanza disponibili".
- Devi specificare un nome di dispositivo per ogni dispositivo a blocchi. Per ulteriori informazioni, consulta Nomi dei dispositivi per i volumi sulle EC2 istanze Amazon.
- Per le istanze M3, potresti ricevere i volumi di instance store nella mappatura dei dispositivi a blocchi dell'istanza, anche se non li si specifica.

Console

Per specificare una mappatura dei dispositivi a blocchi in una richiesta di avvio dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal pannello di controllo, selezionare Avvia istanza.
3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona l'AMI da utilizzare.
4. Nella sezione Configura storage, il campo Volumi Instance store elenca i volumi dell'archivio dell'istanza che possono essere collegati all'istanza.
5. Per ogni volume dell'archivio dell'istanza da allegare, in Nome dispositivo, seleziona il nome del dispositivo da utilizzare.
6. Configura le impostazioni dell'istanza rimanenti in base alle esigenze, quindi scegli Avvia istanza.

AWS CLI

Per specificare una mappatura dei dispositivi a blocchi in una richiesta di avvio dell'istanza

Utilizzare il comando run-instances con l'opzione `--block-device-mappings`.

```
--block-device-mappings file://mapping.json
```

La mappatura dei dispositivi a blocchi seguente aggiunge due volumi di archivio dell'istanza.

```
[
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral0"
    },
    {
        "DeviceName": "/dev/sdd",
        "VirtualName": "ephemeral1"
    }
]
```

PowerShell

Per specificare una mappatura dei dispositivi a blocchi in una richiesta di avvio dell'istanza

Usa il New-EC2Instance cmdlet con l'opzione. `-BlockDeviceMapping`

```
-BlockDeviceMapping $bdm
```

La mappatura dei dispositivi a blocchi seguente aggiunge due volumi di archivio dell'istanza.

```
$bdm = @()

$sdc = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdc.DeviceName = "/dev/sdc"
$sdc.VirtualName = "ephemeral0"
$bdm += $sdc

$sdd = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdd.DeviceName = "/dev/sdd"
$sdd.VirtualName = "ephemeral1"
$bdm += $sdd
```

Rendere i volumi dell'archivio dell'istanza disponibili per l'utilizzo su un'istanza EC2

Dopo aver avviato un'istanza con volumi di instance store collegati, è necessario montare i volumi prima di potervi accedere.

Istanze Linux

È possibile formattare i volumi con il file system scelto dopo aver effettuato l'avvio dell'istanza.

Rendere un volume archivio istanza disponibile per Linux

1. Connettiti all'istanza tramite un client SSH. Per ulteriori informazioni, consulta Connessione a un'istanza Linux tramite SSH.
2. Utilizza il comando `df -h` per visualizzare i volumi formattati e montati.

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        3.8G   72K  3.8G   1% /dev
tmpfs           3.8G     0  3.8G   0% /dev/shm
/dev/nvme0n1p1  7.9G  1.2G  6.6G  15% /
```

3. Utilizza `lsblk` per visualizzare tutti i volumi che sono stati mappati al lancio, ma che non sono stati formattati e montati.

```
$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme0n1       259:1    0    8G  0 disk
##nvme0n1p1   259:2    0    8G  0 part /
##nvme0n1p128 259:3    0    1M  0 part
nvme1n1       259:0    0 69.9G  0 disk
```

4. Per formattare e montare un volume instance store che è stato solamente mappato, segui il procedimento elencato di seguito:

   a. Crea un file di sistema sul dispositivo utilizzando il comando `mkfs`.

   ```
   $ sudo mkfs -t xfs /dev/nvme1n1
   ```

   b. Crea una directory all'interno della quale montare il dispositivo utilizzando il comando `mkdir`.

   ```
   $ sudo mkdir /data
   ```

   c. Monta il dispositivo nella directory appena creata utilizzando il comando `mount`.

   ```
   $ sudo mount /dev/nvme1n1 /data
   ```

Istanze Windows

Per le istanze Windows, riformattiamo i volumi di instance store con il file di sistema NTFS.

È possibile visualizzare i volumi di archivio dell'istanza tramite Gestione disco di Windows. Per ulteriori informazioni, consulta Elenco dei dischi non NVMe.

Per montare manualmente un volume di instance store

1. Scegliere Inizia, immettere Gestione computer, quindi premere Invio.
2. Nel pannello a sinistra, scegliere Gestione disco.
3. Se viene richiesto di inizializzare il volume, scegliere il volume da inizializzare, selezionare il tipo di partizione richiesta in base al caso d'uso, quindi scegliere OK.
4. Nell'elenco dei volumi, apri il menu contestuale (clic con il pulsante destro del mouse) relativo al volume da montare, quindi scegli Nuovo volume semplice.
5. Nella procedura guidata scegliere Avanti.
6. Nella schermata Specifica dimensioni volume scegliere Avanti per utilizzare la dimensione massima del volume. In alternativa, scegliere una dimensione del volume compresa tra lo spazio minimo e quello massimo su disco.
7. Nella schermata Assegna lettera di unità o percorso eseguire una delle operazioni seguenti e scegliere Avanti.
   - Per montare il volume con una lettera di unità, scegliere Assegna la lettera di unità seguente quindi scegliere la lettera di unità da utilizzare.
   - Per montare il volume come cartella, scegliere Monta nella seguente cartella NTFS vuota e quindi scegliere Sfoglia per creare o selezionare la cartella da utilizzare.
   - Per montare il volume senza una lettera o un percorso di unità, scegliere Non assegnare una lettera di unità o un percorso di unità.
8. Nella schermata Formato partizione, specifica se formattare il volume. Se si sceglie di formattare il volume, scegliere il file system e le dimensioni dell'unità richieste e specificare un'etichetta del volume.
9. Scegliere Avanti, Fine.

Abilita il volume di swap dell'archivio dell'istanza per le istanze EC2 M1 e C1

> **Note**
>
> Questo argomento si applica solo alle istanze Linux `c1.medium` e `m1.small`.

I tipi di istanze `c1.medium` e `m1.small` hanno una quantità limitata di memoria fisica. Pertanto, all'avvio viene loro assegnato un volume di swap da 900 MiB che funge da memoria virtuale o spazio di swap per il sistema Linux. È possibile utilizzare lo spazio di swapping su Linux quando un sistema richiede più memoria di quanta ne è stata allocata fisicamente. Quando lo spazio di swapping è abilitato, i sistemi possono scambiare le pagine di memoria utilizzate meno frequentemente dalla memoria fisica allo spazio di swapping (che sia una partizione dedicata o file di cambio all'interno di un file system esistente) e liberare lo spazio necessario alle pagine di memoria che richiedono un accesso ad alta velocità.

> **Note**
>
> - L'utilizzo dello spazio di scambio il pagine di memoria non è veloce o efficiente come quello della RAM. Se il carico di lavoro sta effettuando regolarmente il paging della memoria nello spazio di scambio, è consigliabile pensare di migrare a un tipo di istanza di dimensioni maggiori e con più RAM. Per ulteriori informazioni, consulta Modifiche del tipo di istanza Amazon EC2.
> - Sebbene il kernel di Linux veda questo spazio di swap come una partizione sul volume root, in realtà è un volume di archivio dell'istanza separato, indipendentemente dal tipo di volume root.

Amazon Linux abilita e utilizza automaticamente questo spazio di swap, ma la tua AMI potrebbe richiedere qualche passaggio ulteriore per il riconoscimento e l'utilizzo di questo spazio di swap. Per vedere se l'istanza sta utilizzando dello spazio di scambio, è possibile utilizzare il comando swapon -s.

```
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
```

```
/dev/xvda3                              partition       917500  0       -1
```

L'istanza sopra elencata dispone di un volume di scambio di 900 MiB allegato e abilitato. Se non si visualizza un volume di scambio elencato con questo comando, potrebbe essere necessaria l'abilitazione dello spazio di scambio per il dispositivo. Controllare i dischi disponibili utilizzando il comando lsblk.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk
```

In questo caso, il volume di swap `xvda3` è disponibile per l'istanza, ma non è abilitato (notare che il campo `MOUNTPOINT` è vuoto). È possibile abilitare il volume di swap con il comando swapon.

> **Note**
>
> È necessario inserire come prefisso `/dev/` al nome del dispositivo elencato da lsblk. Il dispositivo può avere un nome diverso, come `sda3`, `sde3`, oppure `xvde3`. Utilizza il nome del dispositivo per il sistema nel comando di seguito.

```
[ec2-user ~]$ sudo swapon /dev/xvda3
```

Adesso lo spazio di scambio dovrebbe comparire nell'output lsblk e swapon -s.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk [SWAP]
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

È inoltre necessario modificare i file `/etc/fstab` perché questo spazio di swapping sia abilitato automaticamente ad ogni avvio del sistema.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Aggiungere la seguente linea al file `/etc/fstab` (utilizzando il nome del dispositivo di scambio per il sistema):

```
/dev/xvda3       none    swap    sw  0       0
```

Utilizzare un volume di instance store a uno spazio di swap

È possibile utilizzare un qualsiasi volume di instance store come spazio di swapping. Ad esempio il tipo di istanza `m3.medium` include un volume di instance store volume SSD di 4GB adatto allo spazio di swapping. Se il volume di instance store dovesse essere di dimensioni maggiori (ad esempio 350 GB), potrebbe essere necessaria la partizione del volume in partizioni di swap più piccole di 4-8GB e il resto assegnarlo a un volume di dati.

> **Note**
>
> Questa procedura si applica solamente a tipo di istanze che supportano l'archiviazione di istanze. Per una lista di tipi di istanze supportate, consulta Limiti di volume di archivio dell'istanza per le istanze EC2.

1. Vengono elencati i dispositivi a blocchi collegati all'istanza per ottenere il nome del dispositivo per il volume di instance store.

   ```
   [ec2-user ~]$ lsblk -p
   NAME       MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
   /dev/xvdb  202:16   0   4G  0 disk /media/ephemeral0
   /dev/xvda1 202:1    0   8G  0 disk /
   ```

   In questo esempio, il volume di instance store è `/dev/xvdb`. Poiché si tratta di un'istanza Amazon Linux il volume di instance store viene formattato e montato su `/media/ephemeral0`; questa operazione non viene eseguita automaticamente su tutti i sistemi operativi Linux.
2. (Facoltativo) se il volume di instance store è stato montato (presenta `MOUNTPOINT` nell'output di comando lsblk), smontarlo utilizzando il seguente comando.

   ```
   [ec2-user ~]$ sudo umount /dev/xvdb
   ```
3. Impostare un'area di swapping Linux sul dispositivo con il comando mkswap.

   ```
   [ec2-user ~]$ sudo mkswap /dev/xvdb
   ```

```
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swapspace version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. Abilita la quantità di spazio di swapping.

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. Verifica che il nuovo spazio di swapping sia utilizzato.

```
[ec2-user ~]$ swapon -s
Filename    Type  Size Used Priority
/dev/xvdb                               partition 4188668 0 -1
```

6. Modifica i file `/etc/fstab` così che questo spazio di swapping venga automaticamente abilitato ad ogni avvio di sistema.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Se il file `/etc/fstab` dovesse avere una voce per `/dev/xvdb` (o per `/dev/sdb`) cambiala per farla corrispondere a quella riportata nella riga seguente: se non dovesse avere alcuna voce per questo dispositivo, aggiungi la riga seguente al file `/etc/fstab` (utilizzando il nome del dispositivo di swap per il sistema):

```
/dev/xvdb       none    swap    sw  0       0
```

> **Important**
>
> I dati del volume di instance store vengono persi all'interruzione o all'ibernazione di un'istanza; inclusa la formattazione dello spazio di swapping creata su Step 3. Se si arresta e riavvia un'istanza che è stata configurata per l'utilizzo di uno spazio di swapping di un instance store, è necessario ripetere Step 1 da Step 5 sul nuovo volume di instance store.

Inizializza i volumi dell'archivio dell'istanza sulle istanze EC2

A causa della modalità di visualizzazione dei dischi virtuali di Amazon EC2, la prima scrittura di una qualsiasi destinazione su alcuni volumi di instance store viene eseguita più lentamente delle scritture

successive. Per la maggior parte delle applicazioni, è accettabile ammortizzare questo costo nel ciclo di vita dell'istanza. Tuttavia, se fosse necessaria una prestazione elevata del disco, è consigliabile inizializzare i drive scrivendo una volta sulla posizione di ogni disco prima di utilizzarlo in produzione.

> **Note**
>
> Le tipologie di istanze con supporti Solid State Drive (SSD) e TRIM forniscono le massime prestazioni all'avvio, senza l'inizializzazione. Per ulteriori informazioni sui volumi di instance store per ogni tipo di istanza, consulta Limiti di volume di archivio dell'istanza per le istanze EC2.

Se è necessaria maggiore flessibilità nella latenza o nel throughput. è consigliabile utilizzare Amazon EBS.

Per inizializzare i volumi di instance store, utilizza il seguenti comandi dd a seconda dello store da inizializzare (ad esempio, `/dev/sdb` o `/dev/nvme1n1`).

> **Note**
>
> Assicurati di aver smontato il drive prima di eseguire questo comando.
> L'inizializzazione potrebbe richiedere tempi lunghi (circa 8 ore per un'istanza extra large).

Per inizializzare i volumi di instance store, utilizza i seguenti comandi nei tipi di istanze `m1.large`, `m1.xlarge`, `c1.xlarge`, `m2.xlarge`, `m2.2xlarge` e `m2.4xlarge`:

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M
dd if=/dev/zero of=/dev/sde bs=1M
```

Per eseguire l'inizializzazione su tutti i volumi di instance store contemporaneamente,, utilizza i seguenti comandi:

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

La configurazione dei drive per RAID li inizializza scrivendo su ogni posizione del disco. Durante la configurazione di un software basato sul RAID, assicurati di modificare la velocità minima di ricostruzione:

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

Statistiche dettagliate delle prestazioni per i volumi di archivio dell'istanza Amazon EC2

Amazon EC2 fornisce statistiche sulle prestazioni in tempo reale e ad alta risoluzione per i volumi di storage di istanze NVMe collegati alle istanze Amazon EC2. Nitro-based Queste statistiche sono presentate come contatori aggregati che vengono mantenuti per tutta la durata dell'istanza. Le statistiche forniscono dettagli sul numero cumulativo di operazioni, sui byte inviati e ricevuti, sul tempo impiegato per le operazioni di lettura e scrittura e sugli istogrammi per I/O le operazioni di lettura e scrittura. I/O Queste statistiche mantengono la coerenza con le statistiche dettagliate sulle prestazioni di Amazon EBS, ma includono anche istogrammi di latenza dettagliati suddivisi per I/O dimensione, che possono fornire informazioni più granulari sui modelli di prestazioni dello storage. Questa visibilità migliorata consente di identificare con precisione le I/O dimensioni specifiche che presentano problemi di latenza, consentendo di ottimizzare le prestazioni delle applicazioni e risolvere i problemi in modo più efficace.

È possibile raccogliere queste statistiche con una granularità, fino a intervalli di 1 secondo. Se le richieste vengono effettuate con una frequenza superiore a intervalli di 1 secondo, il driver NVMe potrebbe metterle in coda, insieme ad altri comandi di amministrazione, per essere elaborate in un secondo momento.

Considerazioni

- Le statistiche sono supportate solo per i volumi di storage di istanze NVMe collegati alle istanze. Nitro-based
- I contatori non sono persistenti tra le interruzioni e i riavvii dell'istanza.
- Le statistiche sono disponibili senza costi aggiuntivi.

Statistiche

Il dispositivo a blocchi NVMe fornisce le seguenti statistiche:

Nome della statistica	Nome completo	Tipo	Description
total_rea d_ops	Operazioni di lettura totali	Contatore	Il numero totale di operazioni di lettura.
total_wri te_ops	Operazioni di scrittura totali	Contatore	Il numero totale di operazioni di scrittura.
total_rea d_bytes	Bytes letti totali	Contatore	Il numero totale di byte letti trasferiti.
total_wri te_bytes	Byte scritti totale	Contatore	Il numero totale di byte scritti trasferiti.
total_rea d_time	Tempo di lettura totale	Contatore	Il tempo totale impiegato, in microsecondi, da tutte le operazioni di lettura completate.
total_wri te_time	Tempo di scrittura totale	Contatore	Il tempo totale impiegato, in microsecondi, da tutte le operazioni di scrittura completate.
instance_ store_vol ume_perfo rmance_ex ceeded_io ps	Il tempo totale richiesto ha superato il numero massimo di IOPS del volume	Contatore	Il tempo totale, in microsecondi, durante il quale le richieste di IOPS hanno il volume massimo di IOPS. Qualsiasi valore superiore a 0 indica che il carico di lavoro ha richiesto un numero di IOPS superiore a quello che il volume era in grado di fornire. Idealmente, il conteggio incrementale di questa metrica, tra due tempi di snapshot, dovrebbe essere minimo.
instance_ store_vol ume_perfo rmance_ex ceeded_tp	Il tempo totale richiesto ha superato il numero massimo di throughput del volume	Contatore	Il tempo totale, in microsecondi, durante il quale la richiesta di throughput ha superato il volume massimo di throughput. Qualsiasi valore superiore a 0 indica che il carico di lavoro ha richiesto un numero di throughput superiore a quello che il volume era in grado di fornire. Idealmente, il conteggio incrementale

Nome della statistica	Nome completo	Tipo	Description
			di questa metrica, tra due tempi di snapshot, dovrebbe essere minimo.
volume_queue_length	Lunghezza della coda del volume	Point in time	Il numero di operazioni di lettura e scrittura in attesa di completamento.
read_io_latency_histogram	I/O Leggi l'istogramma	Istogramma *	Il numero di operazioni di lettura completate all'interno di ogni contenitore di latenza, in microsecondi.
write_io_latency_histogram	Scrivi I/O l'istogramma	Istogramma *	Il numero di operazioni di scrittura completate all'interno di ogni contenitore di latenza, in microsecondi.

> **Note**
>
> * Le statistiche dell'istogramma rappresentano solo I/O le operazioni completate con successo. Le I/O operazioni bloccate o compromesse non sono incluse, ma saranno evidenti nelle `volume_queue_length` statistiche, presentate come statistiche puntuali.

Accesso alle statistiche

È necessario accedere alle statistiche direttamente dall'istanza a cui sono collegati i volumi di archivio dell'istanza. Puoi alle statistiche utilizzando uno dei metodi seguenti.

Istanze Linux

Amazon CloudWatch

Puoi configurare l' CloudWatch agente Amazon per raccogliere le statistiche dalla tua istanza e renderle disponibili come metriche personalizzate in. CloudWatch Puoi quindi utilizzare le metriche CloudWatch per analizzare i I/O modelli, tenere traccia delle tendenze delle prestazioni, creare dashboard personalizzate e impostare allarmi automatici in base alle soglie di prestazioni.

Per ulteriori informazioni sulla configurazione CloudWatch dell'agente, consulta Collect Amazon EC2 instance store metrics.

nvme-cli tool

Per accedere alle statistiche

1. Connetti all'istanza a cui è collegato il volume.
2. Le AMI Amazon Linux 2023 rilasciate dopo il 15 settembre 2025 includono l'ultima versione dello strumento `nvme-cli`. Se utilizzi una vecchia AMI Amazon Linux, aggiorna lo strumento `nvme-cli`.

```
sudo yum install nvme-cli
```

3. Esegui il comando seguente e specifica il nome dispositivo per il volume.

```
sudo nvme amzn stats /dev/nvme0n1
```

Le statistiche forniscono anche istogrammi di latenza dettagliati suddivisi per dimensione. I/O Per visualizzare le statistiche suddivise per I/O dimensione, includi l'opzione. `--details` Ad esempio:

```
sudo nvme amzn stats --details /dev/nvme0n1
```

È possibile ottenere ulteriori informazioni su come utilizzare lo strumento specificando l'opzione `--help`. Ad esempio:

```
sudo nvme amzn stats --help
```

Istanze Windows

nvme_amzn.exe tool

Per accedere alle statistiche

1. Connetti all'istanza a cui è collegato il volume.
2. Assicurati di utilizzare la versione `1.7.0` o successiva del driver AWSNVMe. Per ulteriori informazioni sull'aggiornamento del driver AWSNVMe, consultare AWS Driver NVMe.

3. Ottieni il numero del disco per il volume. Per ulteriori informazioni, consultare Map NVMe disks on Amazon EC2 Windows instance to volumes.
4. Esegui il comando seguente come amministratore e specifica il numero del disco per il volume.

```
.\nvme_amzn.exe stats disk_number
```

Le statistiche forniscono anche istogrammi di latenza dettagliati suddivisi per dimensione. I/O Per visualizzare le statistiche suddivise per I/O dimensione, includi l'opzione. `--details` Ad esempio:

```
.\nvme_amzn.exe stats --details disk_number
```

Volumi root per le tue istanze Amazon EC2

Quando avvii un'istanza, viene creato un volume root per l'istanza. Il volume root contiene l'immagine utilizzata per avviare l'istanza. Ogni istanza ha un singolo volume root. Puoi aggiungere volumi di archiviazione alle istanze durante o dopo l'avvio.

L'AMI utilizzata per avviare l'istanza determina il tipo di volume root. Puoi avviare un'istanza da un' EBS-backed AMI Amazon (istanze Linux e Windows) o da un'Amazon S3-backed AMI (solo istanze Linux). Esistono differenze significative in merito a cosa è possibile fare con ciascun tipo di AMI. Per ulteriori informazioni su queste differenze, consulta Tipo di volume root.

Consigliamo di utilizzare le AMI supportate da Amazon EBS perché queste istanze sono caratterizzate da un avvio più veloce e utilizzano un'archiviazione persistente.

Riserviamo nomi di dispositivi specifici per i volumi root. Per ulteriori informazioni, consulta Nomi dei dispositivi per i volumi sulle EC2 istanze Amazon.

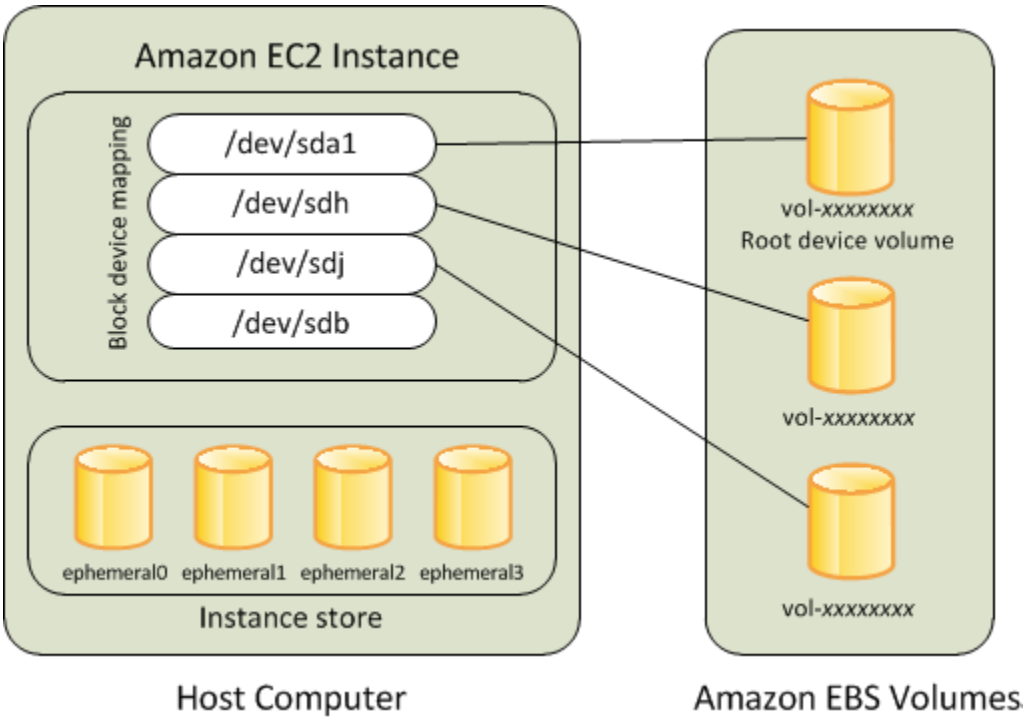
Indice

- Istanze con volume root Amazon EBS
- Istanze con un volume root di archivio dell'istanza (solo istanze Linux)
- Conservazione di un volume root Amazon EBS dopo aver terminato un'istanza Amazon EC2
- Sostituzione di un volume root per un'istanza Amazon EC2 senza interromperlo

Istanze con volume root Amazon EBS

Alle istanze che utilizzano Amazon EBS per il volume root viene collegato automaticamente un volume Amazon EBS. Quando avvii un'istanza con Amazon EBS-AMI, creiamo un volume Amazon EBS per ogni snapshot Amazon EBS a cui fa riferimento l'AMI. Puoi facoltativamente utilizzare altri volumi Amazon EBS o volumi instance store, a seconda del tipo di istanza.

Un'istanza con volume root EBS può essere arrestata e riavviata in un secondo momento senza alcuna ripercussione sui dati archiviati nei volumi collegati. Puoi eseguire varie attività relative alle istanze e ai volumi quando un'istanza con volume root EBS si trova in uno stato arrestato. Ad esempio, puoi modificare le proprietà dell'istanza, modificarne le dimensioni o aggiornare il kernel utilizzato oppure puoi collegare il volume root a una diversa istanza in esecuzione a scopo di debug o altro. Per ulteriori informazioni consulta Amazon EBS volumes.



Limitazione

Non è possibile utilizzare i volumi EBS `st1` o `sc1` come volumi root.

Errore di un'istanza

Se si verifica un errore su un'istanza con volume root EBS, puoi ripristinare la sessione seguendo uno di questi metodi:

- Arrestare e quindi riavviare di nuovo (provare questo metodo come primo tentativo di soluzione).

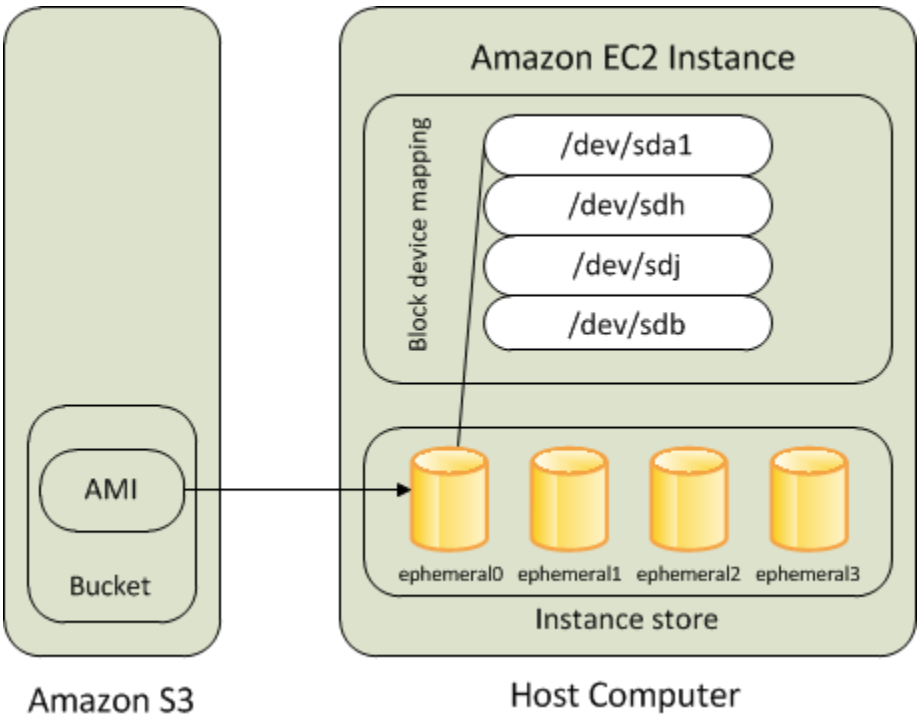
- Creare automaticamente snapshot di tutti i volumi rilevanti e creare una nuova AMI. Per ulteriori informazioni, consulta Crea un' EBS-backed AMI Amazon.
- Collegare il volume a una nuova istanza effettuando la seguente procedura:
  1. Creare una snapshot del volume root.
  2. Registrare una nuova AMI utilizzando lo snapshot.
  3. Avviare una nuova istanza dalla nuova AMI.
  4. Scollegare i restanti volumi Amazon EBS dalla vecchia istanza.
  5. Ricollegare i volumi Amazon EBS alla nuova istanza.

Istanze con un volume root di archivio dell'istanza (solo istanze Linux)

> **Note**
>
> Le istanze Windows non supportano i volumi root di archivio dell'istanza.

Le istanze che utilizzano un archivio dell'istanza come volume root dispongono automaticamente di uno o più volumi di archivio dell'istanza disponibili, dove un volume funge da volume root. Quando un'istanza viene avviata da un' S3-backed AMI Amazon, l'AMI viene copiata nel volume principale. Puoi facoltativamente utilizzare volumi instance store aggiuntivi, a seconda del tipo di istanza.

I dati presenti nei volumi di archivio dell'istanza sono persistenti finché l'istanza è in esecuzione, ma vengono eliminati quando l'istanza viene terminata (le istanze con un volume root di archivio dell'istanza non supportano l'operazione Arresta) o se l'avvio dell'istanza ha esito negativo (ad esempio se si verifica un problema in un'unità sottostante). Per ulteriori informazioni, consulta Archivio dell'istanza archiviazione a blocchi temporanea per le istanze EC2.



Tipi di istanze supportati

Solo i seguenti tipi di istanza supportano un volume dell'archivio dell'istanza come volume root: C1, C3, D2, I2, M1, M2, M3, R3 e X1.

Errore di un'istanza

Quando un'istanza con un volume root di archivio dell'istanza non riesce o viene terminata, non può essere ripristinata. Se prevedi di utilizzare istanze con un volume root di archivio dell'istanza, ti consigliamo vivamente di distribuire i dati su volumi di archivio dell'istanza in più zone di disponibilità. Consigliamo anche di eseguire regolarmente una copia di backup dei dati critici dai volumi dell'archivio istanza in modo da rendere persistente l'archiviazione.

Conservazione di un volume root Amazon EBS dopo aver terminato un'istanza Amazon EC2

Per impostazione predefinita, il volume root Amazon EBS per un'istanza viene eliminato quando quest'ultima viene terminata. Puoi modificare il comportamento predefinito per assicurarti che il volume root Amazon EBS persista dopo che l'istanza viene terminata. Per modificare il comportamento predefinito, imposta l'attributo `DeleteOnTermination` su `false`. Puoi farlo all'avvio dell'istanza o in un secondo momento.

Processi

- Configurare il volume root per la persistenza durante l'avvio dell'istanza
- Configurare il volume root in modo che persista per un'istanza esistente
- Confermare che un volume root è configurato per la persistenza

Configurare il volume root per la persistenza durante l'avvio dell'istanza

Puoi configurare il volume root in modo che persista quando avvii un'istanza.

Console

Per configurare il volume root affinché sia persistente quando avvii un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Instances (Istanze), quindi selezionare Launch Instance (Avvia istanza).
3. Scegliere una Amazon Machine Image (AMI), scegliere un tipo di istanza, scegliere una coppia di chiavi e configurare le impostazioni di rete.
4. Per Configura archiviazione, selezionare Avanzate.
5. Espandere il volume root.
6. In Elimina al termine, scegliere No.
7. Al termine della configurazione dell'istanza, scegliere Avvia istanza.

AWS CLI

Per configurare il volume root affinché sia persistente quando avvii un'istanza

Usa il comando run-instances e includi la seguente opzione.

```
--block-device-mappings file://mapping.json
```

In `mapping.json`, specifica una mappatura dei dispositivi a blocchi che imposti l'attributo `DeleteOnTermination` su `false`.

```
[
    {
        "DeviceName": "/dev/sda1",
```

```
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

PowerShell

Per configurare il volume root affinché sia persistente quando avvii un'istanza

Usa il New-EC2Instance cmdlet e includi il seguente parametro.

```
-BlockDeviceMapping $bdm
```

Crea una mappatura dei dispositivi a blocchi che imposti l'attributo `DeleteOnTermination` su `$false`.

```
$ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
$ebs.DeleteOnTermination = $false
$bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "dev/xvda"
$bdm.Ebs = $ebs
```

Configurare il volume root in modo che persista per un'istanza esistente

Puoi configurare il volume root in modo che persista per un'istanza in esecuzione. Tieni presente che non è possibile completare questa attività utilizzando la console Amazon EC2.

AWS CLI

Per configurare il volume root affinché sia persistente per un'istanza esistente

Utilizzare il comando modify-instance-attribute con una mappatura dei dispositivi a blocchi che imposta l'attributo `DeleteOnTermination` su `false`.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --block-device-mappings file://mapping.json
```

Specifica quanto segue nel file `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

PowerShell

Per configurare il volume root affinché sia persistente per un'istanza esistente

Utilizza il Edit-EC2InstanceAttribute cmdlet con una mappatura dei dispositivi a blocchi che imposta l'attributo su. `DeleteOnTermination` `$false`

```
$ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification
$ebs.DeleteOnTermination = $false
$bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification
$bdm.DeviceName = "/dev/xvda"
$bdm.Ebs = $ebs
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -BlockDeviceMapping $bdm
```

Confermare che un volume root è configurato per la persistenza

Puoi confermare che un volume root sia configurato per la persistenza.

Console

Per confermare che un volume root è configurato per la persistenza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e quindi selezionare l'istanza desiderata.
3. Nella scheda Storage (archiviazione) in Block devices (Dispositivi a blocchi), individuare la voce per il volume root. Se l'opzione Delete on termination (Elimina all'interruzione) è No, il volume è configurato per la persistenza.

AWS CLI

Per confermare che un volume root è configurato per la persistenza

Usa il comando describe-instances e verifica che l'attributo `DeleteOnTermination` sia impostato su `false`.

```
aws ec2 describe-instances \
    --instance-id i-1234567890abcdef0 \
    --query "Reservations[].Instances[].BlockDeviceMappings"
```

Di seguito è riportato un output di esempio.

```
[
    [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "AttachTime": "2024-07-12T04:05:33.000Z",
                "DeleteOnTermination": false,
                "Status": "attached",
                "VolumeId": "vol-1234567890abcdef0"

        }
    ]
]
```

PowerShell

Per confermare che un volume root è configurato per la persistenza

Utilizzare il Get-EC2Instance cmdlet e verificare che l'attributo sia impostato su. `DeleteOnTermination` `False`

```
(Get-EC2Instance -InstanceId i-
i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

Di seguito è riportato un output di esempio.

```
AssociatedResource  :
AttachTime          : 7/12/2024 4:05:33 AM
DeleteOnTermination : False
```

```
Operator            :
Status              : attached
VolumeId            : vol-1234567890abcdef0
```

Sostituzione di un volume root per un'istanza Amazon EC2 senza interromperlo

Amazon EC2 consente di sostituire il volume Amazon EBS root per un'istanza in esecuzione mantenendo i seguenti elementi:

- Dati archiviati nei volumi di archivio dell'istanza: i volumi di archivio dell'istanza restano collegati all'istanza dopo il ripristino del volume root.
- Dati archiviati su volumi di dati (non root) di Amazon EBS: i volumi Non-root Amazon EBS rimangono collegati all'istanza dopo il ripristino del volume root.
- Configurazione di rete — Tutte le interfacce di rete rimangono collegate all'istanza e conservano gli indirizzi IP, gli identificatori e gli ID allegati. Quando l'istanza diventa disponibile, tutto il traffico di rete in sospeso viene scaricato. Inoltre, l'istanza rimane sullo stesso host fisico, quindi conserva gli indirizzi IP pubblici e privati e il nome DNS.
- Policy IAM — IAM I profili e le policy (ad esempio, le policy basate su tag) associati all'istanza vengono mantenuti e applicati.

Indice

- Come funziona la sostituzione del volume root
- Considerazioni
- Sostituzione di un volume root

Come funziona la sostituzione del volume root

Quando sostituisci il volume root per un'istanza, viene creata un'attività di sostituzione del volume root. Il volume root originale viene scollegato dall'istanza e al suo posto viene collegato il nuovo volume. La mappatura dei dispositivi a blocchi dell'istanza viene aggiornata per riflettere l'ID del volume root sostitutivo.

Quando si sostituisce il volume principale per un'istanza, è necessario specificare l'origine del nuovo volume. Di seguito sono indicate le possibili opzioni.

Ripristino di un volume root allo stato originale

Questa opzione sostituisce il volume root corrente con un volume basato sullo snapshot utilizzato per crearlo.

Considerazioni sull'utilizzo dello stato di avvio

Il volume root sostitutivo ottiene gli stessi attributi di tipo, dimensione ed eliminazione alla terminazione del volume root originale.

Sostituzione del volume root utilizzando uno snapshot

Questa opzione sostituisce il volume root corrente con uno sostitutivo basato sullo snapshot specificato. Ad esempio, uno snapshot specifico creato in precedenza da questo volume root. Questa opzione è utile se devi risolvere problemi causati dal danneggiamento del volume root o da errori di configurazione di rete nel sistema operativo ospite.

Il volume root sostitutivo ottiene gli stessi attributi di tipo, dimensione ed eliminazione alla terminazione del volume root originale.

Considerazioni sull'utilizzo di uno snapshot

- Puoi utilizzare solamente snapshot creati direttamente dai volumi root attuali o precedenti dell'istanza.
- Non è possibile utilizzare copie snapshot create da snapshot acquisiti dal volume root.
- Dopo aver ripristinato correttamente il volume root, puoi utilizzare comunque gli snapshot acquisiti dal volume root originale per ripristinare il nuovo volume root (sostitutivo).

Sostituzione del volume root tramite un'AMI

Questa opzione sostituisce il volume root corrente utilizzando un AMI specificata. Questa funzionalità è utile se devi applicare patch o eseguire aggiornamenti del sistema operativo e delle applicazioni. Il codice di prodotto, le informazioni di fatturazione, il tipo di architettura e il tipo di virtualizzazione dell'AMI devono essere uguali a quelli dell'istanza.

Se l'istanza è abilitata per ENA o sriov-net, devi utilizzare un'AMI che supporti tali funzionalità. Se l'istanza non è abilitata per ENA o sriov-net, puoi selezionare un'AMI che non supporti tali funzionalità oppure puoi aggiungere automaticamente il supporto se selezioni un'AMI che le supporti.

Se l'istanza è abilitata per NitroTPM, devi utilizzare un'AMI con NitroTPM abilitato. Il supporto NitroTPM non è abilitato se l'istanza non è stata configurata per tale istanza, indipendentemente dall'AMI selezionata.

Puoi selezionare un'AMI con una modalità di avvio diversa da quella dell'istanza, purché l'istanza supporti la modalità di avvio dell'AMI. Se l'istanza non supporta la modalità di avvio, la richiesta non va a buon fine. Se l'istanza supporta la modalità di avvio, la nuova modalità di avvio viene propagata all'istanza e i relativi dati UEFI vengono aggiornati di conseguenza. Se hai modificato manualmente l'ordine di avvio o hai aggiunto una chiave UEFI Secure Boot privata per caricare i moduli privati del kernel, le modifiche vengono perse durante la sostituzione del volume root.

Il volume root sostitutivo ottiene gli stessi attributi di tipo, dimensione ed eliminazione alla terminazione del volume root originale. La dimensione del volume root sostitutivo è la maggiore tra la dimensione di mappatura del dispositivo a blocchi del volume principale AMI e la dimensione del volume root corrente.

Una volta completata l'attività di sostituzione del volume principale, le seguenti informazioni nuove e aggiornate si riflettono nella descrizione dell'istanza utilizzando la console AWS CLI o AWS gli SDK:

- Nuovo ID AMI
- Nuovo ID volume per il volume root
- Configurazione della modalità di avvio aggiornata (se modificata dall'AMI)
- Configurazione NitroTPM aggiornata (se abilitata dall'AMI)
- Configurazione ENA aggiornata (se abilitata dall'AMI)
- Configurazione sriov-net aggiornata (se abilitata dall'AMI)

Il nuovo ID AMI si riflette anche nei metadati dell'istanza.

Considerazioni sull'utilizzo di un'AMI:

- Se utilizzi un'AMI con più mappature dei dispositivi a blocchi, viene utilizzato solo il volume root dell'AMI. Gli altri volumi (non root) vengono ignorati.
- Puoi utilizzare questa funzionalità solo se disponi delle autorizzazioni per l'AMI e per la snapshot del volume root associato. Non è possibile utilizzare questa funzionalità con Marketplace AWS le AMI.
- Puoi utilizzare un'AMI senza un codice prodotto solo se l'istanza non dispone di un codice prodotto.

- La dimensione del volume root sostitutivo è la maggiore tra la dimensione di mappatura del dispositivo a blocchi del volume principale AMI e la dimensione corrente del volume root.
- I documenti di identità dell'istanza per l'istanza vengono aggiornati automaticamente.
- Se l'istanza supporta NitroTPM, i dati NitroTPM per l'istanza vengono ripristinati e vengono generate nuove chiavi.

Sostituisci il volume principale utilizzando un volume Amazon EBS esistente

A differenza delle opzioni snapshot e AMI, che creano un nuovo volume, questa opzione sostituisce il volume root corrente con un volume Amazon EBS esistente che hai già configurato. Ciò è utile per carichi di lavoro con stato, come i database, in cui desideri preparare metadati o software sul volume principale prima di collegarlo all'istanza.

Prima di utilizzare questa opzione, devi creare e preparare il volume Amazon EBS sostitutivo. Puoi prepararlo collegandolo a un'istanza come volume di dati, copiandovi i dati richiesti e quindi scollegandolo. Il volume deve trovarsi nella stessa zona di disponibilità dell'istanza.

Il volume principale sostitutivo mantiene le dimensioni, il tipo e gli altri attributi configurati al momento della creazione e della preparazione. L'attributo delete on termination del volume root originale non viene trasferito al volume root sostitutivo.

Considerazioni sull'utilizzo di un volume Amazon EBS esistente

- Il volume sostitutivo deve trovarsi nella stessa zona di disponibilità dell'istanza.
- Il volume sostitutivo non deve essere collegato a nessuna istanza al momento della richiesta.
- Il volume sostitutivo deve essere nello `available` stato.
- Se il volume sostitutivo non soddisfa questi requisiti, la richiesta di sostituzione del volume principale ha esito negativo.
- Puoi utilizzare questa opzione con Marketplace AWS le istanze, ma sia i codici prodotto del marketplace che i codici di fatturazione sul volume sostitutivo devono corrispondere a quelli sull'istanza.
- Se il volume principale originale è crittografato, anche il volume sostitutivo deve essere crittografato. È possibile passare da un volume non crittografato a uno crittografato, ma non da crittografato a non crittografato. Quando il volume sostitutivo è crittografato, il responsabile IAM deve disporre delle AWS KMS autorizzazioni necessarie per scollegare il volume originale. È inoltre necessario disporre delle autorizzazioni per allegare e decrittografare il volume sostitutivo. Queste sono le stesse autorizzazioni necessarie per collegare un volume crittografato.

Dopo il completamento del processo di sostituzione, puoi decidere se mantenere il volume root originale. Se decidi di eliminare il volume root originale dopo il completamento del processo di sostituzione, questo viene eliminato automaticamente e non può più essere recuperato. Se decidi di mantenere il volume root originale dopo il completamento del processo, il volume rimane nel tuo account e dovrai eliminarlo manualmente quando non ne avrai più bisogno.

L'attività di sostituzione del volume root passa attraverso i seguenti stati:

- `pending`: il volume di sostituzione è in fase di creazione.
- `in-progress`: il volume originale è in fase di scollegamento e il volume di sostituzione è in fase di collegamento.
- `succeeded`: il volume di sostituzione è stato collegato correttamente all'istanza e l'istanza è disponibile.
- `failing`: l'attività di sostituzione sta per non essere eseguita correttamente.
- `failed`: l'attività di sostituzione non è stata eseguita correttamente ma il volume root è ancora collegato.
- `failing-detached`: l'attività di sostituzione sta per non essere eseguita correttamente e l'istanza potrebbe non avere un volume root collegato.
- `failed-detached`: l'attività di sostituzione non è stata eseguita correttamente e all'istanza non è collegato alcun volume root.

Se l'operazione di sostituzione del volume root non riesce, l'istanza viene riavviata e il volume root originale rimane collegato all'istanza.

Considerazioni

Prima di iniziare, prendi in considerazioni le seguenti informazioni.

Requisiti

- L'istanza deve essere nello stato `running`.
- L'istanza viene riavviata automaticamente durante il processo. Il contenuto della memoria (RAM) viene cancellato durante il riavvio. Non sono necessari riavvii manuali.
- Non è possibile sostituire il volume root se si tratta di un volume di instance store. Sono supportate solo le istanze con volumi root di Amazon EBS.
- Puoi sostituire il volume root per tutti i tipi di istanza virtualizzati e per le istanze bare metal di EC2 per Mac. Nessun altro tipo di istanza bare metal è supportato.

- Quando si utilizza un'istantanea, è possibile utilizzare solo le istantanee create direttamente dai volumi root correnti o precedenti dell'istanza.
- Se il tuo account è abilitato per Crittografia Amazon EBS di default nella regione corrente, il volume radice sostitutivo creato dall'attività di sostituzione del volume radice è sempre crittografato, indipendentemente dallo stato di crittografia dell'istantanea specificata o dal volume radice dell'AMI specificata.

Risultati della crittografia

La tabella seguente riepiloga i possibili risultati della crittografia.

	Volume root originale	Istantanea, AMI o volume specificati	Crittografia per impostazione predefinita	Volume root sostitutivo	Chiave di crittografia utilizzata per sostituire il volume root
Ripristino del volume root sostitutivo allo stato di avvio	Crittografato	Non applicabile	Non considerato	Crittografato	Stessa chiave KMS del volume principale originale
	Non crittografato	Non applicabile	Disabilitato	Non crittografato	Non applicabile
	Non crittografato	Non applicabile	Abilitato	Crittografato	Accountchiave KMS predefinita per la crittografia Amazon EBS
Ripristina il volume root sostitutivo da	Crittografato	Non crittografato	Non considerato	Crittografato	Stessa chiave KMS del volume

	Volume root originale	Istantanea, AMI o volume specificati	Crittografia per impostazione predefinita	Volume root sostitutivo	Chiave di crittografia utilizzata per sostituire il volume root
snapshot o AMI					principale originale
	Crittografato	Crittografato	Non considerato	Crittografato	Stessa chiave KMS del volume principale originale
	Non crittografato	Non crittografato	Disabilitato	Non crittografato	Non applicabile
	Non crittografato	Non crittografato	Abilitato	Crittografato	Accountchiave KMS predefinita per la crittografia Amazon EBS

	Volume root originale	Istantanea, AMI o volume specificati	Crittografia per impostazione predefinita	Volume root sostitutivo	Chiave di crittografia utilizzata per sostituire il volume root
	Non crittografato	Crittografato	Non considerato	Crittografato	Se l'AMI o l'istantanea è di proprietà dell'account, il volume sostitutivo viene crittografato con la chiave KMS dell'AMI o dell'istantanea. Se AMI o snapshot sono condivisi con l'account, il volume sostitutivo viene crittografato con quello dell'account KMS predefinita per la crittografia Amazon EBS.

	Volume root originale	Istantanea, AMI o volume specificati	Crittografia per impostazione predefinita	Volume root sostitutivo	Chiave di crittografia utilizzata per sostituire il volume root
Ripristina il volume principale sostitutivo da un volume Amazon EBS esistente	Crittografato	Crittografato	Non applicabile	Crittografato	Chiave KMS del volume specificato
	Crittografato	Non crittografato	Non applicabile	Non consentito o Non è possibile sostituire un volume radice crittografato con un volume non crittografato. Amazon EC2 rifiuta l'attività di sostituzione.	Non applicabile
	Non crittografato	Non crittografato	Non applicabile	Non crittografato	Non applicabile
	Non crittografato	Crittografato	Non applicabile	Crittografato	Chiave KMS del volume specificato

Sostituzione di un volume root

Quando sostituisci il volume root per un'istanza, viene creata un'attività di sostituzione del volume root. Puoi utilizzare l'attività di sostituzione del volume root per monitorare l'avanzamento e l'esito del processo di sostituzione.

Console

Per sostituire il volume root

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza per la quale sostituire il volume root e scegliere Operazioni, Monitoraggio e risoluzione dei problemi, Sostituzione di un volume root.

   > **Note**
   >
   > Se l'istanza selezionata non è nello stato `running`, l'operazione Replace root volume (Sostituisci il volume root) è disabilitata.

4. In Ripristina, scegli una delle seguenti opzioni:
   - Stato di avvio: ripristina il volume root sostitutivo dallo snapshot utilizzato per creare il volume root corrente.
   - Snapshot: ripristina il volume root sostitutivo nello snapshot specificato. In Snapshot, seleziona lo snapshot da utilizzare.
   - Immagine: ripristina il volume root sostitutivo utilizzando l'AMI specificata. In Immagine, seleziona l'AMI da utilizzare.
5. (Facoltativo) Per la velocità di inizializzazione del volume, puoi specificare la velocità di inizializzazione del volume di Amazon EBS (velocità di inizializzazione del volume), in MiB/s, in base alla quale i blocchi di istantanee devono essere scaricati da Amazon S3 sul volume. Per ulteriori informazioni, consulta Use an Amazon EBS Provisioned Rate for Volume Initialization. Per utilizzare la velocità di inizializzazione predefinita o il ripristino rapido degli snapshot (se abilitato per lo snapshot selezionato), non specificare una velocità.
6. (Facoltativo) Per eliminare il volume root che stai sostituendo, seleziona Elimina volume root sostituito.
7. Scegli Crea attività sostitutiva.
8. Per monitorare l'attività sostitutiva, scegli la scheda Archiviazione per l'istanza ed espandi Attività sostitutive recenti del volume root.

AWS CLI

Ripristino del volume root sostitutivo allo stato di avvio

Utilizzare il comando create-replace-root-volume-task. Per `--instance-id`, specifica l'ID dell'istanza per la quale sostituire il volume root. Ometti i parametri `--snapshot-id` e `--image-id`. Per eliminare il volume root originale dopo che è stato sostituito, includi `--delete-replaced-root-volume` e specifica `true`. Per specificare la velocità di inizializzazione del volume con cui i blocchi di snapshot vengono scaricati da Amazon S3 sul volume, specifica un valore compreso tra e. `--volume-initialization-rate` `100` `300` MiB/s

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--delete-replaced-root-volume \
--volume-initialization-rate 150
```

Ripristino del volume root sostitutivo in uno snapshot specifico

Utilizzare il comando create-replace-root-volume-task. Per `--instance-id`, specifica l'ID dell'istanza per la quale sostituire il volume root. Per `--snapshot-id`, specifica l'ID dello snapshot da utilizzare. Per eliminare il volume root originale dopo che è stato sostituito, includi `--delete-replaced-root-volume` e specifica `true`. Per specificare la velocità di inizializzazione del volume con cui i blocchi di snapshot vengono scaricati da Amazon S3 sul volume, specifica un valore compreso tra e. `--volume-initialization-rate` `100` `300` MiB/s

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--snapshot-id snap-9876543210abcdef0 \
--delete-replaced-root-volume \
--volume-initialization-rate 150
```

Ripristino del volume root sostitutivo tramite un'AMI

Utilizzare il comando create-replace-root-volume-task. Per `--instance-id`, specifica l'ID dell'istanza per la quale sostituire il volume root. Per `--image-id`, specifica l'ID dell'AMI da utilizzare. Per eliminare il volume root originale dopo che è stato sostituito, includi `--delete-replaced-root-volume` e specifica `true`. Per specificare la velocità di inizializzazione del volume con cui i blocchi di snapshot vengono scaricati da Amazon S3 sul volume, specifica un valore compreso tra e. `--volume-initialization-rate` `100` `300` MiB/s

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--image-id ami-09876543210abcdef \
--delete-replaced-root-volume \
--volume-initialization-rate 150
```

Per sostituire il volume principale utilizzando un volume Amazon EBS esistente

Utilizzare il comando create-replace-root-volume-task. Per `--instance-id`, specifica l'ID dell'istanza per cui sostituire il volume principale (ad esempio, `i-1234567890abcdef0`). Per `--volume-id`, specifica l'ID del volume Amazon EBS da utilizzare come nuovo volume root. Per eliminare il volume root originale dopo il completamento della sostituzione, includi. `--delete-replaced-root-volume` Amazon EC2 accetta il `--volume-initialization-rate` parametro ma lo ignora con questa opzione perché non scarica i dati delle istantanee.

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--volume-id vol-0123456789abcdef0 \
--delete-replaced-root-volume
```

Per visualizzare lo stato di un'attività di sostituzione del volume root

Utilizza il comando describe-replace-root-volume-tasks e specifica gli ID delle attività di sostituzione del volume root da visualizzare.

```
aws ec2 describe-replace-root-volume-tasks \
    --replace-root-volume-task-ids replacevol-1234567890abcdef0 \
    --query ReplaceRootVolumeTasks[].TaskState
```

Di seguito è riportato un output di esempio.

```
[
    "succeeded"
]
```

In alternativa, specificare il filtro `instance-id` per filtrare i risultati in base all'istanza.

```
$ aws ec2 describe-replace-root-volume-tasks \
```

```
    --filters Name=instance-id,Values=i-1234567890abcdef0
```

PowerShell

Ripristino del volume root sostitutivo allo stato di avvio

Utilizza il comando New-EC2ReplaceRootVolumeTask. Per `-InstanceId`, specifica l'ID dell'istanza per la quale sostituire il volume root. Ometti i parametri `-SnapshotId` e `-ImageId`. Per eliminare il volume root originale dopo che è stato sostituito, includi `-DeleteReplacedRootVolume` e specifica `$true`. Per specificare la velocità di inizializzazione del volume con cui i blocchi di snapshot vengono scaricati da Amazon S3 sul volume, specifica un valore compreso tra e. `-VolumeInitializationRate` `100` `300` MiB/s

```
New-EC2ReplaceRootVolumeTask `
    -InstanceId i-1234567890abcdef0 `
    -VolumeInitializationRate 150 `
    -DeleteReplacedRootVolume $true
```

Ripristino del volume root sostitutivo in uno snapshot specifico

Utilizza il comando New-EC2ReplaceRootVolumeTask. Per `--InstanceId`, specifica l'ID dell'istanza per la quale sostituire il volume root. Per `-SnapshotId`, specifica l'ID dello snapshot da utilizzare. Per eliminare il volume root originale dopo che è stato sostituito, includi `-DeleteReplacedRootVolume` e specifica `$true`. Per specificare la velocità di inizializzazione del volume con cui i blocchi di snapshot vengono scaricati da Amazon S3 sul volume, specifica un valore compreso tra e. `-VolumeInitializationRate` `100` `300` MiB/s

```
New-EC2ReplaceRootVolumeTask `
    -InstanceId i-1234567890abcdef0 `
    -SnapshotId snap-9876543210abcdef0 `
    -VolumeInitializationRate 150 `
    -DeleteReplacedRootVolume $true
```

Ripristino del volume root sostitutivo tramite un'AMI

Utilizza il comando New-EC2ReplaceRootVolumeTask. Per `-InstanceId`, specifica l'ID dell'istanza per la quale sostituire il volume root. Per `-ImageId`, specifica l'ID dell'AMI da utilizzare. Per eliminare il volume root originale dopo che è stato sostituito, includi `-DeleteReplacedRootVolume` e specifica `$true`. Per specificare la velocità di inizializzazione

del volume con cui i blocchi di snapshot vengono scaricati da Amazon S3 sul volume, specifica un valore compreso tra e. `-VolumeInitializationRate` `100` `300` MiB/s

```
New-EC2ReplaceRootVolumeTask `
    -InstanceId i-1234567890abcdef0 `
    -ImageId ami-0abcdef1234567890 `
    -VolumeInitializationRate 150 `
    -DeleteReplacedRootVolume $true
```

Per sostituire il volume principale utilizzando un volume Amazon EBS esistente

Utilizza il comando New-EC2ReplaceRootVolumeTask. Per`-InstanceId`, specifica l'ID dell'istanza per cui sostituire il volume principale (ad esempio,`i-1234567890abcdef0`). Per`-VolumeId`, specifica l'ID del volume Amazon EBS da utilizzare come nuovo volume root. Per eliminare il volume root originale dopo il completamento della sostituzione, includi `-DeleteReplacedRootVolume` e specifica. `$true` Amazon EC2 accetta il `-VolumeInitializationRate` parametro ma lo ignora con questa opzione perché non scarica i dati delle istantanee.

```
New-EC2ReplaceRootVolumeTask `
    -InstanceId i-1234567890abcdef0 `
    -VolumeId vol-0123456789abcdef0 `
    -DeleteReplacedRootVolume $true
```

Per visualizzare lo stato di un'attività di sostituzione del volume root

Usa il Get-EC2ReplaceRootVolumeTask comando e specifica gli ID delle attività di sostituzione del volume principale da visualizzare.

```
(Get-EC2ReplaceRootVolumeTask `
    -ReplaceRootVolumeTaskIds replacevol-1234567890abcdef0).TaskState.Value
```

Di seguito è riportato un output di esempio.

```
Succeeded
```

In alternativa, specificare il filtro `instance-id` per filtrare i risultati in base all'istanza.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -Filters @{Name = 'instance-id'; Values =
 'i-1234567890abcdef0'} | Format-Table
```

Nomi dei dispositivi per i volumi sulle EC2 istanze Amazon

Quando colleghi un volume alla tua istanza, includi un nome di dispositivo per il volume. Questo nome di dispositivo viene utilizzato da Amazon EC2. Il driver del dispositivo a blocchi per l'istanza assegna il nome effettivo del volume durante il montaggio del volume e il nome assegnato può essere diverso dal nome EC2 utilizzato da Amazon.

Il numero di volumi che l'istanza può supportare viene determinato dal sistema operativo. Per ulteriori informazioni, consulta Limiti di volume di Amazon EBS per le istanze Amazon EC2.

Indice

- Nomi dei dispositivi disponibili
- Considerazioni sul nome dei dispositivi

Nomi dei dispositivi disponibili

Istanze Linux

Sono disponibili due tipi di virtualizzazione per le istanze Linux: paravirtuale (PV) e della macchina virtuale hardware (HVM). Il tipo di virtualizzazione viene determinato dall'AMI utilizzata per avviare l'istanza. Tutti i tipi di istanza supportano HVM AMIs. Alcuni tipi di istanze della generazione precedente supportano AMIs PV. Assicurati di prendere nota del tipo di virtualizzazione della tua AMI, poiché i nomi di dispositivo consigliati e disponibili dipendono dal tipo di virtualizzazione dell'istanza. Per ulteriori informazioni, consulta Tipi di virtualizzazione.

Nella tabella seguente sono elencati i nomi dei dispositivi disponibili che è possibile specificare in una mappatura dei dispositivi a blocchi o quando si collega un volume EBS.

Tipo di virtualizzazione	Disponibilità	Riservato per il volume root	Consigliato per volumi di dati EBS	Volumi di archivio dell'istanza
Paravirtuale	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hd[a-z]	/dev/sda1	/dev/sd[f-p] /dev/sd[f-p][1-6]	/dev/sd[b-e]

Tipo di virtualizzazione	Disponibilità	Riservato per il volume root	Consigliato per volumi di dati EBS	Volumi di archivio dell'istanza
	/dev/hd[a-z][1-15]			
HVM	/dev/sd[a-z] /dev/xvd[a-c][a-z] /dev/xvdd[a-x]	Differisce per AMI /dev/sda1 or /dev/xvda	/dev/sd[b-z] /dev/xvdb[b-z] *	/dev/sd[b-e] /dev/sd[b-h] (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge) /dev/sd[b-i] (i2.8xlarge) **

* I nomi dei dispositivi specificati per NVMe i volumi EBS in una mappatura a blocchi dei dispositivi vengono rinominati utilizzando i nomi dei NVMe dispositivi (). `/dev/nvme[0-26]n1` Il driver del dispositivo a blocchi può assegnare i nomi dei NVMe dispositivi in un ordine diverso da quello specificato per i volumi nella mappatura dei dispositivi a blocchi.

** I volumi dell' NVMe instance store vengono enumerati automaticamente e viene assegnato un nome di dispositivo. NVMe

Istanze Windows

AWS Windows AMIs utilizza uno dei seguenti set di driver per consentire l'accesso all'hardware virtualizzato:

- AWS PV: Driver paravirtuali per le istanze Windows
- AWS NVMe: Driver NVMe

Nomi dei dispositivi per le istanze basate su Nitro

Nella tabella seguente sono elencati i nomi dei dispositivi disponibili che è possibile specificare in una mappatura dei dispositivi a blocchi o quando si collega un volume EBS a un'istanza basata su Nitro.

Tipo del driver	Disponibilità	Riservato per il volume root	Consigliato per volumi EBS	Volumi di archivio dell'istanza
AWS NVMe	xvd[a-z] xvd[a-c][a-z] xvdd[a-x] /dev/sda1	/dev/sda1	xvd[b-z] xvdb[b-z]	*

* i volumi dell' NVMe instance store vengono enumerati automaticamente e viene assegnata una lettera di unità Windows.

Nomi dei dispositivi per le istanze basate su Xen

Nella tabella seguente sono elencati i nomi dei dispositivi disponibili che è possibile specificare in una mappatura dei dispositivi a blocchi o quando si collega un volume EBS a un'istanza basata su Xen.

Tipo del driver	Disponibilità	Riservato per il volume root	Consigliato per volumi EBS	Volumi di archivio dell'istanza
AWS PV	xvd[b-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-z]	xvdc[a-x] xvd[a-e]
Citrix PV (non più supportato)	xvd[b-z] xvd[b-c][a-z] /dev/sda1	/dev/sda1	xvd[f-z]	xvdc[a-x] xvd[a-e]

Tipo del driver	Disponibilità	Riservato per il volume root	Consigliato per volumi EBS	Volumi di archivio dell'istanza
	/dev/sd[b-e]			
Red Hat PV (non più supportato)	xvd[a-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-p]	xvdc[a-x] xvd[a-e]

Per ulteriori informazioni sui volumi di instance store, consulta Archivio dell'istanza archiviazione a blocchi temporanea per le istanze EC2. Per ulteriori informazioni sui volumi NVMe EBS (istanze basate su Nitro), incluso come identificare il dispositivo EBS, consulta Amazon EBS e NVMe la Amazon EBS User Guide.

Considerazioni sul nome dei dispositivi

Quando selezioni un nome di dispositivo, tieni presenti le informazioni seguenti:

- La parte finale dei nomi dei dispositivi che usi non dovrebbe sovrapporsi in quanto può causare problemi all'avvio dell'istanza. Ad esempio, evita di utilizzare combinazioni come `/dev/xvdf` e `xvdf` per volumi collegati alla stessa istanza.
- Sebbene tu possa collegare i volumi EBS utilizzando i nomi di dispositivo usati per collegare i volumi instance store, ti sconsigliamo fortemente di procedere in tal modo perché il comportamento potrebbe essere imprevedibile.
- Il numero di volumi di NVMe Instance Store per un'istanza dipende dalla dimensione dell'istanza. NVMe i volumi di instance store vengono automaticamente enumerati e assegnati un nome di NVMe dispositivo (istanze Linux) o una lettera di unità Windows (istanze Windows).
- (istanze Windows) AWS Windows è AMIs dotato di software aggiuntivo che prepara un'istanza al primo avvio. Si tratta del servizio EC2 Config (Windows AMIs precedente a Windows Server 2016) o EC2 Launch (Windows Server 2016 e versioni successive). Dopo essere stati mappati alle unità, i dispositivi vengono inizializzati e montati. L'unità root viene inizializzata e montata come `C:\`. Per impostazione predefinita, quando un volume EBS viene collegato a un'istanza Windows, può comparire come qualsiasi lettera di unità nell'istanza. Puoi modificare le impostazioni

per configurare le lettere di unità dei volumi in base alle tue specifiche. Ad esempio, i volumi di archiviazione, l'impostazione predefinita dipende dal driver. AWS I driver PV e i driver Citrix PV assegnano ai volumi di archiviazione delle istanze le lettere di unità che vanno da Z: a A:. I driver Red Hat assegnano, ai volumi instance store, lettere di unità che vanno dalla D: alla Z:. Per ulteriori informazioni, consultare Agenti di avvio Windows su istanze Amazon EC2 Windows e Come vengono collegati e mappati i volumi per le istanze Windows di Amazon EC2.

- (Istanze Linux) A seconda del driver del dispositivo a blocchi del kernel, il dispositivo potrebbe essere collegato con un nome diverso da quello che hai specificato. Ad esempio, se specifichi un nome dispositivo `/dev/sdh`, il tuo dispositivo potrebbe essere rinominato `/dev/xvdh` o `/dev/hdh`. Nella maggior parte dei casi, la lettera finale rimane la stessa. In alcune versioni di Red Hat Enterprise Linux (e relative varianti, come CentOS), anche la lettera finale potrebbe cambiare (`/dev/sda` potrebbe diventare `/dev/xvde`). In questi casi, la lettera finale del nome di ciascun dispositivo aumenta dello stesso numero di volte. Ad esempio, se `/dev/sdb` è rinominato `/dev/xvdf`, `/dev/sdc` viene rinominato `/dev/xvdg`. Amazon Linux crea un collegamento simbolico per il nome che hai specificato per il dispositivo rinominato. Altri sistemi operativi potrebbero avere un comportamento diverso.
- (Istanze Linux) HVM AMIs non supporta l'uso di numeri finali nei nomi dei dispositivi, ad eccezione di`/dev/sda1`, che è riservato al volume root e. `/dev/sda2` Sebbene sia possibile utilizzare `/dev/sda2`, l'uso di questa mappatura dei dispositivi non è consigliata con istanze HVM.
- (Istanze Linux) Quando si utilizza PV AMIs, non è possibile allegare volumi che condividono le stesse lettere del dispositivo con e senza cifre finali. Ad esempio, se colleghi un volume come `/dev/sdc` e un altro volume come `/dev/sdc1`, solo `/dev/sdc` è visibile per l'istanza. Per utilizzare cifre finali nei nomi dei dispositivi, è necessario usarle in tutti i nomi che condividono le stesse lettere di base (come `/dev/sdc1`, `/dev/sdc2`, `/dev/sdc3`).
- (Istanze Linux) Alcuni kernel personalizzati possono presentare restrizioni che limitano l'uso a `/dev/sd[f-p]` o `/dev/sd[f-p][1-6]`. Se riscontri problemi con l'utilizzo di `/dev/sd[q-z]` o `/dev/sd[q-z][1-6]`, prova a passare a `/dev/sd[f-p]` o `/dev/sd[f-p][1-6]`.

Prima di specificare il nome del dispositivo selezionato, verifica che sia disponibile. In caso contrario, verrà restituito un errore che indica che il nome del dispositivo è già in uso. Per visualizzare i dispositivi a disco e i relativi punti di montaggio, utilizza il comando lsblk (istanze Linux) o l'utilità Gestione disco o il comando diskpart (istanze Windows).

Mappature dei dispositivi a blocchi per i volumi sulle istanze Amazon EC2

Ogni istanza che avvii dispone di un volume root associato, che è un volume Amazon EBS o un volume di archivio dell'istanza. Puoi utilizzare le mappature dei dispositivi a blocchi per specificare ulteriori volumi EBS o volumi di archivio dell'istanza da collegare a un'istanza quando viene avviata. Puoi anche collegare volumi EBS aggiuntivi a un'istanza in esecuzione. Tuttavia, il solo modo di collegare volumi di archivio dell'istanza a un'istanza è utilizzare mappature dei dispositivi a blocchi per collegarli quando l'istanza viene avviata.

Indice

- Concetti relativi alla mappatura dei dispositivi a blocchi
- Aggiungere mappature dei dispositivi a blocchi a un'AMI
- Aggiungi mappature dei dispositivi a blocchi all'istanza Amazon EC2

Concetti relativi alla mappatura dei dispositivi a blocchi

Un dispositivo a blocchi è un dispositivo di archiviazione che sposta i dati in sequenze di byte o bit (blocchi). Questi dispositivi supportano l'accesso casuale e generalmente utilizzano il buffer I/O. Gli esempi includono dischi rigidi, CD-ROM unità e unità flash. Un dispositivo a blocchi può essere collegato fisicamente a un computer oppure è possibile accedervi in remoto come se fosse collegato fisicamente.

Amazon EC2 supporta due tipi di dispositivi a blocchi:

- Volumi di instance store (dispositivi virtuali il cui hardware sottostante è fisicamente collegato al computer host per l'istanza)
- Volumi EBS (dispositivi di archiviazione remoti)

Una mappatura dei dispositivi a blocchi definisce i dispositivi a blocchi (volumi instance store e volumi EBS) da collegare a un'istanza. Puoi specificare una mappatura dei dispositivi a blocchi come parte del processo di creazione di un'AMI in modo che la mappatura venga utilizzata da tutte le istanze avviate dall'AMI. In alternativa, puoi specificare una mappatura dei dispositivi a blocchi quando avvii un'istanza, in modo che la mappatura sostituisca quella specificata nell'AMI da cui hai avviato l'istanza. Tieni presente che i volumi instance store NVMe supportati da un tipo di istanza vengono

enumerati e assegnati a un nome di dispositivo automaticamente all'avvio dell'istanza; includerli nella mappatura dei dispositivi a blocchi non ha nessuna conseguenza.

Indice

- Voci della mappatura dei dispositivi a blocchi
- Precisazioni sui volumi instance store nelle mappature dei dispositivi a blocchi
- Esempio di mappatura dei dispositivi a blocchi
- Come i dispositivi vengono resi disponibili nel sistema operativo

Voci della mappatura dei dispositivi a blocchi

Quando crei una mappatura dei dispositivi a blocchi, devi specificare le seguenti informazioni per ogni dispositivo a blocchi che devi collegare all'istanza:

- Il nome del dispositivo utilizzato in Amazon EC2. Il driver dei dispositivi a blocchi dell'istanza assegna il nome del volume effettivo durante il montaggio del volume. Il nome assegnato può essere diverso dal nome che Amazon EC2 consiglia. Per ulteriori informazioni, consulta Nomi dei dispositivi per i volumi sulle EC2 istanze Amazon.

Per i volumi dell'Instance store, è inoltre possibile specificare le seguenti informazioni:

- Il dispositivo virtuale: `ephemeral[0-23]`. Tieni presente che il numero e la dimensione dei volumi instance store per l'istanza variano a seconda del tipo di istanza stessa.

Per i volumi dell'Instance store di NVMe, si applicano anche le seguenti informazioni:

- Questi volumi vengono enumerati e assegnati a un nome di dispositivo automaticamente all'avvio dell'istanza; includerli nella mappatura dei dispositivi a blocchi non ha nessuna conseguenza.

Per i volumi EBS, specificare anche le seguenti informazioni:

- L'ID dello snapshot da utilizzare per creare il dispositivo a blocchi (snap-xxxxxxxx). Questo valore è opzionale se specifichi una dimensione per il volume. Non è possibile specificare l'ID di uno snapshot archiviato.
- La dimensione del volume in GiB. La dimensione specificata deve essere maggiore o uguale a quella della snapshot specificata.

- Determina se eliminare il volume al momento dell'interruzione dell'istanza (`true` o `false`). Il valore predefinito è `true` per il volume root e `false` per i volumi collegati. Quando crei un'AMI, la relativa mappatura dei dispositivi a blocchi eredita questa impostazione dall'istanza. Quando avvii un'istanza, eredita questa impostazione dall'AMI.
- Il tipo di volume, che può essere `gp2` e `gp3` per SSD per scopo generico, `io1` e `io2` per SSD IOPS con provisioning, `st1` per HDD ottimizzati per velocità effettiva, `sc1` per HDD Cold o `standard` per Magnetici.
- Il numero di input/output operazioni al secondo (IOPS) supportate dal volume. (Utilizzato solo con i volumi `io1` e `io2`).
- Alcuni tipi di istanza supportano più di una scheda EBS. È possibile selezionare la scheda EBS per il volume a cui collegare specificando l'indice della scheda EBS. Per ulteriori informazioni, consulta Schede EBS.

Precisazioni sui volumi instance store nelle mappature dei dispositivi a blocchi

Ci sono molte precisazioni da tenere in considerazione quando avvii le istanze con le AMIs che nelle mappature dei dispositivi a blocchi hanno dei volumi instance store.

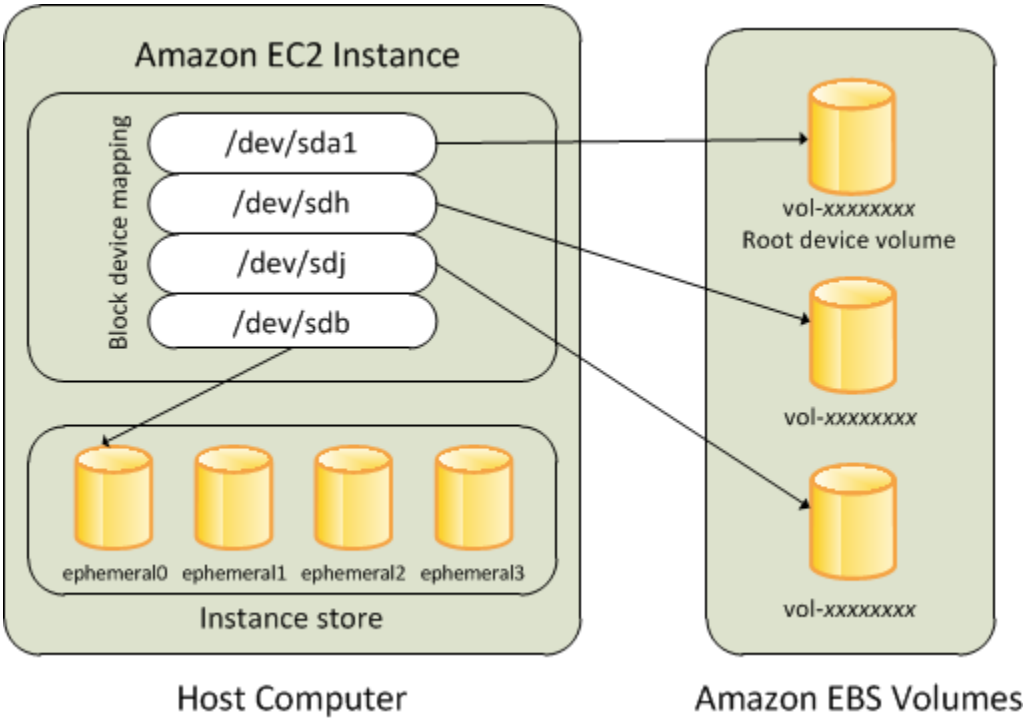
- Alcuni tipi di istanza includono più volumi instance store di altre, mentre alcune non ne contengono affatto. Se il tuo tipo di istanza supporta un volume instance store e la tua AMI dispone di mappature per due volumi instance store, l'istanza verrà avviata con un volume instance store.
- I volumi instance store possono essere mappati solo al momento dell'avvio. Non puoi arrestare un'istanza senza volumi instance store (come `t2.micro`), modificare l'istanza in un tipo che supporta i volumi instance store e riavviarla con volumi instance store. Tuttavia, puoi creare un'AMI dall'istanza e avviarla su un tipo di istanza che supporta i volumi instance store, quindi mappare questi volumi all'istanza.
- Se avvii un'istanza con volumi instance store mappati, quindi la arresti e la modifichi in un tipo di istanza con meno volumi instance store e la riavvii, le mappature dei volumi instance store dell'avvio iniziale mostreranno ancora i metadati dell'istanza. Tuttavia, per l'istanza è disponibile solo il numero massimo di volumi instance store supportati per quel tipo di istanza.

> **Note**
>
> Quando un'istanza viene arrestata, tutti i dati sui volumi instance store vengono persi.

- A seconda della capacità dell'instance store al momento dell'avvio, le istanze M3 potrebbero ignorare le mappature dei dispositivi a blocchi dell'instance store dell'AMI, a meno che non vengano specificate all'avvio. Per essere certo che i volumi instance store siano disponibili all'avvio dell'istanza, anche se l'AMI che stai avviando include volumi instance store mappati nell'AMI, devi specificare le mappature dei dispositivi a blocchi dell'instance store.

Esempio di mappatura dei dispositivi a blocchi

Questa figura mostra un esempio di mappatura dei dispositivi a blocchi per un'istanza. EBS-backed `/dev/sdb` viene mappato a `ephemeral0`, mentre un volume EBS viene mappato a `/dev/sdh` e l'altro a `/dev/sdj`. Nell'illustrazione è mostrato anche il volume EBS che rappresenta il volume root, `/dev/sda1`.



Tieni presente che in questo argomento l'esempio di mappatura dei dispositivi a blocchi viene utilizzando nei comandi e nelle API di esempio. Puoi trovare i comandi e le API di esempio che consentono di creare le mappatura dei dispositivi a blocchi in Specificare una mappatura dei dispositivi a blocchi di un'AMI e Aggiornamento della mappatura dei dispositivi a blocchi all'avvio di un'istanza.

Come i dispositivi vengono resi disponibili nel sistema operativo

Nomi di dispositivo come `/dev/sdh` e `xvdh` vengono utilizzati da Amazon EC2 per descrivere i dispositivi a blocchi. La mappatura dei dispositivi a blocchi è utilizzata da Amazon EC2 per specificare i dispositivi a blocchi da collegare a un'istanza EC2. Prima che si possa accedere al dispositivo di archiviazione, dopo che è stato allegato a un'istanza, un dispositivo a blocchi deve essere montato dal sistema operativo. Se viene distaccato da un'istanza, un dispositivo a blocchi viene smontato dal sistema operativo e non è più possibile accedere al dispositivo di archiviazione.

Istanze Linux: al primo avvio, i nomi di dispositivo specificati nella mappatura dei dispositivi a blocchi vengono mappati ai dispositivi a blocchi corrispondenti. Il tipo di istanza determina quali volumi instance store formattare e montare per impostazione predefinita. Puoi montare volumi instance store aggiuntivi all'avvio, a condizione che non venga superato il numero consentito di volumi instance store per il tipo di istanza che hai scelto. Per ulteriori informazioni, consulta Archivio dell'istanza archiviazione a blocchi temporanea per le istanze EC2. Il driver dei dispositivi a blocchi dell'istanza determina quali dispositivi utilizzare quando i volumi vengono formattati e montati.

Istanze Windows: al primo avvio, i nomi di dispositivo specificati nella mappatura dei dispositivi a blocchi vengono mappati ai dispositivi a blocchi corrispondenti, quindi il servizio Ec2Config inizializza e monta le unità. Il volume root è montato come `C:\`. I volumi instance store vengono montati come `Z:\`, `Y:\` e così via. Per montare un volume EBS, puoi utilizzare qualsiasi lettera di unità disponibile. Tuttavia, puoi configurare come vengono assegnate le lettere ai volumi EBS. Per ulteriori informazioni, consulta the section called "Agenti di avvio Windows".

Aggiungere mappature dei dispositivi a blocchi a un'AMI

Ogni AMI dispone di una mappatura dei dispositivi a blocchi che specifica i dispositivi a blocchi da collegare a un'istanza al suo avvio dall'AMI. Per aggiungere ulteriori dispositivi a blocchi a un'AMI devi creare una tua AMI.

Indice

- Specificare una mappatura dei dispositivi a blocchi di un'AMI
- Visualizzazione dei volumi EBS nella mappatura dei dispositivi a blocchi di un'AMI

Specificare una mappatura dei dispositivi a blocchi di un'AMI

Ci sono due modi per specificare i volumi oltre al volume root quando crei un'AMI. Se hai già collegato i volumi a un'istanza in esecuzione prima di creare un'AMI dall'istanza, la mappatura dei

dispositivi a blocchi dell'AMI includerà gli stessi volumi. Per i volumi EBS, i dati esistenti vengono salvati in una nuova snapshot, che è specificata nella mappatura dei dispositivi a blocchi. Per i volumi instance store, i dati non vengono conservati.

Per un' EBS-backed AMI, è possibile aggiungere volumi EBS e volumi di storage di istanze utilizzando una mappatura dei dispositivi a blocchi. Per un' S3-backed AMI Amazon, puoi aggiungere volumi di storage di istanze solo modificando le voci di mappatura dei dispositivi a blocchi nel file manifest dell'immagine al momento della registrazione dell'immagine.

> **Note**
>
> Per le istanze M3, devo specificare i volumi instance store nella mappatura dei dispositivi a blocchi dell'istanza quando la avvii. Quando avvii un'istanza M3, i volumi instance store specificati nella mappatura dei dispositivi a blocchi dell'AMI potrebbero venire ignorati se non sono stati specificati come parte della mappatura.

Console

Per aggiungere volumi a un'AMI

1. Aprire la console Amazon EC2.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare un'istanza e scegliere Actions (Operazioni), Image and templates (Immagine e modelli), Create image (Crea immagine).
4. Inserire un nome e una descrizione per l'immagine.
5. I volumi di istanza vengono visualizzati in Instance volumes (Volumi istanza). Per aggiungere un altro volume, scegliere Add volume (Aggiungi volume).
6. Per Volume type (Tipo di volume), scegliere il tipo di volume. Per Device (Dispositivo), scegliere il nome del dispositivo. Per un volume EBS, è possibile specificare dettagli aggiuntivi, ad esempio uno snapshot, la dimensione del volume, il tipo di volume, lo IOPS e lo stato di crittografia.
7. Scegliere Create Image (Crea immagine).

AWS CLI

Per aggiungere volumi a un'AMI

Usa il comando create-image per specificare una mappatura dei dispositivi a blocchi per un'AMI. EBS-backed Usa il comando register-image per specificare una mappatura dei dispositivi a blocchi per un'AMI Amazon. S3-backed

Specificare la mappatura dei dispositivi a blocchi utilizzando il parametro `--block-device-mappings`. Puoi specificare argomenti codificati in JSON direttamente sulla riga di comando o facendo riferimento a un file JSON, come illustrato di seguito.

```
--block-device-mappings file://mapping.json
```

Per aggiungere un volume instance store, utilizzare la mappatura seguente: Nota che i volumi dell'archivio dell'istanza NVMe vengono aggiunti in automatico.

```
{
    "DeviceName": "device_name",
    "VirtualName": "ephemeral0"
}
```

Per aggiungere un volume di 100 GiB vuoto, utilizzare la seguente mappatura:

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Per aggiungere un volume EBS basato su uno snapshot, utilizzare la seguente mappatura:

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "SnapshotId": "snap-1234567890abcdef0"
    }
}
```

Per omettere la mappatura per un dispositivo, utilizzare la seguente mappatura:

```
{
    "DeviceName": "device_name",
```

```
    "NoDevice": ""
}
```

PowerShell

Usa il New-EC2Image cmdlet per specificare una mappatura dei dispositivi a blocchi per un'AMI. EBS-backed Usa il Register-EC2Image cmdlet per specificare una mappatura dei dispositivi a blocchi per un'AMI Amazon. S3-backed

Aggiungi l'opzione `-BlockDeviceMapping`, specificando gli aggiornamenti in `bdm`:

```
-BlockDeviceMapping $bdm
```

La mappatura seguente aggiunge un volume in base a uno snapshot.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.SnapshotId = "snap-1234567890abcdef0"
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "device_name"
$bdm.Ebs = $ebd
```

La mappatura seguente aggiunge un volume di 100 GB vuoto.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.VolumeSize = 100
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "device_name"
$bdm.Ebs = $ebd
```

Visualizzazione dei volumi EBS nella mappatura dei dispositivi a blocchi di un'AMI

Puoi enumerare facilmente i volumi EBS nella mappatura dei dispositivi a blocchi dell'AMI.

Console

Per visualizzare i volumi EBS di un'AMI

1. Aprire la console Amazon EC2.
2. Nel riquadro di navigazione scegliere AMIs (AMI).
3. Scegli le immagini EBS dall'elenco dei filtri per ottenere un elenco di AMI. EBS-backed

4. Selezionare l'AMI desiderata e controllare la scheda Details (Dettagli). Al minimo, le seguenti informazioni sono disponibili per il volume root (dove il termine dispositivo root equivale a volume root):

   - Root Device Type (Tipo dispositivo root (`ebs`)
   - Root Device Name (Nome dispositivo root) (ad esempio, `/dev/sda1`)
   - Block Devices (Dispositivi a blocchi) (ad esempio, `/dev/sda1=snap-1234567890abcdef0:8:true`)

   Se l'AMI è stata creata con volumi EBS aggiuntivi tramite la mappatura dei dispositivi a blocchi, nel campo Block Devices (Dispositivi a blocchi) viene visualizzata anche la mappatura di tali volumi aggiuntivi (Questa schermata non visualizza i volumi instance store).

AWS CLI

Per visualizzare i volumi EBS di un'AMI

Utilizzare il comando describe-images .

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Image[0].BlockDeviceMappings
```

PowerShell

Per visualizzare i volumi EBS di un'AMI

Utilizza il cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).BlockDeviceMappings
```

Aggiungi mappature dei dispositivi a blocchi all'istanza Amazon EC2

Per impostazione predefinita, un'istanza avviata include eventuali dispositivi di archiviazione specificati nella mappatura dei dispositivi a blocchi di un'AMI da cui l'istanza è stata avviata. Puoi specificare le modifiche alle mappatura dei dispositivi a blocchi di un'istanza quando la avvii; tali aggiornamenti sostituiscono la mappatura dei dispositivi a blocchi dell'AMI o si uniscono a essa.

Limitazioni

- Per il volume root, puoi solo modificare: le dimensioni, il tipo e il contrassegno È possibile modificare il Delete on Termination (Elimina al termine).
- Quando modifichi un volume EBS non puoi ridurne le dimensioni, pertanto devi specificare una snapshot le cui dimensioni siano uguali o maggiori di quelle della snapshot specificata nella mappatura dei dispositivi a blocchi dell'AMI.

Processi

- Aggiornamento della mappatura dei dispositivi a blocchi all'avvio di un'istanza
- Aggiornamento della mappatura dei dispositivi a blocchi di un'istanza in esecuzione
- Visualizzazione dei volumi EBS nella mappatura dei dispositivi a blocchi di un'istanza
- Visualizzazione della mappatura dei dispositivi a blocchi di un'istanza per i volumi instance store

Aggiornamento della mappatura dei dispositivi a blocchi all'avvio di un'istanza

Puoi aggiungere volumi EBS e volumi instance store a un'istanza al momento del suo avvio. Tieni presente che l'aggiornamento della mappatura dei dispositivi a blocchi di un'istanza non comporta una modifica permanente della mappatura dell'AMI da cui l'istanza è stata avviata.

Console

Per aggiornare i volumi per un'istanza all'avvio

1. Segui la procedura di avvio di un'istanza, ma non avviare l'istanza finché non avrai completato i seguenti passaggi per aggiornare i volumi.
2. (Facoltativo) Per aggiungere un volume, scegli Configura archiviazione, Aggiungi nuovo volume. Seleziona la dimensione e il tipo di volume.
3. (Facoltativo) Per sopprimere un volume specificato dalla mappatura dei dispositivi a blocchi dell'AMI, scegli Configura archiviazione, Rimuovi.
4. (Facoltativo) Per modificare la configurazione di un volume EBS, nel riquadro Configura archiviazione, scegli Avanzato. Espandi le informazioni relative al volume e apporta le modifiche necessarie.
5. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

AWS CLI

Per aggiornare i volumi per un'istanza all'avvio

Utilizzare il comando run-instances con l'opzione `--block-device-mappings`.

```
--block-device-mappings file://mapping.json
```

Ad esempio, si supponga che un'AMI di mappatura dei dispositivi a blocchi specifichi ciò che segue:

- `/dev/xvda`: volume root EBS
- `/dev/sdh`: volume EBS creato da `snap-1234567890abcdef0`
- `/dev/sdj`: volume EBS vuoto con una dimensione di `100`
- `/dev/sdb`: volume di archivio dell'istanza `ephemeral0`

Supponiamo che quanto segue sia l'istanza di mappatura dei dispositivi a blocchi in `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 100
        }
    },
    {
        "DeviceName": "/dev/sdj",
        "NoDevice": ""
    },
    {
        "DeviceName": "/dev/sdh",
        "Ebs": {
            "VolumeSize": 300
        }
    },
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral1"
    }
```

```
]
```

L'istanza di mappatura dei dispositivi a blocchi esegue le seguenti operazioni:

- Sostituisce la dimensione del volume root, `/dev/xvda`, aumentandola a 100 GiB.
- Impedisce a `/dev/sdj` di collegarsi all'istanza.
- Sostituisce la dimensione di `/dev/sdh`, aumentandola a 300 GiB. Nota che non è necessario specificare nuovamente l'ID snapshot.
- Aggiunge un volume effimero, `/dev/sdc`. Se il tipo di istanza non supporta più volumi di archivio dell'istanza, questo non ha effetto. Se lil tipo dell'istanza supporta i volumi di archivio dell'istanza NVMe, questi vengono enumerati automaticamente, inclusi nell'istanza di mappatura dei dispositivi a blocchi e non possono essere sostituiti.

PowerShell

Per aggiornare i volumi per un'istanza all'avvio

Usa il `-BlockDeviceMapping` parametro con il New-EC2Instance cmdlet con il parametro. `-BlockDeviceMapping`

```
-BlockDeviceMapping $bdm
```

Supponiamo che quanto segue sia l'istanza di mappatura dei dispositivi a blocchi in `$bdm`.

```
$bdm = @()

$root = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$root.DeviceName = "/dev/xvda"
$ebs1 = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebs1.VolumeSize = 100
$root.Ebs = $ebs1
$bdm += $root

$sdj = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdj.DeviceName = "/dev/sdj"
$sdj.NoDevice = ""
$bdm += $sdj

$sdh = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdh.DeviceName = "/dev/sdh"
```

```
$ebs2 = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebs2.VolumeSize = 300
$sdh.Ebs = $ebs2
$bdm += $sdh

$sdc = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdc.DeviceName = "/dev/sdc"
$sdc.VirtualName = "ephemeral1"
$bdm += $sdc
```

L'istanza di mappatura dei dispositivi a blocchi esegue le seguenti operazioni:

- Sostituisce la dimensione del volume root, `/dev/xvda`, aumentandola a 100 GiB.
- Impedisce a `/dev/sdj` di collegarsi all'istanza.
- Sostituisce la dimensione di `/dev/sdh`, aumentandola a 300 GiB. Nota che non è necessario specificare nuovamente l'ID snapshot.
- Aggiunge un volume effimero, `/dev/sdc`. Se il tipo di istanza non supporta più volumi di archivio dell'istanza, questo non ha effetto. Se lil tipo dell'istanza supporta i volumi di archivio dell'istanza NVMe, questi vengono enumerati automaticamente, inclusi nell'istanza di mappatura dei dispositivi a blocchi e non possono essere sostituiti.

Aggiornamento della mappatura dei dispositivi a blocchi di un'istanza in esecuzione

Non è necessario arrestare l'istanza prima di cambiare questo attributo.

AWS CLI

Per aggiornare la mappatura dei dispositivi a blocchi di un'istanza in esecuzione

Utilizza il comando modify-instance-attribute.

Aggiungere l'opzione `--block-device-mappings`:

```
--block-device-mappings file://mapping.json
```

In `mapping.json`, specifica gli aggiornamenti. Ad esempio, il seguente aggiornamento modifica il volume root in modo che persista.

```
[
```

```
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

PowerShell

Per aggiornare la mappatura dei dispositivi a blocchi di un'istanza in esecuzione

Utilizza il cmdlet Edit-EC2InstanceAttribute.

Aggiungere l'opzione `-BlockDeviceMapping`:

```
-BlockDeviceMapping $bdm
```

In `bdm`, specifica gli aggiornamenti. Ad esempio, il seguente aggiornamento modifica il volume root in modo che persista.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.DeleteOnTermination = false
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "/dev/sda1"
$bdm.Ebs = $ebd
```

Visualizzazione dei volumi EBS nella mappatura dei dispositivi a blocchi di un'istanza

Puoi enumerare facilmente i volumi EBS mappati a un'istanza.

Console

Per visualizzare i volumi EBS di un'istanza

1. Aprire la console Amazon EC2.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza ed esaminare i dettagli visualizzati nella scheda Storage (Archiviazione). Al minimo, le seguenti informazioni sono disponibili per il volume root (dove il termine dispositivo root equivale a volume root):

- Tipo di dispositivo root (ad esempio, EBS)
- Nome dispositivo root (ad esempio, `/dev/xvda`)
- Dispositivi a blocchi (ad esempio, `/dev/xvda`, `/dev/sdf` e `/dev/sdj`)

Se l'istanza è stata avviata con volumi EBS aggiuntivi utilizzando una mappatura di dispositivi a blocchi, questi vengono visualizzati in Block devices (Dispositivi a blocchi). Qualsiasi volume dell'instance store non viene visualizzato in questa scheda.

4. Per visualizzare ulteriori informazioni su un volume EBS, scegliere il relativo ID volume per andare alla pagina del volume.

AWS CLI

Per visualizzare i volumi EBS di un'istanza

Utilizzare il comando describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[*].Instances[0].BlockDeviceMappings
```

PowerShell

Per visualizzare i volumi EBS di un'istanza

Utilizza il cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-0bac57d7472c89bac).Instances.BlockDeviceMappings
```

Visualizzazione della mappatura dei dispositivi a blocchi di un'istanza per i volumi instance store

Il tipo di istanza determina il numero e il tipo di volumi dell'archivio dell'istanza disponibili. Se il numero di volumi instance store in una mappatura dei dispositivi a blocchi supera il numero disponibile di volumi instance store per un'istanza, i volumi vengono ignorati. Per visualizzare i volumi dell'archivio dell'istanza per l'istanza, esegui il comando lsblk (istanza Linux) o apri Windows Disk Management (istanza Windows). Per conoscere il numero di volumi instance store supportati da ogni tipo di istanza, consulta le specifiche del tipo di istanza Amazon EC2.

Quando visualizzi la mappatura dei dispositivi a blocchi della tua istanza, puoi vedere solo i volumi EBS e non i volumi instance store. Il metodo utilizzato per visualizzare i volumi dell'archivio istanza per l'istanza dipende dal tipo di volume.

Volumi di archivio istanza NVMe

Istanze Linux

È possibile utilizzare il pacchetto della riga di comando NVMe, nvme-cli, per eseguire query sui volumi dell'archivio istanza NVMe nella mappatura dei dispositivi a blocchi. Scarica e installa il pacchetto sull'instanza, quindi emetti il seguente comando.

```
[ec2-user ~]$ sudo nvme list
```

Di seguito è riportato un esempio di output per un'istanza. Il testo nella colonna Modello indica se il volume è un volume EBS o un volume dell'archivio istanza. In questo esempio, entrambi `/dev/nvme1n1` e `/dev/nvme2n1` sono volumi dell'archivio istanza.

```
Node             SN                   Model
 Namespace
---------------- -------------------- ----------------------------------------
 ---------
/dev/nvme0n1     vol06afc3f8715b7a597 Amazon Elastic Block Store              1

/dev/nvme1n1     AWS2C1436F5159EB6614 Amazon EC2 NVMe Instance Storage        1

/dev/nvme2n1     AWSB1F4FF0C0A6C281EA Amazon EC2 NVMe Instance Storage        1
  ...
```

Istanze Windows

È possibile utilizzare Disk Management o PowerShell per elencare sia i volumi EBS che quelli NVMe dell'Instance Store. Per ulteriori informazioni, consulta the section called “Mappare i dischi NVMe ai volumi”.

Volumi di archivio istanza HDD o SSD

È possibile utilizzare i metadati dell'istanza per effettuare query sui volumi dell'archivio istanza HDD o SSD nella mappatura dei dispositivi a blocchi. I volumi dell'instance store NVMe non sono inclusi nella mappatura dei dispositivi a blocchi.

L'URI di base di tutte le richieste dei metadati dell'istanza è `http://169.254.169.254/latest/`. Per ulteriori informazioni, consulta Utilizzo dei metadati dell'istanza per gestire l'istanza EC2.

Istanze Linux

Innanzitutto connettiti all'istanza in esecuzione, quindi da essa utilizza questa query per ottenere la relativa mappatura dei dispositivi a blocchi.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

La risposta include i nomi dei dispositivi a blocchi dell'istanza. Ad esempio, l'output di un'istanza `m1.small` supportata da archivio istanza somiglia a quello seguente.

```
ami
ephemeral0
root
swap
```

Il dispositivo `ami` è il volume root come visto dall'istanza. I volumi instance store sono denominati `ephemeral[0-23]`. Il dispositivo `swap` è destinato al file di paging. Se hai mappato anche i volumi EBS, questi appariranno come `ebs1`, `ebs2` e così via.

Per ottenere i dettagli su un singolo dispositivo a blocchi nella mappatura dei dispositivi a blocchi, aggiungi il suo nome alla query precedente, come mostrato.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
ephemeral0
```

Istanze Windows

Innanzitutto connettiti all'istanza in esecuzione, quindi da essa utilizza questa query per ottenere la relativa mappatura dei dispositivi a blocchi.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-
mapping/
```

La risposta include i nomi dei dispositivi a blocchi dell'istanza. Ad esempio, l'output di un'istanza `m1.small` supportata da archivio istanza somiglia a quello seguente.

```
ami
ephemeral0
root
swap
```

Il dispositivo `ami` è il volume root come visto dall'istanza. I volumi instance store sono denominati `ephemeral[0-23]`. Il dispositivo `swap` è destinato al file di paging. Se hai mappato anche i volumi EBS, questi appariranno come `ebs1`, `ebs2` e così via.

Per ottenere i dettagli su un singolo dispositivo a blocchi nella mappatura dei dispositivi a blocchi, aggiungi il suo nome alla query precedente, come mostrato.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-
mapping/ephemeral0
```

Come vengono collegati e mappati i volumi per le istanze Windows di Amazon EC2

> **Note**
>
> Questo argomento si applica solo alle istanze Windows.

La tua istanza Windows include un volume EBS che funge da volume root. Se la vostra istanza Windows utilizza driver AWS PV o Citrix PV, potete aggiungere facoltativamente fino a 25 volumi, per un totale di 26 volumi. Per ulteriori informazioni, consulta Limiti di volume di Amazon EBS per le istanze Amazon EC2.

A seconda del tipo di istanza della tua istanza, avrai da 0 a 24 volumi di instance store disponibili possibili per l'istanza. Per utilizzare qualsiasi dei volumi di instance store disponibili per l'istanza, è necessario specificarli alla creazione dell'AMI o all'avvio dell'istanza. Puoi inoltre aggiungere volumi EBS alla creazione dell'AMI o all'avvio dell'istanza o collegarli durante l'esecuzione dell'istanza.

Quando aggiungi un volume all'istanza, è necessario specificare il nome del dispositivo utilizzato da Amazon EC2. Per ulteriori informazioni, consulta Nomi dei dispositivi per i volumi sulle EC2 istanze Amazon. AWS Le Amazon Machine Image (AMI) di Windows contengono un set di driver utilizzati da Amazon EC2 per mappare volume di archivio istanza e EBS ai dischi Windows e alle lettere di unità.

Metodi per mappare i dischi ai volumi EBS

- Mappare i dischi NVMe ai volumi nell'istanza Amazon EC2 Windows
- Mappare i dischi non NVMe ai volumi nell'istanza Amazon EC2 Windows

Mappare i dischi NVMe ai volumi nell'istanza Amazon EC2 Windows

Con Nitro-based le istanze, i volumi EBS sono esposti come dispositivi NVMe. Questo argomento spiega come visualizzare i dischi NVMe disponibili per il sistema operativo Windows sulla tua istanza. Mostra anche come mappare tali dischi NVMe ai volumi Amazon EBS sottostanti e ai nomi dei dispositivi specificati per le mappature dei dispositivi a blocchi utilizzate da Amazon EC2.

Argomenti

- Elenco dei dischi NVMe
- Mappare i dischi NVMe ai volumi

Elenco dei dischi NVMe

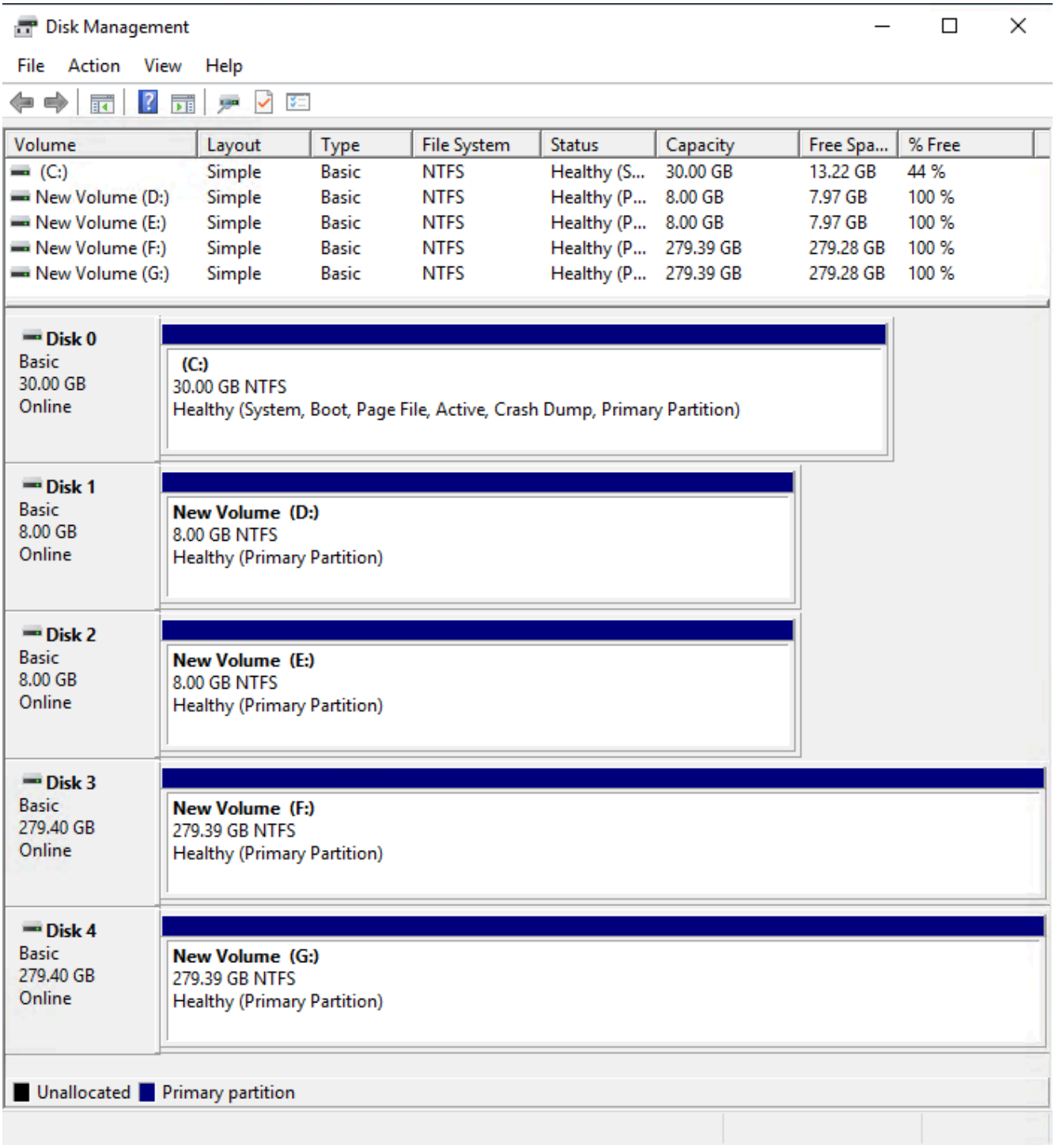
Puoi individuare i dischi sull'istanza Windows tramite Disk Management (Gestione disco) o Powershell.

Disk Management

Individuazione dei dischi sulla tua istanza Windows

1. Accedere all'istanza Windows tramite Remote Desktop. Per ulteriori informazioni, consulta Connessione all'istanza Windows con il protocollo RDP.
2. Avviare l'utilità Disk Management (Gestione disco).
3. Esamina i dischi. Il volume root è un volume EBS montato come `C:\`. Se non sono visualizzati altri dischi, significa che non hai specificato volumi aggiuntivi alla creazione dell'AMI o all'avvio dell'istanza.

   Di seguito è riportato un esempio che mostra i dischi disponibili se si avvia un'istanza `r5d.4xlarge` con due volumi EBS aggiuntivi.



PowerShell

PowerShell Lo script seguente elenca ogni disco e il nome e il volume del dispositivo corrispondenti. È destinato all'uso con Nitro-based istanze che utilizzano NVMe EBS e volumi di storage di istanze.

Connettiti alla tua istanza Windows ed esegui il seguente comando per abilitare l'esecuzione degli script. PowerShell

```
Set-ExecutionPolicy RemoteSigned
```

Copiare lo script seguente e salvarlo come `mapping.ps1` nell'istanza Windows.

```
# List the disks for NVMe volumes

function Get-EC2InstanceMetadata {
    param([string]$Path)
    (Invoke-WebRequest -Uri "http://169.254.169.254/latest/$Path").Content
}

function GetEBSVolumeId {
    param($Path)
    $SerialNumber = (Get-Disk -Path $Path).SerialNumber
    if($SerialNumber -clike 'vol*'){
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("vol","vol-")
    }
    else {
       $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("AWS","AWS-")
    }
    return $EbsVolumeId
}

function GetDeviceName{
    param($EbsVolumeId)
    if($EbsVolumeId -clike 'vol*'){

        $Device  = ((Get-EC2Volume -VolumeId $EbsVolumeId ).Attachment).Device
        $VolumeName = ""
    }
     else {
        $Device = "Ephemeral"
        $VolumeName = "Temporary Storage"
    }
    Return $Device,$VolumeName
}

function GetDriveLetter{
    param($Path)
    $DiskNumber =  (Get-Disk -Path $Path).Number
```

```
    if($DiskNumber -eq 0){
        $VirtualDevice = "root"
        $DriveLetter = "C"
        $PartitionNumber = (Get-Partition -DriveLetter C).PartitionNumber
    }
    else
    {
        $VirtualDevice = "N/A"
        $DriveLetter = (Get-Partition -DiskNumber $DiskNumber).DriveLetter
        if(!$DriveLetter)
        {
            $DriveLetter = ((Get-Partition -DiskId $Path).AccessPaths).Split(",")[0]
        }
        $PartitionNumber = (Get-Partition -DiskId $Path).PartitionNumber
    }

    return $DriveLetter,$VirtualDevice,$PartitionNumber

}

$Report = @()
foreach($Path in (Get-Disk).Path)
{
    $Disk_ID = ( Get-Partition -DiskId $Path).DiskId
    $Disk = ( Get-Disk -Path $Path).Number
    $EbsVolumeId  = GetEBSVolumeId($Path)
    $Size =(Get-Disk -Path $Path).Size
    $DriveLetter,$VirtualDevice, $Partition = (GetDriveLetter($Path))
    $Device,$VolumeName = GetDeviceName($EbsVolumeId)
    $Disk = New-Object PSObject -Property @{
      Disk          = $Disk
      Partitions    = $Partition
      DriveLetter   = $DriveLetter
      EbsVolumeId   = $EbsVolumeId
      Device        = $Device
      VirtualDevice = $VirtualDevice
      VolumeName= $VolumeName
    }
 $Report += $Disk
}

$Report | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, VolumeName
```

Eseguire lo script come segue:

```
PS C:\> .\mapping.ps1
```

Di seguito è riportato un output di esempio per un'istanza con un volume root, due volumi EBS e due volumi instance store.

```
Disk Partitions DriveLetter EbsVolumeId           Device    VirtualDevice VolumeName
---- ---------- ----------- -----------           ------    ------------- ----------
   0          1 C           vol-03683f1d861744bc7 /dev/sda1 root
   1          1 D           vol-082b07051043174b9 xvdb      N/A
   2          1 E           vol-0a4064b39e5f534a2 xvdc      N/A
   3          1 F           AWS-6AAD8C2AEEE1193F0 Ephemeral N/A           Temporary
 Storage
   4          1 G           AWS-13E7299C2BD031A28 Ephemeral N/A           Temporary
 Storage
```

Se non hai configurato le credenziali per Tools for Windows PowerShell sull'istanza Windows, lo script non può ottenere l'ID del volume EBS e gli usi N/A nella `EbsVolumeId` colonna.

Mappare i dischi NVMe ai volumi

Puoi utilizzare il Get-Disk comando per mappare i numeri dei dischi di Windows ai volumi Amazon EBS e ai volumi degli store di istanze Amazon EC2.

```
PS C:\> Get-Disk
Number Friendly Name Serial Number                    HealthStatus
 OperationalStatus      Total Size Partition

                      Style
------ ------------- -------------                    ------------
 -----------------      ---------- ----------
3      NVMe Amazo... AWS6AAD8C2AEEE1193F0_00000001.   Healthy              Online
              279.4 GB MBR
4      NVMe Amazo... AWS13E7299C2BD031A28_00000001.   Healthy              Online
              279.4 GB MBR
2      NVMe Amazo... vol0a4064b39e5f534a2_00000001.   Healthy              Online
                  8 GB MBR
0      NVMe Amazo... vol03683f1d861744bc7_00000001.   Healthy              Online
                 30 GB MBR
```

```
1      NVMe Amazo... vol082b07051043174b9_00000001.   Healthy             Online
                8 GB MBR
```

È anche possibile eseguire il comando ebsnvme-id per eseguire la mappatura dei numeri del disco NVMe con gli ID volume EBS e i nomi dei dispositivi.

```
PS C:\> C:\PROGRAMDATA\Amazon\Tools\ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-03683f1d861744bc7
Device Name: sda1

Disk Number: 1
Volume ID: vol-082b07051043174b9
Device Name: xvdb

Disk Number: 2
Volume ID: vol-0a4064b39e5f534a2
Device Name: xvdc
```

Mappare i dischi non NVMe ai volumi nell'istanza Amazon EC2 Windows

Per le istanze avviate da un'AMI Windows che utilizza driver AWS PV o Citrix PV, puoi utilizzare le relazioni descritte in questa pagina per mappare i dischi di Windows all'Instance Store e ai volumi EBS. Questo argomento spiega come visualizzare i dischi non NVMe disponibili per il sistema operativo Windows sulla tua istanza. Mostra anche come mappare tali dischi non NVMe ai volumi Amazon EBS sottostanti e ai nomi dei dispositivi specificati per le mappature dei dispositivi a blocchi utilizzate da Amazon EC2.

> **Note**
>
> Se si avvia un'istanza e la tua AMI Windows utilizza driver Red Hat PV, è possibile aggiornare l'istanza per utilizzare i driver Citrix. Per ulteriori informazioni, consulta the section called “Aggiornamento dei driver PV”.

Argomenti

- Elenco dei dischi non NVMe
- Mappare i dischi non NVMe ai volumi

Elenco dei dischi non NVMe

È possibile trovare i dischi sull'istanza di Windows utilizzando Gestione disco o. PowerShell

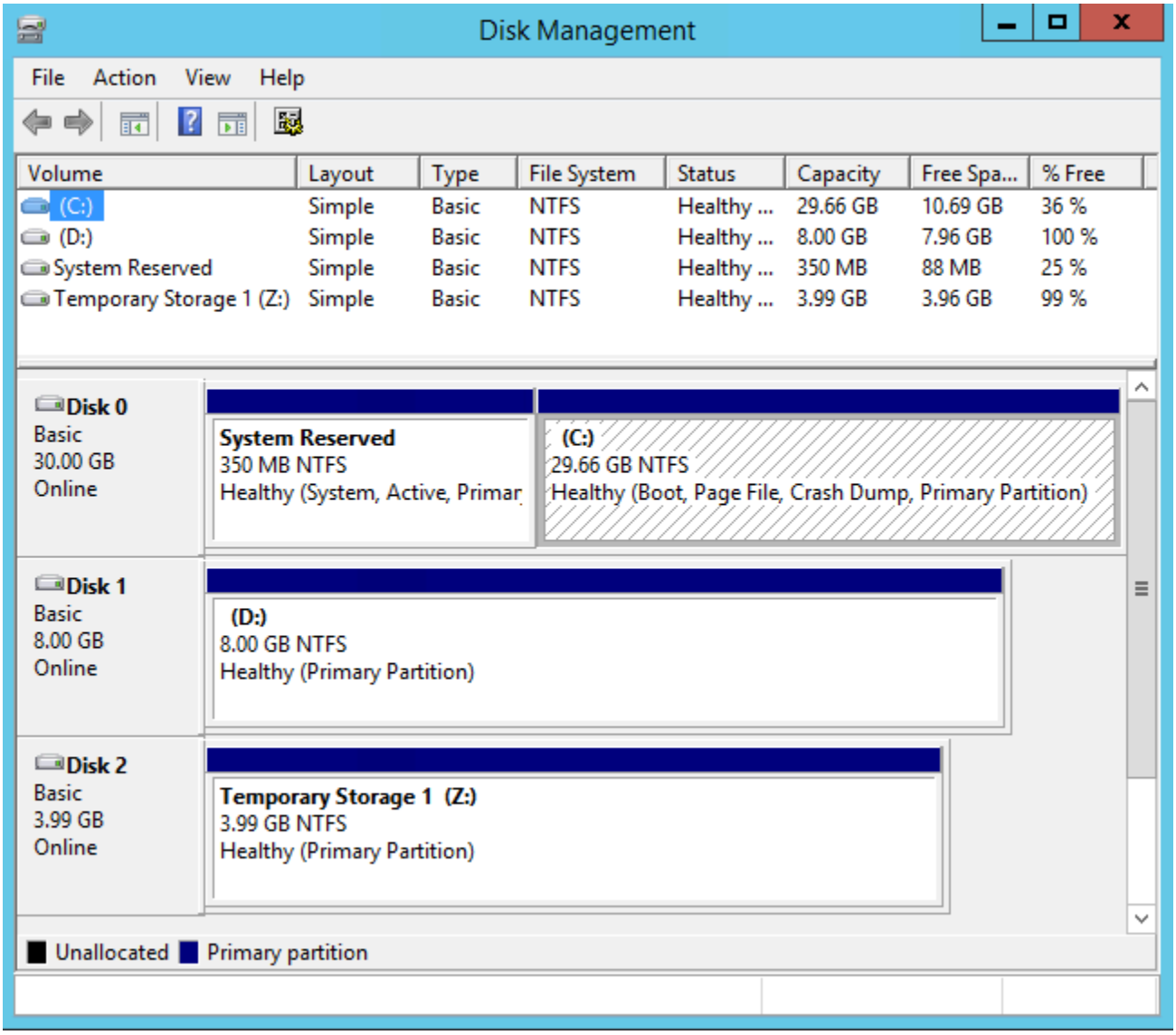
Disk Management

Individuazione dei dischi sulla tua istanza Windows

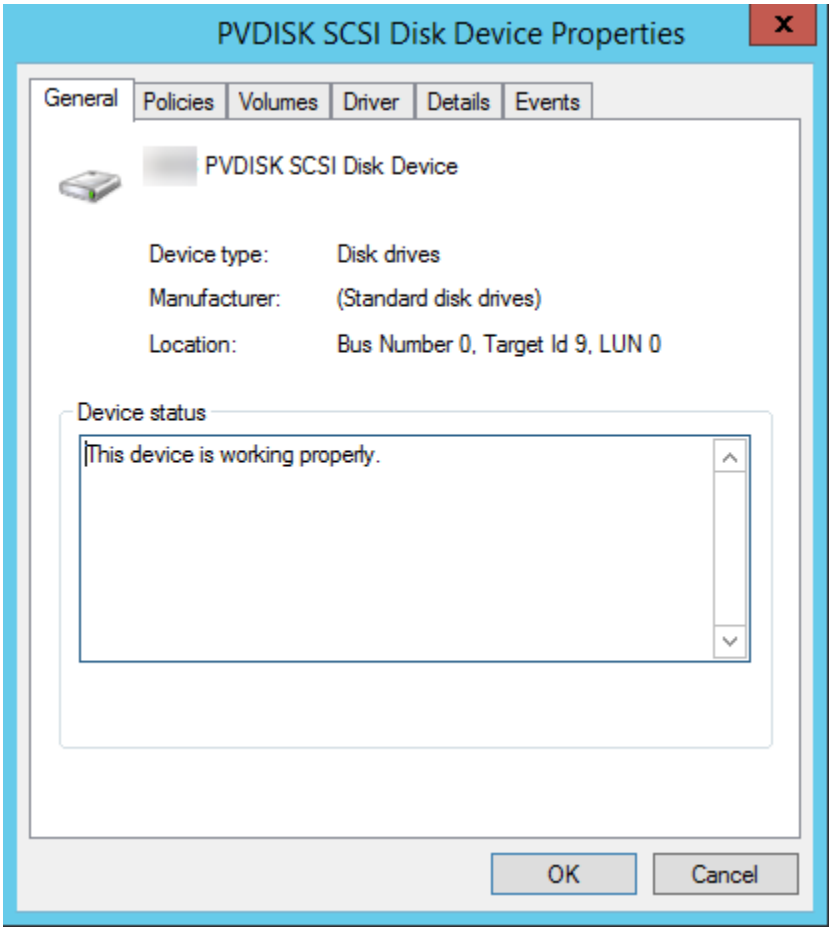
1. Accedere all'istanza Windows tramite Remote Desktop. Per ulteriori informazioni, consulta Connessione all'istanza Windows con il protocollo RDP.
2. Avviare l'utilità Disk Management (Gestione disco).

   Sulla barra delle applicazioni, apri il menu contestuale (clic con il pulsante destro del mouse) per il logo Windows, quindi scegli Gestione disco.
3. Esamina i dischi. Il volume root è un volume EBS montato come `C:\`. Se non sono visualizzati altri dischi, significa che non hai specificato volumi aggiuntivi alla creazione dell'AMI o all'avvio dell'istanza.

   Nell'esempio riportato di seguito sono illustrati i dischi disponibili lanciando un'istanza `m3.medium` con un volume instance store (Disco 2) e un volume EBS aggiuntivo (Disco 1).



4. Apri il menu contestuale (clic con il pulsante destro del mouse) per il riquadro grigio denominato Disco 1, quindi seleziona Proprietà. Prendi nota del valore di Location (Ubicazione) e cercalo nelle tabelle in Mappare i dischi non NVMe ai volumi. Ad esempio, il disco seguente presenta l'ubicazione Bus Number 0, Target Id 9, LUN 0. In base alla tabella dei volumi EBS, il nome del dispositivo di questa ubicazione è `xvdj`.



PowerShell

PowerShell Lo script seguente elenca ogni disco e il nome e il volume del dispositivo corrispondenti.

Requisiti e limitazioni

- Richiede Windows Server 2012 o versione successiva.
- Richiede le credenziali per ottenere l'ID del volume EBS. È possibile configurare un profilo utilizzando gli Strumenti per PowerShell o allegare un ruolo IAM all'istanza.
- Non supporta volumi NVMe.
- Non supporta dischi dinamici.

Connettiti alla tua istanza Windows ed esegui il comando seguente per abilitare l'esecuzione PowerShell dello script.

```
Set-ExecutionPolicy RemoteSigned
```

Copiare lo script seguente e salvarlo come `mapping.ps1` nell'istanza Windows.

```
# List the disks
function Convert-SCSITargetIdToDeviceName {
  param([int]$SCSITargetId)
  If ($SCSITargetId -eq 0) {
    return "sda1"
  }
  $deviceName = "xvd"
  If ($SCSITargetId -gt 25) {
    $deviceName += [char](0x60 + [int]($SCSITargetId / 26))
  }
  $deviceName += [char](0x61 + $SCSITargetId % 26)
  return $deviceName
}

[string[]]$array1 = @()
[string[]]$array2 = @()
[string[]]$array3 = @()
[string[]]$array4 = @()

Get-WmiObject Win32_Volume | Select-Object Name, DeviceID | ForEach-Object {
  $array1 += $_.Name
  $array2 += $_.DeviceID
}

$i = 0
While ($i -ne ($array2.Count)) {
  $array3 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-
Disk).SerialNumber) -replace "_[^ ]*$" -replace "vol", "vol-"
  $array4 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-
Disk).FriendlyName)
  $i ++
}

[array[]]$array = $array1, $array2, $array3, $array4

Try {
  $InstanceId = Get-EC2InstanceMetadata -Category "InstanceId"
  $Region = Get-EC2InstanceMetadata -Category "Region" | Select-Object -
ExpandProperty SystemName
```

```
}
Catch {
  Write-Host "Could not access the instance Metadata using AWS Get-
EC2InstanceMetadata CMDLet.
Verify you have AWSPowershell SDK version '3.1.73.0' or greater installed and
 Metadata is enabled for this instance." -ForegroundColor Yellow
}
Try {
  $BlockDeviceMappings = (Get-EC2Instance -Region $Region -Instance
 $InstanceId).Instances.BlockDeviceMappings
  $VirtualDeviceMap = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").GetEnumerator() | Where-Object { $_.Key -ne "ami" }
}
Catch {
  Write-Host "Could not access the AWS API, therefore, VolumeId is not available.
Verify that you provided your access keys or assigned an IAM role with adequate
 permissions." -ForegroundColor Yellow
}

Get-disk | ForEach-Object {
  $DriveLetter = $null
  $VolumeName = $null
  $VirtualDevice = $null
  $DeviceName = $_.FriendlyName

  $DiskDrive = $_
  $Disk = $_.Number
  $Partitions = $_.NumberOfPartitions
  $EbsVolumeID = $_.SerialNumber -replace "_[^ ]*$" -replace "vol", "vol-"
  if ($Partitions -ge 1) {
    $PartitionsData = Get-Partition -DiskId $_.Path
    $DriveLetter = $PartitionsData.DriveLetter | Where-object { $_ -notin @("",
 $null) }
    $VolumeName = (Get-PSDrive | Where-Object { $_.Name -in
 @($DriveLetter) }).Description | Where-object { $_ -notin @("", $null) }
  }
  If ($DiskDrive.path -like "*PROD_PVDISK*") {
    $BlockDeviceName = Convert-SCSITargetIdToDeviceName((Get-WmiObject -Class
 Win32_Diskdrive | Where-Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" +
 $DiskDrive.Number) }).SCSITargetId)
    $BlockDeviceName = "/dev/" + $BlockDeviceName
    $BlockDevice = $BlockDeviceMappings | Where-Object { $BlockDeviceName -like "*"
 + $_.DeviceName + "*" }
    $EbsVolumeID = $BlockDevice.Ebs.VolumeId
```

```
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -
eq $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON_EC2_NVME*") {
    $BlockDeviceName = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping")."ephemeral$((Get-WmiObject -Class Win32_Diskdrive | Where-
Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" + $DiskDrive.Number) }).SCSIPort - 2)"
    $BlockDevice = $null
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -
eq $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
  }
  ElseIf ($DiskDrive.path -like "*NETAPP*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $EbsVolumeID = "FSxN Volume"
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
  }
  Else {
    $BlockDeviceName = $null
```

```
    $BlockDevice = $null
  }
  New-Object PSObject -Property @{
    Disk          = $Disk;
    Partitions    = $Partitions;
    DriveLetter   = If ($DriveLetter -eq $null) { "N/A" } Else { $DriveLetter };
    EbsVolumeId   = If ($EbsVolumeID -eq $null) { "N/A" } Else { $EbsVolumeID };
    Device        = If ($BlockDeviceName -eq $null) { "N/A" } Else
 { $BlockDeviceName };
    VirtualDevice = If ($VirtualDevice -eq $null) { "N/A" } Else { $VirtualDevice };
    VolumeName    = If ($VolumeName -eq $null) { "N/A" } Else { $VolumeName };
    DeviceName    = If ($DeviceName -eq $null) { "N/A" } Else { $DeviceName };
  }
} | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, DeviceName, VolumeName
```

Eseguire lo script come segue:

```
PS C:\> .\mapping.ps1
```

Di seguito è riportato un output di esempio.

```
Disk  Partitions  DriveLetter   EbsVolumeId             Device      VirtualDevice
 DeviceName              VolumeName
----  ----------  -----------   -----------             ------      -------------
 ----------              ----------
   0           1            C   vol-0561f1783298efedd   /dev/sda1   N/A
 NVMe Amazon Elastic B   N/A
   1           1            D   vol-002a9488504c5e35a   xvdb        N/A
 NVMe Amazon Elastic B   N/A
   2           1            E   vol-0de9d46fcc907925d   xvdc        N/A
 NVMe Amazon Elastic B   N/A
```

Se non hai fornito le tue credenziali sull'istanza Windows, lo script non può ottenere l'ID del volume EBS e gli usi N/A nella `EbsVolumeId` colonna.

Mappare i dischi non NVMe ai volumi

Il driver del dispositivo a blocchi dell'istanza assegna i nomi del volume effettivi durante il montaggio dei volumi.

Mappature

- Volumi di archivio dell'istanza
- Volumi EBS

Volumi di archivio dell'istanza

La tabella seguente descrive come i driver Citrix PV e AWS PV mappano i volumi di archiviazione delle istanze non NVMe ai volumi Windows. Il numero di volumi instance store disponibili è determinato dal tipo di istanza. Per ulteriori informazioni, consulta Limiti di volume di archivio dell'istanza per le istanze EC2.

Ubicazione	Nome dispositivo
Bus Number 0, Target ID 78, LUN 0	xvdca
Bus Number 0, Target ID 79, LUN 0	xvdcb
Bus Number 0, Target ID 80, LUN 0	xvdcc
Bus Number 0, Target ID 81, LUN 0	xvdcd
Bus Number 0, Target ID 82, LUN 0	xvdce
Bus Number 0, Target ID 83, LUN 0	xvdcf
Bus Number 0, Target ID 84, LUN 0	xvdcg
Bus Number 0, Target ID 85, LUN 0	xvdch
Bus Number 0, Target ID 86, LUN 0	xvdci
Bus Number 0, Target ID 87, LUN 0	xvdcj
Bus Number 0, Target ID 88, LUN 0	xvdck
Bus Number 0, Target ID 89, LUN 0	xvdcl

Volumi EBS

La tabella seguente descrive come i driver Citrix PV e AWS PV mappano i volumi EBS non NVMe ai volumi Windows.

Location (Ubicazione)	Nome dispositivo
Bus Number 0, Target ID 0, LUN 0	/dev/sda1
Bus Number 0, Target ID 1, LUN 0	xvdb
Bus Number 0, Target ID 2, LUN 0	xvdc
Bus Number 0, Target ID 3, LUN 0	xvdd
Bus Number 0, Target ID 4, LUN 0	xvde
Bus Number 0, Target ID 5, LUN 0	xvdf
Bus Number 0, Target ID 6, LUN 0	xvdg
Bus Number 0, Target ID 7, LUN 0	xvdh
Bus Number 0, Target ID 8, LUN 0	xvdi
Bus Number 0, Target ID 9, LUN 0	xvdj
Bus Number 0, Target ID 10, LUN 0	xvdk
Bus Number 0, Target ID 11, LUN 0	xvdl
Bus Number 0, Target ID 12, LUN 0	xvdm
Bus Number 0, Target ID 13, LUN 0	xvdn
Bus Number 0, Target ID 14, LUN 0	xvdo
Bus Number 0, Target ID 15, LUN 0	xvdp
Bus Number 0, Target ID 16, LUN 0	xvdq
Bus Number 0, Target ID 17, LUN 0	xvdr

Location (Ubicazione)	Nome dispositivo
Bus Number 0, Target ID 18, LUN 0	xvds
Bus Number 0, Target ID 19, LUN 0	xvdt
Bus Number 0, Target ID 20, LUN 0	xvdu
Bus Number 0, Target ID 21, LUN 0	xvdv
Bus Number 0, Target ID 22, LUN 0	xvdw
Bus Number 0, Target ID 23, LUN 0	xvdx
Bus Number 0, Target ID 24, LUN 0	xvdy
Bus Number 0, Target ID 25, LUN 0	xvdz

Prevenzione delle distorsioni di scrittura sulle istanze Amazon EC2 di Linux

> **Note**
>
> La prevenzione delle scritture danneggiate è supportata solo per le istanze Linux.

La prevenzione della scrittura danneggiata è una funzionalità di storage a blocchi progettata AWS per migliorare le prestazioni dei carichi di lavoro dei database I/O-intensive relazionali e ridurre la latenza senza influire negativamente sulla resilienza dei dati. I database relazionali che utilizzano InnoDB o XtraDB come motore di database, come MySQL e MariaDB, trarranno vantaggio dalla prevenzione delle distorsioni di scrittura.

In genere, i database relazionali che utilizzano pagine più grandi dell'atomicità in caso di interruzione dell'alimentazione del dispositivo di archiviazione utilizzano meccanismi di registrazione dei dati per proteggersi dalle distorsioni di scrittura. MariaDB e MySQL utilizzano un file buffer di doppia scrittura per registrare i dati prima di scriverli nelle tabelle di dati. In caso di scritture incomplete o errate a causa di arresti anomali del sistema operativo o di interruzione dell'alimentazione durante le transazioni di scrittura, il database può recuperare i dati dal buffer di doppia scrittura. L' I/O overhead

aggiuntivo associato alla scrittura nel buffer di doppia scrittura influisce sulle prestazioni del database e sulla latenza delle applicazioni e riduce il numero di transazioni che possono essere elaborate al secondo. Per ulteriori informazioni sul buffer di doppia scrittura, consulta la documentazione di MariaDB e MySQL.

Con la prevenzione delle distorsioni di scrittura, i dati vengono scritti nell'archivio in transazioni di scrittura tutto o niente, il che elimina la necessità di utilizzare il buffer di doppia scrittura. Ciò impedisce che dati parziali o incompleti vengano scritti nell'archivio in caso di arresti anomali del sistema operativo o di interruzione dell'alimentazione durante le transazioni di scrittura. È possibile aumentare il numero di transazioni elaborate al secondo fino a un massimo del 30 percento e ridurre la latenza di scrittura fino a un massimo del 50 percento senza compromettere la resilienza dei carichi di lavoro.

Prezzi

L'utilizzo della prevenzione delle distorsioni di scrittura non prevede costi aggiuntivi.

Indice

- Dimensioni dei blocchi per la prevenzione delle distorsioni di scrittura su Amazon EC2
- Requisiti per l'utilizzo della prevenzione delle distorsioni di scrittura su Amazon EC2
- Verifica il supporto dell'istanza Amazon EC2 per la prevenzione delle distorsioni di scrittura
- Configura il carico di lavoro su Amazon EC2 per la prevenzione delle distorsioni di scrittura

Dimensioni dei blocchi per la prevenzione delle distorsioni di scrittura su Amazon EC2

La prevenzione delle distorsioni di scrittura supporta operazioni di scrittura per blocchi di dati da 4 KiB, 8 KiB e 16 KiB. L'indirizzo del blocco logico (LBA) di inizio del blocco di dati deve essere allineato alla rispettiva dimensione del limite del blocco di 4 KiB, 8 KiB o 16 KiB. Ad esempio, per le operazioni di scrittura da 16 KiB, l'LBA di inizio del blocco di dati deve essere allineato a una dimensione del limite del blocco di 16 KiB.

La tabella seguente mostra il supporto per tutti i tipi di archiviazione e di istanza.

	Blocchi da 4 KiB	Blocchi da 8 KiB	Blocchi da 16 KiB
Volumi di archivio dell'istanza	Tutte le istanze NVMe archiviano i volumi collegati alle istanze di generazione corrente. I-family	Istanze i4i, iM4GN, iS4Gen, i7i, i7IE, i8G e i8GE supportate da Nitro SSD. AWS	
Volumi Amazon EBS	Tutti i volumi Amazon Nitro-based EBS collegati alle istanze.		

Per verificare se l'istanza e il volume supportano la prevenzione delle distorsioni di scrittura, esegui una query per verificare se l'istanza supporta la funzionalità e altri dettagli, come le dimensioni dei blocchi e dei limiti supportate. Per ulteriori informazioni, consulta Verifica il supporto dell'istanza Amazon EC2 per la prevenzione delle distorsioni di scrittura.

Requisiti per l'utilizzo della prevenzione delle distorsioni di scrittura su Amazon EC2

Affinché la prevenzione delle scritture anomale funzioni correttamente, un' I/O operazione deve soddisfare i requisiti di dimensione, allineamento e limiti, come specificato nei campi,,. `NTWPU` `NTWGU` `NTWBU` È necessario configurare il sistema operativo per garantire che lo specifico sottosistema di storage (file system, LVM, RAID, ecc.) non modifichi I/O le proprietà dello stack di storage, incluse le unioni di blocchi, le suddivisioni o il trasferimento degli indirizzi a blocchi, prima di essere inviato al dispositivo.

La prevenzione delle distorsioni di scrittura è stata testata con la seguente configurazione:

- Un tipo di istanza e un tipo di archiviazione che supportano la dimensione del blocco richiesta.
- Amazon Linux 2 con versione del kernel 5.10 o successiva.
- ext4 con la funzione `bigalloc` abilitata, una dimensione del cluster di 16 KiB e le utilità ext4 più recenti (e2fsprogs 1.46.5 o versioni successive).
- Modalità di accesso ai file `O_DIRECT` per bypassare la cache del buffer del kernel Linux.

> **Note**
>
> Non è necessario disabilitare la I/O fusione per i carichi di lavoro MySQL e MariaDB.

Verifica il supporto dell'istanza Amazon EC2 per la prevenzione delle distorsioni di scrittura

Per verificare se l'istanza e il volume supportano la prevenzione delle scritture strappate e per visualizzare i dati specifici del fornitore dello spazio dei nomi NVMe che contengono informazioni sulla prevenzione delle scritture danneggiate, utilizzate il seguente comando.

```
$ sudo nvme id-ns -v device_name
```

> **Note**
>
> Il comando restituisce le informazioni specifiche del fornitore in formato esadecimale con interpretazione ASCII. Nelle applicazioni potrebbe essere necessario creare uno strumento simile a `ebsnvme-id` che sia in grado di leggere e analizzare l'output.

Ad esempio, il comando seguente restituisce i dati specifici del fornitore dello spazio dei nomi NVMe che contengono informazioni sulla prevenzione della scrittura danneggiata per. `/dev/nvme1n1`

```
$ sudo nvme id-ns -v /dev/nvme1n1
```

Se l'istanza e il volume supportano la prevenzione delle scritture danneggiate, vengono restituite le seguenti informazioni sulla prevenzione delle scritture danneggiate nei dati specifici del fornitore dello spazio AWS dei nomi NVMe.

> **Note**
>
> I byte nella tabella seguente rappresentano l'offset in byte rispetto all'inizio dei dati specifici del fornitore dello spazio dei nomi NVMe.

Byte	Description
0:31	Il nome del punto di montaggio del dispositivo, ad esempio /dev/xvda . Lo fornisci durante la richiesta di collegamenti al volume e può essere utilizzato dall'istanza Amazon EC2 per creare un collegamento simbolico al dispositivo a blocchi NVMe (nvmeXn1).
32:63	L'ID del volume. Ad esempio, vol01234567890abcdef . Questo campo può essere utilizzato per mappare il dispositivo NVMe al volume collegato.
64:255	Riservato per uso futuro.
256:257	Dimensione dell'unità di prevenzione delle distorsioni di scrittura del namespace (NTWPU). Questo campo indica la dimensione specifica del namespace dell'operazione di scrittura garantita per la scrittura atomica sulla NVM durante un'interruzione di corrente o una condizione di errore. Il campo è specificato in blocchi logici rappresentati in valori a base zero.
258:259	Dimensione della granularità di prevenzione delle distorsioni di scrittura del namespace (NTWPU). Questo campo indica gli incrementi di dimensione specifici del namespace al di sotto di NTWPU dell'oper azione di scrittura garantita per la scrittura atomica sulla NVM durante un'interruzione di corrente o una condizione di errore. Cioè, la dimension e dovrebbe essere NTWPG * n <= NTWPU dove n è un numero intero positivo. Anche l'offset dell'LBA dell'operazione di scrittura deve essere allineato a questo campo. Il campo è specificato in blocchi logici rappresentati in valori a base zero.
260:263	Dimensione del limite di prevenzione delle distorsioni di scrittura del namespace (NTWPU). Questo campo indica la dimensione del limite atomico per questo namespace per il valore NTWPU. Non è garantito che le scritture che superano i limiti atomici su questo namespace vengano scritte atomicamente sulla NVM durante un'interruzione di corrente o una condizione di errore. Il valore di 0h indica che non esistono limiti atomici per le interruzioni di corrente o le condizioni di errore. Tutti gli altri

Byte	Description
	valori specificano una dimensione in termini di blocchi logici utilizzando la stessa codifica del campo NTWPU.

Configura il carico di lavoro su Amazon EC2 per la prevenzione delle distorsioni di scrittura

La prevenzione delle distorsioni di scrittura è abilitata per impostazione predefinita sui tipi di istanze supportati con volumi supportati. Non è necessario configurare alcuna impostazione aggiuntiva per abilitare la prevenzione delle scritture danneggiate.

> **Note**
>
> I carichi di lavoro che non supportano la prevenzione delle scritture errate non hanno alcun impatto sulle prestazioni. Non è necessario apportare modifiche per questi carichi di lavoro. I carichi di lavoro che supportano la prevenzione delle scritture danneggiate, ma non sono configurati per utilizzarla, continuano a utilizzare il buffer doublewrite e non ricevono alcun vantaggio in termini di prestazioni.

Per configurare lo stack software MySQL o MariaDB in modo da disabilitare il buffer di doppia scrittura e utilizzare la prevenzione delle distorsioni di scrittura, completa i seguenti passaggi:

1. Configura il tuo volume per utilizzare il file system ext4 con l' BigAlloc opzione e imposta la dimensione del cluster su 4 KiB, 8 KiB o 16 KiB. L'utilizzo BigAlloc con una dimensione del cluster di 4 KiB, 8 KiB o 16 KiB garantisce che il file system allochi i file che si allineano con il rispettivo limite.

   ```
   $  mkfs.ext4 -O bigalloc -C 4096|8192|16384 device_name
   ```

   > **Note**
   >
   > Per MySQL e MariaDB, è necessario utilizzare `-C 16384` per eguagliare la dimensione della pagina del database. L'impostazione della granularità di allocazione su un valore diverso da un multiplo della dimensione della pagina può comportare allocazioni che

potrebbero non corrispondere ai limiti di prevenzione delle distorsioni di scrittura del dispositivo di archiviazione.

Ad esempio:

```
$  mkfs.ext4 -O bigalloc -C 16384 /dev/nvme1n1
```

2. Configura InnoDB per l'utilizzo del metodo di svuotamento `O_DIRECT` e disattiva la doppia scrittura di InnoDB. Utilizza un editor di testo per aprire `/etc/my.cnf` e modifica i parametri `innodb_flush_method` e `innodb_doublewrite` come segue:

```
innodb_flush_method=O_DIRECT
innodb_doublewrite=0
```

Important

Se utilizzi Logical Volume Manager (LVM) o un altro livello di virtualizzazione dell'archiviazione, assicurati che gli offset iniziali dei volumi siano allineati su multipli di 16 KiB. Ciò è relativo all'archiviazione NVMe sottostante, che deve tenere conto delle intestazioni dei metadati e dei superblocchi utilizzati dal livello di virtualizzazione dell'archiviazione. L'aggiunta di un offset al volume fisico LVM può causare un disallineamento tra le allocazioni del file system e gli offset del dispositivo NVMe, il che invaliderebbe la prevenzione delle distorsioni di scrittura. Per ulteriori informazioni, consulta la sezione `--dataalignmentoffset` nella pagina del manuale Linux.

Snapshot Amazon EBS coerenti a livello di applicazione basati su Windows VSS

Puoi creare snapshot coerenti a livello di applicazione di tutti i volumi Amazon EBS collegati alle istanze Amazon EC2 di Windows utilizzando AWS Systems Manager Run Command. Il processo di istantanea utilizza il servizio Windows Volume Shadow Copy Service (VSS) per eseguire backup a livello di volume EBS delle applicazioni. VSS-aware Gli snapshot includono dati delle transazioni in sospeso tra queste applicazioni e il disco. Non è necessario arrestare le istanze o scollegarle per eseguire il backup di tutti i volumi collegati.

L'utilizzo di snapshot EBS basate su tecnologia VSS non comporta costi supplementari. Paghi solo gli snapshot EBS creati dal processo di backup. Per ulteriori informazioni, consulta Come mi vengono fatturati i miei snapshot di Amazon EBS?

> **Note**
>
> Gli snapshot basati su Windows VSS coerenti a livello di applicazione sono supportati solo con le istanze Windows.

Indice

- Cos'è VSS?
- Come funziona la soluzione con snapshot Amazon EBS basati su VSS
- Prerequisiti per creare snapshot EBS basati su Windows VSS
- Crea snapshot EBS basati su VSS per l'istanza EC2 Windows
- Risolvere problemi relativi agli snapshot EBS basati su Windows VSS
- Usa il AWS Soluzione VSS per ripristinare i dati per la tua istanza
- AWS Cronologia delle versioni della soluzione VSS

Cos'è VSS?

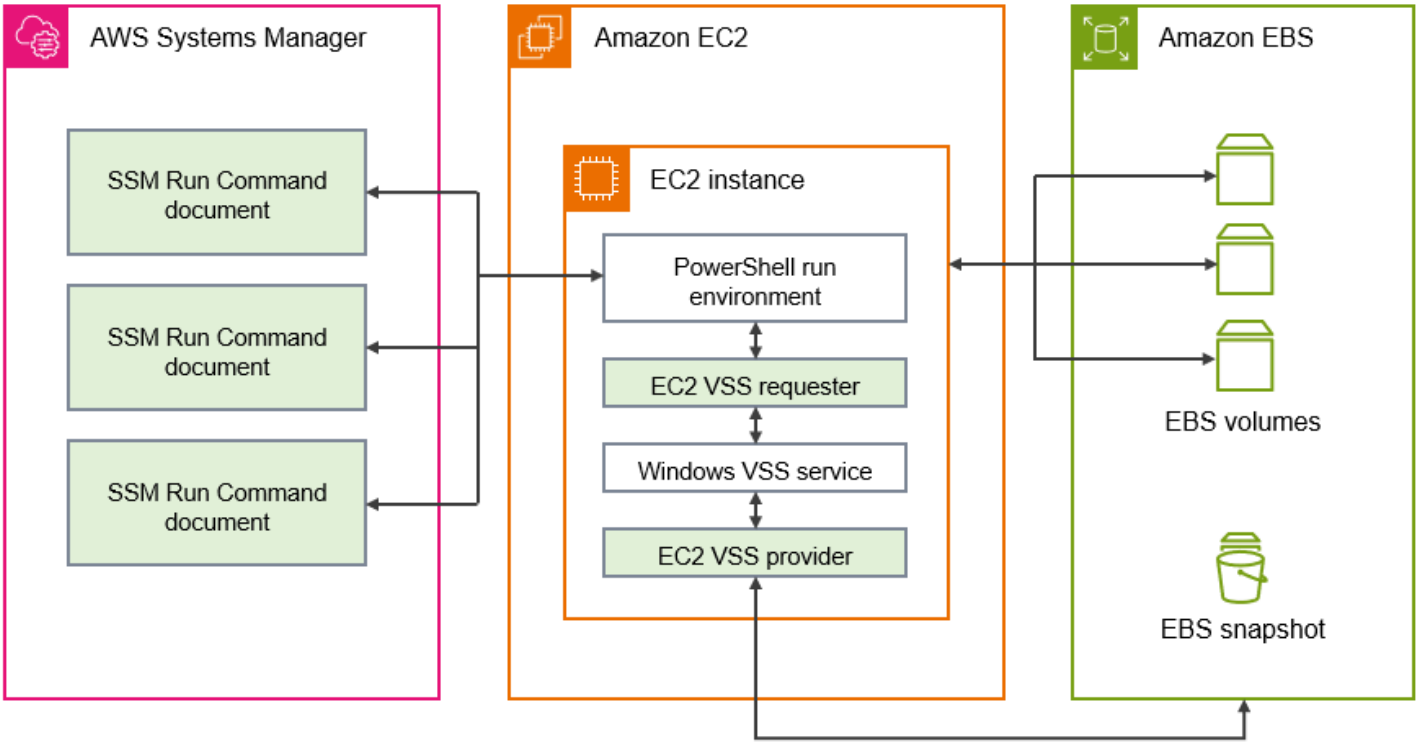
Volume Shadow Copy Service (VSS) è una tecnologia di backup e ripristino inclusa in Microsoft Windows. Può creare copie di backup, o snapshot, di file o volumi di computer mentre sono in uso. Per ulteriori informazioni, consulta la pagina Volume Shadow Copy Service.

Per creare uno snapshot coerente con l'applicazione, sono necessari i seguenti componenti software.

- Servizio VSS: parte del sistema operativo Windows
- Richiedente VSS: il software che richiede la creazione di copie shadow
- Scrittore VSS: in genere fornito come parte di un'applicazione, come SQL Server, per garantire la coerenza del set di dati di cui eseguire il backup
- Fornitore VSS: il componente che crea le copie shadow dei volumi sottostanti

La soluzione con snapshot Amazon EBS basati su Windows VSS è costituita da più documenti Systems Manager (SSM) Run Command, che facilitano la creazione di backup, e un pacchetto

Systems Manager Distributor, chiamato `AwsVssComponents`, che include un richiedente EC2 VSS e un fornitore EC2 VSS. Per acquisire snapshot dei volumi EBS coerenti con l'applicazione, sulle istanze Windows di EC2 deve essere installato il pacchetto `AwsVssComponents`. Il diagramma seguente illustra la relazione tra questi componenti software.



Come funziona la soluzione con snapshot Amazon EBS basati su VSS

Di seguito è illustrata la procedura di creazione di script di snapshot EBS basati su tecnologia VSS coerenti a livello di applicazione.

1. Completa Prerequisiti per creare snapshot EBS basati su Windows VSS.
2. Inserire i parametri per il documento SSM `AWSEC2-VssInstallAndSnapshot` per poi eseguirlo tramite Run Command. Per ulteriori informazioni, consulta Esegui il documento di AWSEC2-VssInstallAndSnapshot comando (consigliato).
3. Il servizio Windows VSS sull'istanza coordina tutte le I/O operazioni in corso per l'esecuzione delle applicazioni.
4. Il sistema svuota tutti i I/O buffer e sospende temporaneamente tutte le operazioni. I/O La sospensione dura al massimo dieci secondi.
5. In questo lasso di tempo, il sistema crea gli snapshot di tutti i volumi associati all'istanza.
6. La pausa viene annullata e riprende il funzionamento. I/O

7. Il sistema aggiunge tutti gli snapshot appena creati all'elenco degli snapshot di EBS. Il sistema contrassegna tutte le istantanee EBS basate su VSS create con successo da questo processo con. AppConsistent:true
8. Se è necessario eseguire il ripristino da uno snapshot, è possibile utilizzare il processo EBS standard di creazione di un volume da uno snapshot. In alternativa, è possibile ripristinare tutti i volumi su un'istanza utilizzando uno script di esempio, illustrato in Usa il AWS Soluzione VSS per ripristinare i dati per la tua istanza.

Prerequisiti per creare snapshot EBS basati su Windows VSS

Puoi creare istantanee EBS basate su VSS con Systems Manager Run Command o Amazon Data Lifecycle AWS Backup Manager. I seguenti prerequisiti si applicano a tutte le soluzioni.

Requisiti di sistema

Assicurati che la tua istanza EC2 per Windows soddisfi tutti i requisiti di sistema per creare istantanee basate su VSS, incluse le versioni supportate del sistema operativo Windows, del framework.NET e dell'agente. PowerShell AWS Tools for Windows PowerShell AWS Systems Manager

autorizzazioni IAM

Il ruolo IAM collegato all'istanza Amazon EC2 Windows deve avere l'autorizzazione a creare snapshot coerenti a livello di applicazione con VSS. Per concedere le autorizzazioni necessarie, puoi allegare la policy gestita da `AWSEC2VssSnapshotPolicy` al profilo dell'istanza.

Componenti VSS

Per creare snapshot coerenti a livello di applicazione sui sistemi operativi Windows, il pacchetto `AwsVssComponents` deve essere installato nell'istanza. Il pacchetto contiene un agente VSS su istanza EC2 che funge da richiedente VSS e un fornitore VSS di EC2 per i volumi EBS.

Requisiti di sistema

Installazione di Agente Systems Manager

VSS è orchestrato dal Systems Manager Agent utilizzando. PowerShell Assicurati di aver installato la versione dell'agente SSM `3.0.502.0` o successiva sull'istanza EC2. Se utilizzi una versione obsoleta dell'agente SSM, puoi effettuare l'aggiornamento tramite Run Command. Per

ulteriori informazioni, consulta le pagine Setting up Systems Manager for Amazon EC2 instances e Working with SSM Agent on Amazon EC2 instances for Windows Server della Guida per l'utente di AWS Systems Manager .

Requisiti di un'istanza Windows di Amazon EC2

Gli snapshot EBS basati su VSS sono supportati dalle istanze che eseguono Windows Server 2016 o versioni successive.

Versione .NET Framework

Il pacchetto `AwsVssComponents` richiede .NET Framework versione `4.6` o successive. Le versioni del sistema operativo Windows precedenti a Windows Server 2016 utilizzano per impostazione predefinita una versione precedente di. NET Framework. Se l'istanza utilizza una versione precedente di. NET Framework, devi installare la versione `4.6` o una versione successiva che usa Windows Update.

AWS Tools for Windows PowerShell versione

Assicurati che la tua istanza stia eseguendo AWS Tools for Windows PowerShell una versione `3.3.48.0` o successiva. Per verificare la tua versione, esegui il seguente comando nel PowerShell terminale dell'istanza.

```
C:\> Get-AWSPowerShellVersion
```

Se devi eseguire l'aggiornamento AWS Tools for Windows PowerShell sulla tua istanza, consulta Installazione AWS Tools for Windows PowerShell nella Guida per l'AWS Strumenti per PowerShell utente.

PowerShell Versione per Windows

Assicurati che sulla tua istanza sia in esecuzione la versione PowerShell principale di Windows `3`4,, o`5`. Per verificare la tua versione, esegui il seguente comando in un PowerShell terminale sull'istanza.

```
C:\> $PSVersionTable.PSVersion
```

PowerShell modalità linguistica

Assicurati che la modalità PowerShell lingua dell'istanza sia impostata su`FullLanguage`. Per ulteriori informazioni, consulta about_ Language_Modes nella documentazione Microsoft.

Utilizza una policy gestita da IAM per concedere le autorizzazioni per gli snapshot basati su VSS

La policy gestita AWSEC2VssSnapshotPolicy consente a Systems Manager di eseguire le seguenti azioni sull'istanza di Windows:

- Crea e applica tag agli snapshot EBS
- Creare ed etichettare Amazon Machine Images (AMIs)
- collega metadati, come ad esempio l'ID dispositivo, ai tag degli snapshot predefiniti creati da VSS.

In questo argomento vengono illustrati i dettagli delle autorizzazioni per la policy gestita da VSS e come collegarla al ruolo IAM del profilo dell'istanza EC2.

Indice

- AWSEC2VssSnapshotPolicy dettagli della politica gestita
- Collega la policy gestita degli snapshot VSS al ruolo del profilo dell'istanza

AWSEC2VssSnapshotPolicy dettagli della politica gestita

Una politica AWS gestita è una politica autonoma che Amazon fornisce ai AWS clienti. AWS le politiche gestite sono progettate per concedere autorizzazioni per casi d'uso comuni. Non è possibile modificare le autorizzazioni definite nelle politiche AWS gestite. Tuttavia, è possibile copiare la policy e utilizzarla come base per una policy gestita dal cliente per il caso d'uso specifico.

Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

Per utilizzare la policy gestita da AWSEC2VssSnapshotPolicy, puoi collegarla al ruolo IAM associato alle istanze Windows EC2. Questa policy consente alla soluzione VSS EC2 di creare e aggiungere tag ad Amazon Machine Images (AMIs) e EBS Snapshots. Per collegare la policy, consultare Collega la policy gestita degli snapshot VSS al ruolo del profilo dell'istanza.

Autorizzazioni concesse da AWSEC2VssSnapshotPolicy

La policy AWSEC2VssSnapshotPolicy include le seguenti autorizzazioni Amazon EC2 per consentire ad Amazon EC2 di creare e gestire snapshot VSS per tuo conto. Puoi collegare questa policy gestita al ruolo del profilo dell'istanza IAM che usi per le istanze EC2 Windows.

- ec2: CreateTags — Aggiungi tag agli snapshot EBS e aiuta a identificare e AMIs classificare le risorse.
- ec2: DescribeInstanceAttribute — Recupera i volumi EBS e le corrispondenti mappature dei dispositivi a blocchi collegati all'istanza di destinazione.
- ec2: CreateSnapshots — Crea istantanee dei volumi EBS.
- ec2: CreateImage — Crea un AMI da un'istanza EC2 in esecuzione.
- ec2: DescribeImages — Recupera le informazioni per EC2 e le istantanee. AMIs
- ec2: DescribeSnapshots — Determina l'ora e lo stato di creazione delle istantanee per verificare la coerenza dell'applicazione.

> **Note**
>
> Per vedere le autorizzazioni per questa policy, consulta AWSEC2VssSnapshotPolicy nella Guida di riferimento sulle policy gestite da AWS .

Semplifica le autorizzazioni per casi d'uso specifici: avanzate

La policy gestita `AWSEC2VssSnapshotPolicy` include le autorizzazioni per tutti i modi in cui è possibile creare snapshot basati su VSS. È possibile creare una policy personalizzata che include solo le autorizzazioni necessarie.

Caso d'uso: creazione di AMI, caso d'uso: AWS Backup servizio di utilizzo

Se si utilizza esclusivamente l'`CreateAmi`opzione o se si creano istantanee basate su VSS solo tramite il AWS Backup servizio, è possibile semplificare le dichiarazioni politiche come segue.

- Omettete le dichiarazioni politiche identificate dalla seguente dichiarazione (): IDs SIDs
  - `CreateSnapshotsWithTag`
  - `CreateSnapshotsAccessInstance`
  - `CreateSnapshotsAccessVolume`
- Modifica l'istruzione `CreateTagsOnResourceCreation` come segue:
  - Rimuovi `arn:aws:ec2:*:*:snapshot/*` dalle risorse.
  - Rimuovi `CreateSnapshots` dalla condizione `ec2:CreateAction`.
- Modifica l'istruzione `CreateTagsAfterResourceCreation` per rimuovere `arn:aws:ec2:*:*:snapshot/*` dalle risorse.

- Modifica l'istruzione `DescribeImagesAndSnapshots` per rimuovere `ec2:DescribeSnapshots` dall'azione presente nell'istruzione.

Caso d'uso: solo snapshot

Se non si utilizza l'opzione `CreateAmi`, è possibile semplificare le istruzioni della policy come segue.

- Omettete le dichiarazioni politiche identificate dalla seguente dichiarazione IDs ()SIDs:
  - `CreateImageAccessInstance`
  - `CreateImageWithTag`
- Modifica l'istruzione `CreateTagsOnResourceCreation` come segue:
  - Rimuovi `arn:aws:ec2:*:*:image/*` dalle risorse.
  - Rimuovi `CreateImage` dalla condizione `ec2:CreateAction`.
- Modifica l'istruzione `CreateTagsAfterResourceCreation` per rimuovere `arn:aws:ec2:*:*:image/*` dalle risorse.
- Modifica l'istruzione `DescribeImagesAndSnapshots` per rimuovere `ec2:DescribeImages` dall'azione presente nell'istruzione.

> **Note**
>
> Per garantire che la policy personalizzata funzioni come previsto, si consiglia di rivedere e incorporare regolarmente gli aggiornamenti alla policy gestita.

Collega la policy gestita degli snapshot VSS al ruolo del profilo dell'istanza

Per concedere le autorizzazioni per gli snapshot basati su VSS per l'istanza EC2 Windows, puoi collegare la policy gestita da AWSEC2VssSnapshotPolicy al ruolo del profilo dell'istanza come segue. È importante assicurarsi che l'istanza soddisfi tutti i Requisiti di sistema.

> **Note**
>
> Per utilizzare la policy gestita, sull'istanza deve essere installata la versione `2.3.1` o successiva del pacchetto `AwsVssComponents`. Per la cronologia delle versioni, consulta AwsVssComponents versioni del pacchetto.

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Ruoli per visualizzare un elenco di ruoli IAM a cui hai accesso.
3. Seleziona il link al Nome ruolo associato all'istanza. Si apre la pagina dei dettagli del ruolo.
4. Per collegare la policy gestita, scegli Aggiungi autorizzazioni, che si trova nell'angolo in alto a destra del pannello dell'elenco. Quindi dall'elenco a discesa seleziona Collega policy.
5. Per semplificare i risultati, inserisci il nome della policy nella barra di ricerca (`AWSEC2VssSnapshotPolicy`).
6. Seleziona la casella di controllo accanto al nome della policy da collegare, quindi scegli Aggiungi autorizzazioni.

Gestisci il pacchetto di componenti VSS per gli snapshot EBS basati su Windows VSS

Prima di creare snapshot EBS basati su VSS, assicurati di avere installata la versione più recente del pacchetto di componenti VSS sull'istanza Windows. È possibile installare il pacchetto `AwsVssComponents` su un'istanza esistente in diversi modi:

- (Consigliato) Esegui il documento di AWSEC2-VssInstallAndSnapshot comando (consigliato). In questo modo il componente si installa o si aggiorna automaticamente a ogni esecuzione.
- Installazione manuale dei componenti VSS su un'istanza di Windows EC2.
- Aggiorna il pacchetto di componenti VSS sull'istanza di Windows EC2.

È anche possibile creare un'AMI con EC2 Image Builder che utilizzi il componente gestito `aws-vss-components-windows` per installare il pacchetto `AwsVssComponents` per l'immagine. Il componente gestito utilizza AWS Systems Manager Distributor per installare il pacchetto. Dopo la creazione dell'immagine con Image Builder, ogni istanza avviata dall'AMI associata avrà il pacchetto VSS installato. Per ulteriori informazioni su come creare un'AMI con installato il pacchetto VSS, consulta Distributor package managed components for Windows nella Guida per l'utente di EC2 Image Builder.

Indice

- Installazione manuale dei componenti VSS su un'istanza di Windows EC2
- Aggiorna il pacchetto di componenti VSS sull'istanza di Windows EC2

Installazione manuale dei componenti VSS su un'istanza di Windows EC2

L'istanza Windows di EC2 deve avere installati i componenti VSS prima di poter creare snapshot coerenti a livello di applicazione con Systems Manager. Se non si esegue il documento di comando `AWSEC2-VssInstallAndSnapshot` per installare o aggiornare il pacchetto ogni volta che si creano snapshot coerenti a livello di applicazione, è necessario installare manualmente il pacchetto.

È necessario eseguire l'installazione manuale anche se si prevede di utilizzare uno dei seguenti metodi per creare snapshot coerenti a livello di applicazione dall'istanza EC2.

- Crea istantanee VSS utilizzando AWS Backup
- Creazione di snapshot VSS mediante Amazon Data Lifecycle Manager

Se è necessario eseguire un'installazione manuale, si consiglia di utilizzare il pacchetto di componenti AWS VSS più recente per migliorare l'affidabilità e le prestazioni delle istantanee coerenti con le applicazioni sulle istanze EC2 Windows.

> **Note**
>
> Per installare o aggiornare automaticamente il pacchetto `AwsVssComponents` ogni volta che si creano snapshot coerenti con l'applicazione, si consiglia di utilizzare Systems Manager per eseguire il documento `AWSEC2-VssInstallAndSnapshot`. Per ulteriori informazioni, consulta Esegui il documento di AWSEC2-VssInstallAndSnapshot comando (consigliato).

Per installare i componenti VSS su un'istanza Windows di Amazon EC2, segui i passaggi per il tuo ambiente preferito.

Console

Installazione dei componenti VSS utilizzando SSM Distributor

1. Apri la console all'indirizzo. AWS Systems Manager https://console.aws.amazon.com/systems-manager/
2. Nel riquadro di navigazione selezionare Run Command.
3. Selezionare Run command.
4. Per il documento Command, scegli il pulsante accanto a AWS-ConfigureAWSPackage.
5. In Command parameters (Parametri di comando), effettuare le seguenti operazioni:

a. Verificare che Action (Operazione) sia impostata su Install (Installa).

b. In Name (Nome), immettere `AwsVssComponents`.

c. In Versione, lascia vuoto il campo per consentire a Systems Manager di installare l'ultima versione.

6. In Targets (Destinazioni), identificare le istanze in cui si desidera eseguire questa operazione specificando i tag o selezionando le istanze manualmente.

> **Note**
>
> Se scegli di selezionare manualmente le istanze e l'istanza prevista non è inclusa nell'elenco, consulta Dove sono le mie istanze? nella Guida per l'utente di AWS Systems Manager per suggerimenti sulla risoluzione dei problemi.

7. In Other parameters (Altri parametri):

- (Opzionale) In Comment (Commento) digitare le informazioni su questo comando.
- In Timeout (seconds) (Timeout [secondi]), specificare il numero di secondi che il sistema dovrà aspettare prima di generare un errore per l'intera esecuzione del comando.

8. (Facoltativo) In Rate control (Controllo velocità):

- In Concurrency (Simultaneità), specificare un numero o una percentuale di istanze su cui eseguire contemporaneamente il comando.

> **Note**
>
> Se le destinazioni sono state selezionate scegliendo i tag Amazon EC2 e non si conosce il numero di istanze utilizzate dai tag selezionati, limitare il numero di istanze che possono eseguire il documento contemporaneamente specificando una percentuale.

- In Error threshold (Soglia di errore) specificare quando interrompere l'esecuzione del comando sulle altre istanze dopo un errore su un numero o una percentuale di istanze. Se ad esempio si specificano 3 errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche le istanze che elaborano ancora il comando potrebbero inviare errori.

9. (Opzionale) Nella sezione Output options (Opzioni di output), se si desidera salvare l'output del comando in un file, selezionare la casella accanto a Enable writing to an S3 bucket (Abilita la scrittura in un bucket S3). Specificare i nomi del bucket e (opzionale) del prefisso (cartella).

   > **Note**
   >
   > Le autorizzazioni S3 che assegnano la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza e non quelle dell'utente che esegue questa attività. Per ulteriori informazioni, consulta Configure EC2 instance permissions nella Guida per l'utente AWS Systems Manager .

10. (Opzionale) Specificare le opzioni per SNS notifications (Notifiche SNS).

    Per informazioni sulla configurazione di notifiche Amazon SNS per Run Command, consultare Configurazione delle notifiche Amazon SNS per AWS Systems Manager.

11. Scegli Esegui.

AWS CLI

La seguente procedura consente di scaricare e installare il pacchetto `AwsVssComponents` sulle istanze utilizzando Run Command da AWS CLI. Il pacchetto installa due componenti: un richiedente VSS e un provider VSS. Il sistema copia questi componenti su una directory dell'istanza, poi registra il DLL del provider come provider VSS.

Per installare il pacchetto VSS

Esegui il comando seguente per scaricare e installare i componenti VSS necessari per Systems Manager.

```
aws ssm send-command \
    --document-name "AWS-ConfigureAWSPackage" \
    --instance-ids "i-1234567890abcdef0" \
    --parameters '{"action":["Install"],"name":["AwsVssComponents"]}'
```

PowerShell

Utilizzate la procedura seguente per scaricare e installare il `AwsVssComponents` pacchetto sulle vostre istanze utilizzando il comando Esegui dagli Strumenti per Windows PowerShell. Il

pacchetto installa due componenti: un richiedente VSS e un provider VSS. Il sistema copia questi componenti su una directory dell'istanza, poi registra il DLL del provider come provider VSS.

Per installare il pacchetto VSS

Esegui il comando seguente per scaricare e installare i componenti VSS necessari per Systems Manager.

```
Send-SSMCommand `
    -DocumentName "AWS-ConfigureAWSPackage" `
    -InstanceId "i-1234567890abcdef0" `
    -Parameter @{'action'='Install';'name'='AwsVssComponents'}
```

Verifica la firma su AWS Componenti VSS

Utilizza la procedura seguente per verificare la firma sul pacchetto `AwsVssComponents`.

1. Connettersi all'istanza Windows. Per ulteriori informazioni, consulta Connessione all'istanza Windows con il protocollo RDP.
2. Accedi a C:\Program Files\ Amazon\AwsVssComponents.
3. Apri il menu contestuale (tasto destro del mouse) di `ec2-vss-agent.exe`, quindi seleziona Proprietà.
4. Vai alla scheda Firme digitali e verifica che il nome del firmatario sia Amazon Web Services Inc.
5. Utilizza i passaggi precedenti per verificare la firma su `Ec2VssInstaller` e `Ec2VssProvider.dll`.

Aggiorna il pacchetto di componenti VSS sull'istanza di Windows EC2

Ti consigliamo di mantenere sempre aggiornato il componente VSS all'ultima versione consigliata. Quando viene rilasciata una nuova versione del pacchetto `AwsVssComponents`, è possibile aggiornare i componenti in diversi modi.

Metodi di aggiornamento

- È possibile ripetere i passaggi descritti in Installazione manuale dei componenti VSS su un'istanza di Windows EC2 quando viene rilasciata una nuova versione dei componenti AWS VSS.

- È possibile configurare un'associazione State Manager di Systems Manager per scaricare e installare automaticamente nuovi componenti VSS quando il pacchetto `AwsVssComponents` diventa disponibile.
- Quando si utilizza Systems Manager per eseguire il documento `AWSEC2-VssInstallAndSnapshot`, è possibile installare o aggiornare automaticamente il pacchetto `AwsVssComponents` ogni volta che si creano snapshot coerenti con l'applicazione.

> **Note**
>
> Consigliamo di utilizzare Systems Manager per eseguire il documento del comando `AWSEC2-VssInstallAndSnapshot` che installa o aggiorna automaticamente il pacchetto `AwsVssComponents` prima di creare gli snapshot coerenti con l'applicazione. Per ulteriori informazioni, consulta Esegui il documento di AWSEC2-VssInstallAndSnapshot comando (consigliato).

Per creare un'associazione Systems Manager State Manager, completa le operazioni per il tuo ambiente preferito.

Console

Quando crei un'associazione State Manager di Systems Manager, sono disponibili due opzioni per aggiornare il pacchetto `AwsVssComponents`, come segue:

Disinstalla e reinstalla

Questo metodo scarica e installa il pacchetto senza prerequisiti aggiuntivi.

In-place update

Questa opzione esegue un aggiornamento sul posto del pacchetto e presenta i seguenti prerequisiti:

- La versione dell'agente SSM installata sull'istanza deve essere la versione `3.3.808.0` o successiva. Per ulteriori informazioni, consulta Installazione e configurazione di SSM Agent sulle istanze EC2 per Windows Server nella Guida per l'utente di AWS Systems Manager .
- Se specificata, la versione del pacchetto `AwsVssComponents` deve essere la versione `2.5.0` o successiva. Le versioni precedenti non supportano l'aggiornamento sul posto.

> **Note**
>
> se l'istanza non soddisfa questi prerequisiti, l'aggiornamento sul posto avrà esito negativo. Utilizza, invece, l'opzione Disinstalla e reinstalla.

Per creare un'associazione di State Manager

1. Aprire la AWS Systems Manager console all'indirizzo. https://console.aws.amazon.com/systems-manager/
2. Nel riquadro di navigazione, seleziona State Manager.

   Oppure, se la home page di Systems Manager si apre per prima, apri il riquadro di navigazione e scegli State Manager.
3. Selezionare Create association (Crea associazione).
4. Nel campo Name (Nome), immettere un nome descrittivo.
5. Nell'elenco Document (Documento) scegliere AWS-ConfigureAWSPackage.
6. Nella sezione Parameters (Parametri), scegliere Install (Installa) dall'elenco di operazioni.
7. Per il tipo di installazione, scegli Disinstalla e reinstalla o In-place aggiorna.
8. Nel campo Name (Nome), inserire `AwsVssComponents`. Puoi mantenere vuoti i campi Version (Versione) e Additional Arguments (Argomenti aggiuntivi).
9. Nella sezione Targets (Destinazioni), scegliere un'opzione.

   > **Note**
   >
   > Se si sceglie di definire come target le istanze mediante i tag e si specificano tag che mappano per istanze di Linux, l'associazione va a buon fine sull'istanza di Windows, ma non sulle istanze di Linux. Lo stato globale dell'associazione mostra Failed (Non riuscito).
10. Scegliere una tra le opzioni disponibili in Specify schedule (Specifica la pianificazione).
11. Nella sezione Opzioni avanzate, per Gravità conformità, scegliere un livello di gravità per l'associazione. Per ulteriori informazioni, consulta Learn about association compliance.
    In Calendari di modifica, seleziona un calendario di modifica preconfigurato. Per ulteriori informazioni, consulta la pagina AWS Systems Manager Change Calendar.
12. In Controllo della velocità, procedi come segue:

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.
- Per Soglia di errore, specificare quando interrompere l'esecuzione del comando sulle altri nodi gestiti dopo un errore su un numero o una percentuale di nodi.

13. (Facoltativo) In Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Abilita scrittura dell'output in S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.
14. Selezionare Create association (Crea associazione), poi Close (Chiudi). Il sistema tenta di creare l'associazione sulle istanze e di applicare immediatamente lo stato.

> **Note**
>
> Se le istanze EC2 per Windows Server mostrano lo stato Non riuscito, verifica che l'agente SSM sia in esecuzione sull'istanza e verifica che l'istanza sia configurata con un ruolo AWS Identity and Access Management (IAM) per Systems Manager. Per ulteriori informazioni, consulta Configurazione. AWS Systems Manager

AWS CLI

Utilizza il comando create-association per aggiornare un pacchetto Distributore in base a una pianificazione senza disconnettere l'applicazione associata. Vengono sostituiti solo i file nuovi o aggiornati nel pacchetto.

Per creare un'associazione di State Manager

Esegui il comando seguente per creare un'associazione. Il valore `--name`, ossia il nome del documento, è sempre `AWS-ConfigureAWSPackage`. Il comando seguente utilizza la chiave `InstanceIds` per specificare le istanze di destinazione.

```
aws ssm create-association \
    --name "AWS-ConfigureAWSPackage" \
    --parameters action=Install,installationType="Uninstall and
 reinstall",name=AwsVssComponents \
    --targets Key=InstanceIds,Values=i-1234567890abcdef0,i-000011112222abcde
```

PowerShell

Per creare un'associazione di State Manager

Utilizza il cmdlet New-SSMAssociation.

```
New-SSMAssociation `
    -Name "AWS-ConfigureAWSPackage" `
    -Parameter  @{
        "action" = "Install"
        "installationType" = "Uninstall and reinstall"
        "name" = "AwsVssComponents"
    } `
    -Target @{
        "Key" = "InstanceIds"
        "Values" = @("i-1234567890abcdef0", "i-000011112222abcde")
    }
```

Crea snapshot EBS basati su VSS per l'istanza EC2 Windows

Dopo aver soddisfatto tutti i Prerequisiti per creare snapshot EBS basati su Windows VSS, puoi utilizzare uno dei seguenti metodi per creare snapshot basati su VSS dall'istanza EC2.

AWS Systems Manager documenti di comando

Utilizzare i documenti di comando di Systems Manager per creare snapshot basati su VSS.

Per automatizzare i backup, è possibile creare un'attività della finestra AWS Systems Manager di manutenzione che utilizzi il documento di `AWSEC2-VssInstallAndSnapshot` comando. Per ulteriori informazioni, consulta Utilizzo delle finestre di manutenzione (console) nella Guida per l'utente di AWS Systems Manager .

AWS Backup

È possibile creare un backup VSS durante l'utilizzo AWS Backup abilitando VSS nella console o nella CLI. Per ulteriori informazioni, consulta la pagina Creating Windows VSS backups della Guida per gli sviluppatori di AWS Backup .

> **Note**
>
> AWS Backup non installa automaticamente il `AwsVssComponents` pacchetto sulla tua istanza. È necessario eseguire un'installazione manuale sull'istanza. Per ulteriori

informazioni, consulta Installazione manuale dei componenti VSS su un'istanza di Windows EC2.

Amazon Data Lifecycle Manager

Puoi creare snapshot VSS utilizzando Amazon Data Lifecycle Manager abilitando gli script pre e post nelle policy del ciclo di vita degli snapshot. Per ulteriori informazioni, consulta Automazione degli snapshot coerenti a livello di applicazione nella Guida per l'utente Amazon EBS.

> **Note**
>
> Il Sistema di gestione del ciclo di vita dei dati Amazon non installa automaticamente il pacchetto `AwsVssComponents` sull'istanza. È necessario eseguire un'installazione manuale sull'istanza. Per ulteriori informazioni, consulta Installazione manuale dei componenti VSS su un'istanza di Windows EC2.

Usa i documenti di comando di Systems Manager per creare snapshot basati su VSS

È possibile utilizzare i documenti di AWS Systems Manager comando per creare istantanee basate su VSS. Il seguente contenuto introduce i documenti di comando disponibili e i parametri di runtime utilizzati dai documenti per creare gli snapshot.

Prima di utilizzare uno dei documenti di comando di Systems Manager, assicurati di aver soddisfatto tutti i Prerequisiti per creare snapshot EBS basati su Windows VSS.

Argomenti

- Parametri per i documenti Systems Manager per snapshot VSS
- Esecuzione dei documenti di comando Systems Manager per snapshot VSS

Parametri per i documenti Systems Manager per snapshot VSS

I documenti Systems Manager che creano snapshot VSS utilizzano tutti i seguenti parametri, eccetto dove segnalato:

AmiName(stringa, opzionale)

Se l'CreateAmiopzione è impostata su`True`, specifica il nome dell'AMI creata dal backup.

description (stringa, facoltativo)

Specifica una descrizione per gli snapshot o l'immagine creata da questo processo.

CollectDiagnosticLogs(stringa, opzionale)

Per raccogliere ulteriori informazioni durante le fasi di creazione di snapshot e AMI, imposta questo parametro su "`True`". Il valore predefinito per questo parametro è "`False`". I log di diagnostica consolidati vengono salvati come formato archivio `.zip` nella seguente posizione sull'istanza:

`C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`

CopyOnly(stringa, opzionale)

Se si utilizza il backup nativo di SQL Server in aggiunta a AWS VSS, l'esecuzione di un Copy-only backup impedisce a AWS VSS di interrompere la catena di backup differenziale nativa. Per eseguire un'operazione di Copy-only backup, imposta questo parametro su. `True`

Il valore predefinito per questo parametro è`False`, che fa sì che AWS VSS esegua un'operazione di backup completa.

CreateAmi(stringa, opzionale)

Per creare un'Amazon Machine Image (AMI) basata su VSS per il backup dell'istanza, imposta questo parametro su `True`. Il valore predefinito per questo parametro è `False`, che esegue invece il backup dell'istanza con uno snapshot EBS.

Per ulteriori informazioni sulla creazione di un'AMI da un'istanza, consulta la pagina Crea un' EBS-backed AMI Amazon.

executionTimeout (stringa, facoltativo)

Specifica il tempo massimo in secondi per eseguire il processo di creazione degli snapshot sull'istanza o per creare un'AMI dall'istanza. L'aumento di questo timeout consente al comando di attendere più a lungo l'avvio del blocco da parte di VSS e di completare il tagging delle risorse create. Questo timeout si applica solo alle fasi di creazione degli snapshot o dell'AMI. Il passaggio iniziale per installare o aggiornare il pacchetto `AwsVssComponents` non è incluso nel timeout.

ExcludeBootVolume(stringa, opzionale)

Questa impostazione esclude i volumi di avvio dal processo di backup se si creano snapshot. Per escludere i volumi di avvio dalle istantanee, imposta ExcludeBootVolume su `True` e CreateAmi su`False`.

Se si crea un'AMI per il backup, questo parametro deve essere impostato su `False`. Il valore predefinito per questo parametro è `False`.

NoWriters(stringa, opzionale)

Per escludere i writer VSS dell'applicazione dal processo di snapshot, imposta questo parametro su`True`. L'esclusione dei writer VSS dell'applicazione può aiutarti a risolvere i conflitti con componenti di backup VSS di terze parti. Il valore predefinito per questo parametro è `False`.

Se `SaveVssMetadata` è `True`, questo parametro deve essere impostato su `False`.

SaveVssMetadata(stringa, opzionale)

Per salvare i file di metadati VSS durante ogni snapshot, imposta questo parametro su `True`. Il valore predefinito è `False`. Questi file aiutano a comprendere quali componenti o autori sono stati inclusi in un'operazione di backup e i file e i volumi associati per ciascuna istantanea. I file di metadati vengono utilizzati durante il ripristino di un database SQL utilizzando la soluzione di ripristino VSS. Per ulteriori informazioni su come ripristinare un database SQL da istantanee VSS, vedere Utilizzare un runbook di automazione per ripristinare il database dalle istantanee della soluzione VSS. AWS

I file di metadati hanno l'ID del set di snapshot associato nei loro nomi. Puoi trovarli nella seguente posizione sull'istanza:

```
C:\ProgramData\Amazon\AwsVss\VssMetadata\
```

> **Warning**
>
> - Il salvataggio dei file di metadati VSS richiede `AwsVssComponents` la versione del pacchetto 2.4.0 o successive. Se nell'istanza è installata una versione precedente, l'impostazione di `SaveVssMetadata` su `True`compromette la creazione dello snapshot.
> - I parametri `NoWriters` e `SaveVssMetadata` si escludono a vicenda. Se entrambi sono impostati su `True`, la creazione dello snapshot non va a buon fine.

tags (stringa, facoltativo)

Si consiglia di assegnare tag agli snapshot e alle immagini per facilitare l'individuazione e la gestione delle risorse, ad esempio per ripristinare i volumi da un elenco di snapshot. Il sistema

aggiunge la chiave `Name`, con un valore vuoto in cui è possibile specificare il nome che si desidera applicare agli snapshot o alle immagini di output.

Ulteriori tag possono essere elencati separandoli con un punto e virgola. Ad esempio, `Key=Environment,Value=Test;Key=User,Value=TestUser1`.

> **Note**
>
> Le chiavi e i valori dei tag devono contenere solo caratteri alfanumerici e i caratteri speciali: `() ./\-"'@_+:={}`.

Per impostazione predefinita, il sistema aggiunge i seguenti tag riservati per snapshot e immagini basate su VSS.

- Dispositivo: per snapshot basati su VSS, questo è il nome del dispositivo del volume EBS acquisito dallo snapshot.
- AppConsistent— Questo tag indica la corretta creazione di un'istantanea o AMI basata su VSS.
- AwsVssConfig— Identifica le istantanee e le AMI create con VSS abilitato. Il tag include meta informazioni come la versione `AwsVssComponents` e l'ID del set di snapshot nei loro nomi.

> **Warning**
>
> Specificare uno di questi tag riservati nell'elenco dei parametri causerà un errore.

VssVersion(stringa, opzionale)

Solo per il documento `AWSEC2-VssInstallAndSnapshot`, puoi specificare il parametro `VssVersion` per installare una versione specifica del pacchetto `AwsVssComponents` sull'istanza. Lascia vuoto questo parametro per installare la versione predefinita consigliata.

Se la versione specificata del pacchetto `AwsVssComponents` è già installata, lo script salta la fase di installazione e passa alla fase di backup. Per un elenco delle versioni del pacchetto `AwsVssComponents` e del supporto operativo, consulta AWS Cronologia delle versioni della soluzione VSS.

Esecuzione dei documenti di comando Systems Manager per snapshot VSS

È possibile creare istantanee EBS basate su VSS con i documenti di AWS Systems Manager comando come segue.

Esegui il documento di AWSEC2-VssInstallAndSnapshot comando (consigliato)

Quando si utilizza AWS Systems Manager per eseguire il `AWSEC2-VssInstallAndSnapshot` documento, lo script esegue i seguenti passaggi.

1. Lo script installa o aggiorna innanzitutto il pacchetto `AwsVssComponents` sull'istanza, a seconda che sia già installato.
2. Lo script crea snapshot coerenti con l'applicazione dopo il completamento del primo passaggio.

Per eseguire il documento `AWSEC2-VssInstallAndSnapshot`, segui i passaggi relativi al tuo ambiente preferito.

Console

Creazione di snapshot EBS basatu su VSS dalla console

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, seleziona Esegui comando. Questo mostra un elenco di comandi correntemente in esecuzione nel tuo account, se applicabile.
3. Seleziona Esegui comando. Si apre un elenco di documenti di comando a cui si ha accesso.
4. Seleziona `AWSEC2-VssInstallAndSnapshot` dall'elenco dei documenti di comando. Per semplificare i risultati, puoi inserire tutto o parte del nome del documento. Puoi anche filtrare per proprietario, per tipo di piattaforma o per tag.

   Quando si seleziona un documento di comando, i dettagli vengono inseriti sotto l'elenco.
5. Seleziona `Default version at runtime` dall'elenco delle versioni del documento.
6. Configura i parametri del comando per definire come `AWSEC2-VssInstallAndSnapshot` installerà il pacchetto `AwsVssComponents` ed eseguire il backup con snapshot VSS o un'AMI. Per i dettagli dei parametri, consulta Parametri per i documenti Systems Manager per snapshot VSS.
7. In Selezione della destinazione, specifica i tag o seleziona manualmente le istanze per identificare le istanze su cui eseguire questa operazione.

> **Note**
>
> Se selezioni manualmente le istanze e l'istanza prevista non è inclusa nell'elenco, consulta Dove sono le mie istanze? per suggerimenti sulla risoluzione dei problemi.

8. Per i parametri aggiuntivi per la definizione del comportamento dei comandi di esecuzione di Systems Manager, ad esempio il controllo della velocità, immetti i valori come descritto in Esecuzione di comandi dalla console.
9. Selezionare Run (Esegui).

   In caso di esito positivo, il comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco delle snapshot EBS cercando i tag specificati o `AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando di Systems Manager. Nel caso in cui l'esecuzione del comando risulti completata con successo, ma non sia riuscito il backup di un determinato volume, è possibile risolvere il problema dall'elenco dei volumi EBS.

AWS CLI

È possibile eseguire i seguenti comandi in AWS CLI per creare istantanee EBS basate su VSS e ottenere lo stato della creazione delle istantanee.

Creazione di snapshot basati su VSS

Esegui il comando seguente per creare snapshot EBS basati su VSS. Per creare gli snapshot, devi identificare le istanze con il parametro `--instance-ids`. Per ulteriori informazioni sugli altri parametri che è possibile utilizzare, consulta Parametri per i documenti Systems Manager per snapshot VSS.

```
aws ssm send-command \
 --document-name "AWSEC2-VssInstallAndSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"],"VssVersion":[""]}'
```

In caso di esito positivo, il documento di comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco delle snapshot EBS cercando i

tag specificati o `AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando.

Ottenere lo stato del comando

Per ottenere lo stato corrente degli snapshot, esegui il comando riportato utilizzando l'ID del comando restituito da send-command.

```
aws ssm get-command-invocation
 --instance-ids "i-01234567890abcdef" \
 --command-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
 --plugin-name "CreateVssSnapshot"
```

PowerShell

Eseguite i seguenti comandi AWS Tools for Windows PowerShell per creare istantanee EBS basate su VSS e ottenere lo stato di runtime corrente per la creazione dell'output. Specifica i parametri descritti nell'elenco precedente per modificare il comportamento del processo di snapshot.

Crea istantanee EBS basate su VSS con Tools for Windows PowerShell

Esegui il comando riportato per creare snapshot EBS o AMI basati su VSS.

```
Send-SSMCommand -DocumentName "AWSEC2-VssInstallAndSnapshot" -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value';'VssVersion'=''}
```

Ottenere lo stato del comando

Per ottenere lo stato corrente degli snapshot, esegui il comando riportato utilizzando l'ID del comando restituito da Send-SSMCommand.

```
Get-SSMCommandInvocationDetail -InstanceId "i-01234567890abcdef" -CommandId
 "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -PluginName "CreateVssSnapshot"
```

In caso di esito positivo, il comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco delle snapshot EBS cercando i tag specificati o

`AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando.

Esegui il documento di comando AWSEC2-CreateVssSnapshot

Per eseguire il documento `AWSEC2-CreateVssSnapshot`, segui i passaggi relativi al tuo ambiente preferito.

Console

Creazione di snapshot EBS basatu su VSS dalla console

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, seleziona Esegui comando. Questo mostra un elenco di comandi correntemente in esecuzione nel tuo account, se applicabile.
3. Seleziona Esegui comando. Si apre un elenco di documenti di comando a cui si ha accesso.
4. Seleziona `AWSEC2-CreateVssSnapshot` dall'elenco dei documenti di comando. Per semplificare i risultati, puoi inserire tutto o parte del nome del documento. Puoi anche filtrare per proprietario, per tipo di piattaforma o per tag.

   Quando si seleziona un documento di comando, i dettagli vengono inseriti sotto l'elenco.
5. Seleziona `Default version at runtime` dall'elenco delle versioni del documento.
6. Configura i parametri del comando per definire come `AWSEC2-CreateVssSnapshot` eseguirà il backup con snapshot VSS o un'AMI. Per i dettagli dei parametri, consulta Parametri per i documenti Systems Manager per snapshot VSS.
7. In Selezione della destinazione, specifica i tag o seleziona manualmente le istanze per identificare le istanze su cui eseguire questa operazione.

   > **Note**
   >
   > Se selezioni manualmente le istanze e l'istanza prevista non è inclusa nell'elenco, consulta Dove sono le mie istanze? per suggerimenti sulla risoluzione dei problemi.
8. Per i parametri aggiuntivi per la definizione del comportamento dei comandi di esecuzione di Systems Manager, ad esempio il controllo della velocità, immetti i valori come descritto in Esecuzione di comandi dalla console.

9. Selezionare Run (Esegui).

   In caso di esito positivo, il comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco delle snapshot EBS cercando i tag specificati o `AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando di Systems Manager. Nel caso in cui l'esecuzione del comando risulti completata con successo, ma non sia riuscito il backup di un determinato volume, è possibile risolvere il problema dall'elenco dei volumi EBS.

AWS CLI

È possibile eseguire il seguente comando in AWS CLI per creare istantanee EBS basate su VSS.

Creazione di snapshot basati su VSS

Esegui il comando seguente per creare snapshot EBS basati su VSS. Per creare gli snapshot, devi identificare le istanze con il parametro `--instance-ids`. Per ulteriori informazioni sugli altri parametri che è possibile utilizzare, consulta Parametri per i documenti Systems Manager per snapshot VSS.

```
aws ssm send-command \
 --document-name "AWSEC2-CreateVssSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"]}'
```

In caso di esito positivo, il documento di comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco delle snapshot EBS cercando i tag specificati o `AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando.

PowerShell

Esegui il seguente comando con AWS Tools for Windows PowerShell per creare istantanee EBS basate su VSS.

Crea istantanee EBS basate su VSS con Tools for Windows PowerShell

Esegui il comando seguente per creare snapshot EBS basati su VSS. Per creare gli snapshot, devi identificare le istanze con il parametro `InstanceId`. È possibile specificare più di un'istanza

per cui creare snapshot. Per ulteriori informazioni sugli altri parametri che è possibile utilizzare, consulta Parametri per i documenti Systems Manager per snapshot VSS.

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value'}
```

In caso di esito positivo, il comando compila l'elenco degli snapshot EBS con i nuovi snapshot. È possibile trovare questi snapshot nell'elenco delle snapshot EBS cercando i tag specificati o `AppConsistent`. I motivi dettagliati di un eventuale errore nell'esecuzione del comando sono disponibili nell'output del comando. Nel caso in cui l'esecuzione del comando risulti completata con successo, ma non sia riuscito il backup di un determinato volume, è possibile risolvere il problema dall'elenco degli snapshot EBS.

Esecuzione dei documenti di comando per un cluster di failover Windows con archiviazione EBS condivisa

È possibile utilizzare una qualsiasi delle procedure della linea di comando descritte nella sezione precedente per creare uno snapshot basato su VSS. Il documento del comando (`AWSEC2-VssInstallAndSnapshot` o `AWSEC2-CreateVssSnapshot`) deve essere eseguito sul nodo primario del cluster. Il documento avrà esito negativo sui nodi secondari in quanto non hanno accesso ai dischi condivisi. Se le modifiche primarie e secondarie vengono eseguite in modo dinamico, è possibile AWS Systems Manager eseguire il documento Run Command su più nodi con l'aspettativa che il comando abbia esito positivo sul nodo primario e abbia esito negativo sui nodi secondari.

> **Note**
>
> Per automatizzare i backup, è possibile creare un'attività della finestra di AWS Systems Manager manutenzione che utilizzi il documento. `AWSEC2-VssInstallAndSnapshot` Per ulteriori informazioni, consulta Utilizzo delle finestre di manutenzione (console) nella Guida per l'utente di AWS Systems Manager .

Risolvere problemi relativi agli snapshot EBS basati su Windows VSS

Prima di provare qualsiasi altra procedura di risoluzione dei problemi, consigliamo di verificare le seguenti informazioni.

- Assicurati di aver soddisfatto tutti i Prerequisiti per creare snapshot EBS basati su Windows VSS.
- Verifica di utilizzare la Supporto della versione del sistema operativo Windows più recente del pacchetto `AwsVssComponents` per il sistema operativo. Il problema riscontrato potrebbe essere stato risolto nelle versioni più recenti.

Argomenti

- Verificare i file di registro
- Raccogliere log di diagnostica aggiuntivi
- Utilizzo di VSS su istanze con proxy configurato
- Errore: timeout della connessione del thaw pipe, errore sul thaw, timeout in attesa di VSS Freeze o altri errori di timeout
- Errore: impossibile richiamare il metodo. L'invocazione del metodo è supportata solo sui tipi principali in questa modalità di linguaggio

Verificare i file di registro

Se si verificano problemi o si ricevono messaggi di errore durante la creazione di snapshot EBS basati su VSS, è possibile visualizzare l'output del comando nella console di Systems Manager.

Per i documenti Systems Manager che creano snapshot VSS, è possibile impostare il parametro `CollectDiagnosticLogs` su "`True`" al runtime. Quando il parametro `CollectDiagnosticLogs` è impostato su "`True`", VSS raccoglie registri aggiuntivi per facilitare il debug. Per ulteriori informazioni, consulta Raccogliere log di diagnostica aggiuntivi.

Se raccogli registri di diagnostica, il documento Systems Manager li archivia sulla tua istanza nella seguente posizione: `C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`. Il valore predefinito per il parametro `CollectDiagnosticLogs` è "`False`".

> **Note**
>
> Per ulteriori informazioni sul debug, puoi inviare il `.zip` file a. Supporto

Sono disponibili i seguenti registri aggiuntivi, indipendentemente dal fatto che si raccolgano o meno registri di diagnostica:

- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stdout`
- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stderr`

È inoltre possibile aprire l'applicazione Visualizzatore eventi di Windows e scegliere Registri di Windows, Applicazione per visualizzare i registri aggiuntivi. Per visualizzare gli eventi specificatamente dal provider VSS Windows EC2 e dal servizio Copia shadow del volume, filtrare in base all' origine con i termini **`Ec2VssSoftwareProvider`** e **`VSS`**.

Se utilizzi Systems Manager con endpoint VPC e l'azione API send-command di Systems Manager (Esegui comando nella console) non è riuscita, verifica di aver configurato correttamente il seguente endpoint: com.amazonaws. ***`region`***.ec2.

Se non è definito l'endpoint Amazon EC2, la chiamata per enumerare i volumi EBS collegati ha esito negativo e causa un errore del comando Systems Manager. Per ulteriori informazioni sulla configurazione degli endpoint VPC con Systems Manager, consulta Creazione di un endpoint VPC nella AWS Systems Manager Guida per l'utente di .

Raccogliere log di diagnostica aggiuntivi

Per raccogliere log di diagnostica aggiuntivi quando si utilizza il comando di invio di Systems Manager per eseguire il documento di snapshot VSS, imposta il parametro di input `CollectDiagnosticLogs` su "`True`" al runtime. Ti consigliamo di impostare questo parametro su "`True`" durante la risoluzione dei problemi.

Per visualizzare un esempio di riga di comando, seleziona una delle seguenti schede.

AWS CLI

L'esempio seguente esegue il documento Systems Manager `AWSEC2-CreateVssSnapshot` in AWS CLI:

```
aws ssm send-command \
    --document-name "AWSEC2-CreateVssSnapshot" \
    --instance-ids "i-1234567890abcdef0" \
```

```
    --parameters '{"description":["Example - create diagnostic logs at
 runtime."],"tags":["Key=tag_name,Value=tag_value"],"CollectDiagnosticLogs":
["True"]}'
```

PowerShell

L'esempio seguente esegue il documento `AWSEC2-CreateVssSnapshot` Systems Manager in: PowerShell

```
Send-SSMCommand `
    -DocumentName "AWSEC2-CreateVssSnapshot" `
    -InstanceId "i-1234567890abcdef0" `
    -Parameter @{'description'='Example - create diagnostic logs at
 runtime.';'tags'='Key=tag_name,Value=tag_value';'CollectDiagnosticLogs'='True'}
```

Utilizzo di VSS su istanze con proxy configurato

Se riscontri problemi durante la creazione di snapshot EBS basati su VSS su istanze che utilizzano un proxy per raggiungere gli endpoint EC2, verifica le seguenti impostazioni sulla tua istanza:

- Verifica che il proxy sia configurato in modo che gli endpoint del servizio EC2 nella regione e nell'IMDS dell'istanza siano raggiungibili eseguendo AWS Tools for Windows PowerShell come SYSTEM.
- Per supportare l'utilizzo del proxy WinHTTP configurato dal sistema, assicurati di aver installato la versione `AwsVssComponents` più recente sull'istanza. Per ulteriori informazioni sulla configurazione del proxy WinHTTP, consulta la pagina Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP) sul sito web di Microsoft.

Errore: timeout della connessione del thaw pipe, errore sul thaw, timeout in attesa di VSS Freeze o altri errori di timeout

Il provider VSS Windows EC2 potrebbe scadere a causa di attività o servizi sull'istanza che impediscono agli snapshot basati su VSS di procedere in modo tempestivo. Il framework VSS Windows fornisce una finestra di 10 secondi non configurabile durante la quale la comunicazione con il file system viene sospesa. Durante questo periodo, `AWSEC2-CreateVssSnapshot` crea gli snapshot dei volumi.

I seguenti problemi possono causare il superamento dei limiti di tempo da parte del provider VSS Windows EC2 durante uno snapshot:

- Eccessivo rispetto a un volume I/O
- Reattività lenta dell'API EC2 sull'istanza
- Volumi frammentati
- Incompatibilità con alcuni software antivirus
- Problemi con un autore di applicazioni VSS
- Quando la registrazione dei moduli è abilitata per un numero elevato di PowerShell moduli, ciò può rallentare l' PowerShell esecuzione degli script

La maggior parte dei problemi che si verificano quando si esegue il documento di comando `AWSEC2-CreateVssSnapshot` è legata a un carico di lavoro eccessivamente elevato sull'istanza al momento del backup. Le seguenti azioni consentono di eseguire con successo lo snapshot:

- Riprovare a eseguire il comando `AWSEC2-CreateVssSnapshot` per verificare se il tentativo di snapshot ha esito positivo. Se in alcuni casi il tentativo ha esito positivo, la riduzione del carico dell'istanza potrebbe rendere più efficace gli snapshot.
- Attendere che il carico di lavoro sull'istanza diminuisca e riprovare a eseguire il comando `AWSEC2-CreateVssSnapshot`. In alternativa, è possibile scattare gli snapshot quando si è certi che l'istanza è in una fase di carico ridotto.
- Provare a scattare gli snapshot VSS dopo avere disattivato il software antivirus del sistema. Se questo risolve il problema, fare riferimento alle istruzioni del software antivirus e configurarlo per consentire gli snapshot VSS.
- Se nell'account è presente un volume elevato di chiamate API Amazon EC2 nella stessa regione in cui si esegue uno snapshot, la limitazione (della larghezza di banda della rete) delle API può ritardare le operazioni di snapshot. Per ridurre l'impatto sulla limitazione, utilizza il pacchetto `AwsVssComponents` più recente. Questo pacchetto utilizza l'azione `CreateSnapshots` API EC2 per ridurre il numero di azioni mutanti, come la creazione e l'etichettatura di istantanee per volume.
- Se vi sono più script di comando `AWSEC2-CreateVssSnapshot` in esecuzione contemporaneamente, è possibile seguire questa procedura per ridurre i problemi di simultaneità.
  - Valutare la possibilità di programmare gli snapshot durante periodi di minore attività delle API.
  - Se si utilizza Run Command nella console Systems Manager (oppure SendCommand nell'API) per eseguire lo script di comando, è possibile utilizzare i controlli di velocità di Systems Manager per ridurre la simultaneità.

È inoltre possibile utilizzare i controlli di frequenza di Systems Manager per ridurre la concorrenza per servizi come quelli AWS Backup che utilizzano Systems Manager per eseguire lo script di comando.

- Eseguire il comando `vssadmin list writers` in una shell e verificare se segnala eventuali errori nel campo Ultimo errore per tutti gli autori del sistema. Se un autore segnala un errore di timeout, è consigliabile scattare nuovi snapshot quando l'istanza è sotto un carico minore.
- Quando si utilizzano tipi di istanza più piccoli come *t2 | t3 | t3a* .nano o *t2 | t3 | t3a* .micro, possono verificarsi dei timeout dovuti a vincoli di memoria e CPU. Le seguenti operazioni potrebbero contribuire a ridurre i problemi di timeout.
  - Provare a chiudere le applicazioni con un uso intensivo di memoria e CPU prima di acquisire snapshot.
  - Provare ad acquisire snapshot durante i periodi di minore attività dell'istanza.

Errore: impossibile richiamare il metodo. L'invocazione del metodo è supportata solo sui tipi principali in questa modalità di linguaggio

Questo errore si verifica quando la modalità PowerShell lingua non è impostata su. `FullLanguage` Il documento `AWSEC2-CreateVssSnapshot` SSM richiede PowerShell di essere configurato in `FullLanguage` modalità.

Per verificare la modalità linguistica, esegui il seguente comando sull'istanza in una PowerShell console:

```
$ExecutionContext.SessionState.LanguageMode
```

Per ulteriori informazioni sulle modalità linguistiche, vedere about_ Language_Modes nella documentazione Microsoft.

Usa il AWS Soluzione VSS per ripristinare i dati per la tua istanza

È possibile ripristinare i volumi EBS per un'istanza Windows da istantanee basate su VSS create dalla soluzione VSS. AWS Se le istantanee della soluzione AWS VSS contengono backup di un database Microsoft SQL Server, è possibile ripristinare il database utilizzando il runbook di Automation. `AWSEC2-RestoreSqlServerDatabaseWithVss` AWS Systems Manager

Il runbook di ripristino del database automatizza l'intero processo di ripristino, inclusa la creazione di volumi dagli snapshot e il loro collegamento all'istanza. L'automazione sfrutta la tecnologia VSS per

ripristinare il database, consentendo di eseguire il ripristino senza arrestare l'applicazione SQL Server o disconnettere eventuali connessioni attive.

Per istruzioni dettagliate su come usare il runbook del database Microsoft SQL Server, consulta Restore from VSS based snapshots nella Guida per l'utente di Microsoft SQL Server su Amazon EC2.

Personalizza uno script da cui ripristinare i volumi EBS AWS Istantanee della soluzione VSS

È possibile utilizzare lo `RestoreVssSnapshotSampleScript.ps1` script come modello per creare uno script personalizzato che ripristini i volumi EBS dalle AWS istantanee delle soluzioni VSS. Lo script di esempio esegue le seguenti attività:

- Arresta un'istanza
- Rimuove tutte le unità esistenti dall'istanza (eccetto il volume di avvio, se è stato escluso)
- Crea nuovi volumi dagli snapshot
- Collega i volumi all'istanza utilizzando il tag di ID dispositivo sulla snapshot
- Riavvia l'istanza

> **Important**
>
> Lo script seguente scollega tutti i volumi collegati a un'istanza, poi crea nuovi volumi da una snapshot. Accertati di aver correttamente eseguito il backup dell'istanza. I vecchi volumi non vengono eliminati. All'occorrenza, è possibile modificare lo script per eliminare i vecchi volumi.

Per ripristinare volumi da snapshot EBS basati su VSS

1. Scarica il RestoreVssSnapshotSampleScript.zip file ed estrai il contenuto del file.
2. Apri `RestoreVssSnapshotSampleScript.ps1` in un editor di testo e modifica la chiamata di esempio nella parte inferiore dello script con un ID di istanza EC2 e un ID snapshot EBS validi, quindi esegui lo script da. PowerShell

AWS Cronologia delle versioni della soluzione VSS

Questa pagina include le note di rilascio per versione per il pacchetto di componenti AWS VSS, nonché i requisiti di versione dei componenti e degli script per ciascuna versione supportata di Windows Server.

Argomenti

- AwsVssComponents versioni del pacchetto
- Supporto della versione del sistema operativo Windows

AwsVssComponents versioni del pacchetto

La tabella seguente descrive le versioni rilasciate del pacchetto di componenti AWS VSS.

Versione	Dettagli	Data di rilascio	Scaricabile
2.5.2	• È stato aggiunto il supporto per l'endpoint della `aws-eusc` partizione. • AWS SDK aggiornato per incorporare gli aggiornamenti di sicurezza.	2 settembre 2026	Sì
2.5.1	Risolto un problema che causava il fallimento del ripristino del database SQL quando veniva specificato il parametro del database di destinazione.	13 marzo 2025	Sì
2.5.0	• Aggiunta la possibilità di leggere i file di metadati VSS e ripristinare un database Microsoft SQL Server sull'istanza. Per ulteriori informazioni, consulta Restore from VSS based snapshots nella Guida per l'utente di Microsoft SQL Server su Amazon EC2. •	17 gennaio 2025	Sì

Versione	Dettagli	Data di rilascio	Scaricabile
	Aggiunto supporto per l'opzione di aggiornamento in loco durante l'installazione o l'aggiornamento del pacchetto `AwsVssComponents` .		
2.4.0	È stata aggiunta la possibilità di salvare i file di metadati VSS durante la creazione di snapshot. Per abilitare questa funzione, vedi SaveVssMetadata inParametri per i documenti Systems Manager per snapshot VSS.	7 ottobre 2024	Sì
2.3.3	È stato aggiornato l'agente VSS per garantire che venga utilizzato `Ec2VssProvider` durante la creazione di snapshot.	25 giugno 2024	Sì
2.3.2	È stato risolto un caso in cui la registrazione del provider VSS non viene rimossa durante la disinstal lazione.	9 maggio 2024	Sì
2.3.1	È stato aggiunto un nuovo tag predefinito `AwsVssConfig` per identificare le istantanee e le AMI create da AWS VSS.	7 marzo 2024	Sì

Versione	Dettagli	Data di rilascio	Scaricabile
2.2.1	• È stato aggiunto il supporto per l'utilizzo dell'API `DescribeInstanceAttribute` . • Correzioni di bug e miglioramenti dell'affidabilità. • Supporto obsoleto per Windows Server 2012 e 2012 R2. AWS L'installazione dei componenti VSS versione 2.2.1 su Windows Server 2012 e 2012 R2 avrà esito negativo. AWS La versione 2.1.0 dei componenti VSS è l'ultima versione a supportare Windows Server 2012 e 2012 R2.	18 gennaio 2024	Sì
2.1.0	È stato aggiunto il supporto per l'utilizzo dell'API `CreateSnapshots` .	6 novembre 2023	Sì
2.0.1	È stato aggiunto il supporto per l'utilizzo delle impostazioni del proxy WinHTTP.	26 ottobre 2023	No
2.0.0	È stata aggiunta la funzionalità al componente AWS VSS per creare istantanee e AMI, che consente la compatibilità con la registrazione dei PowerShel l moduli, la registrazione dei blocchi di script e le funzionalità di trascrizione.	28 aprile 2023	No
1.3.2.0	Risolto un caso in cui l'errore di installazione non è stato segnalato correttamente.	10 maggio 2022	No

Versione	Dettagli	Data di rilascio	Scaricabile
1.3.1.0	• Risolti gli snapshot che non funzionavano sui controller di dominio in relazione a un errore di registrazione del writer VSS NTDS. • Risolto l'errore dell'agente VSS durante la disinstal lazione del provider VSS versione 1.0.	06 febbraio 2020	Sì
1.3.00	• Registrazione migliorata riducendo la verbosità indesiderata. • Risolti i problemi di regionalizzazione durante l'install azione. • Codici di reso fissi per alcune condizioni di errore di registrazione del provider. • Risolti vari problemi di installazione.	19 marzo 2019	No
1.2.00	• Aggiunti parametri della riga di comando `-nw` (senza scrittori) e `-copy` (solo copia) all'agente. • Sono stati corretti EventLog gli errori causati da chiamate errate di allocazione della memoria.	15 novembre 2018	No
1.1	Sono stati corretti i componenti AWS VSS utilizzati in modo errato come provider predefinito di Windows Backup and Restore.	12 dicembre 2017	No
1.0	Versione iniziale.	20 novembre 2017	No

Supporto della versione del sistema operativo Windows

La tabella seguente mostra quali versioni della soluzione AWS VSS è necessario eseguire su ciascuna versione di Windows Server su Amazon EC2.

Versione di Windows Server	AwsVssComponents versione	AWSEC2-VssInstallAndSnapshot nome della versione	AWSEC2-CreateVssSnapshot nome della versione
Windows Server 2025	default	default	default
Windows Server 2022	default	default	default
Windows Server 2019	default	default	default
Windows Server 2016	default	default	default
Windows Server 2012 R2	2.1.0	non supportato	2012R2
Windows Server 2012	2.1.0	non supportato	2012R2

Versione di Windows Server	AwsVssComponents versione	AWSEC2-VssInstallAndSnapshot nome della versione	AWSEC2-CreateVssSnapshot nome della versione
Windows Server 2008 R2	1.3.1.0	non supportato	2008R2

Archiviazione di oggetti, archiviazione di file e memorizzazione nella cache dei file su Amazon EC2

L'archiviazione di file nel cloud è un metodo di archiviazione di file nel cloud che permette a server e applicazioni di accedere ai dati tramite file system condivisi. Tale caratteristica di compatibilità rende questo servizio ideale per i carichi di lavoro che fanno affidamento su file system condivisi e fornisce integrazione semplificata per non dover modificare il codice.

Esistono molte soluzioni di storage di file, che vanno da un file server a nodo singolo su un'istanza di calcolo che utilizza lo storage a blocchi come base senza scalabilità o poche ridondanze per proteggere i dati, a una soluzione in do-it-yourself cluster, a una soluzione completamente gestita. Il seguente contenuto presenta alcuni dei servizi di storage forniti da AWS per l'uso con le EC2 istanze Amazon.

Indice

- Utilizzo di Amazon S3 con istanze Amazon EC2
- Utilizzo di Amazon EFS con le istanze Linux Amazon EC2
- Utilizzo di Amazon FSx con istanze Amazon EC2
- Usa Amazon File Cache con le EC2 istanze Amazon

Utilizzo di Amazon S3 con istanze Amazon EC2

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. È possibile utilizzare

Amazon S3 per archiviare e recuperare qualsiasi quantità di dati in un'ampia gamma di casi d'uso, come data lake, siti web, backup e analisi dei big data, da un'istanza Amazon EC2 oppure ovunque tramite Internet. Per ulteriori informazioni, consulta Che cos'è Amazon S3?

Esistono due modi per accedere ai dati di Amazon S3 dalle tue istanze Amazon EC2:

- Accesso ai file: utilizza Amazon S3 Files per montare un bucket S3 come file system ad alte prestazioni sulla tua istanza.
- Accesso agli oggetti: utilizza l'API Amazon S3 AWS CLI, gli AWS SDK o strumenti come wget per copiare oggetti da e verso S3.

Accesso ai file con Amazon S3 Files

Amazon S3 Files è un file system serverless che ti consente di montare il bucket S3 generico come file system ad alte prestazioni sulla tua istanza di calcolo. Con S3 Files, puoi accedere ai tuoi oggetti S3 come file utilizzando operazioni standard del file system come lettura e scrittura sul percorso di montaggio locale.

È possibile montare un file system S3 su un'istanza EC2 all'avvio o dopo l'avvio su un'istanza in esecuzione.

Prerequisiti

Prima di configurare S3 Files con la tua istanza EC2, assicurati di avere quanto segue:

- Un file system S3 e almeno un target di montaggio nello stato disponibile. Per informazioni sulla creazione di un file system S3, consulta Working with Amazon S3 Files nella Amazon S3 User Guide.
- Un'istanza EC2 Linux a cui è associato un profilo di istanza. Per informazioni sulle autorizzazioni richieste per montare il file system, consulta i ruoli e le policy IAM nella Amazon S3 User Guide.
- Gruppi di sicurezza che consentono il traffico NFS (porta 2049) tra l'istanza e le destinazioni di montaggio del file system. Per informazioni sulle impostazioni richieste dei gruppi di sicurezza, consulta i gruppi di sicurezza nella Amazon S3 User Guide.

Per montare un file system su un'istanza EC2 all'avvio utilizzando la console EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Launch Instance (Avvia istanza).

3. Sotto Network settings (Impostazioni di rete) effettua le seguenti operazioni:

   a. Scegli Modifica.

   b. Per Subnet (Sottorete), selezionare una sottorete.

   c. 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, puoi successivamente modificare il gruppo di sicurezza predefinito e aggiungere una regola per consentire SSH, oppure aggiungere un nuovo gruppo di sicurezza che consenta SSH. Puoi utilizzare le seguenti impostazioni:

      i. Tipo: SSH

      ii. Protocollo: TCP

      iii. Intervallo porte: 22

      iv. Fonte: Anywhere 0.0.0. 0/0

4. In Configura archiviazione, procedi come segue:

   a. In File system, scegli S3 Files.

   b. Scegli Add shared file system (Aggiungi file system condiviso).

   c. Per il file system S3, i file system vengono visualizzati nella zona di disponibilità in base alla sottorete selezionata 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.

   d. Inserisci un percorso di montaggio locale sull'istanza EC2 in cui desideri montare il file system (ad esempio,`/mnt/s3files`).

   e. Verrà generato un comando per montare il file system e aggiungerlo a fstab. È possibile aggiungere questo comando al campo Dati utente in Dettagli avanzati. L'istanza EC2 verrà quindi configurata per montare il file system S3 all'avvio e ogni volta che viene riavviata. Puoi anche eseguire questi comandi nella tua istanza EC2 dopo l'avvio.

5. In Dettagli avanzati, allega un profilo di istanza alla tua istanza. Il tuo ruolo IAM deve disporre delle autorizzazioni per montare il file system e accedere al bucket S3. Per ulteriori informazioni sulle autorizzazioni richieste, consulta i ruoli e le policy IAM nella Amazon S3 User Guide.

6. Scegliere Launch Instance (Avvia istanza).

Dopo l'avvio dell'istanza, vengono installate le utilità software richieste e il file system viene montato. È possibile visualizzare il file system accedendo al percorso di montaggio locale.

Per montare un file system su un'istanza EC2 dopo l'avvio

1. Connettiti alla tua istanza EC2 tramite Secure Shell (SSH) o utilizzando EC2 Instance Connect nella console EC2.
2. Per montare il tuo file system S3, usa l'utilità mount helper. `amazon-efs-utils` A seconda della distribuzione Linux in uso, utilizzate uno dei seguenti comandi per installare il `amazon-efs-utils` pacchetto:

   a. Se usi Amazon Linux, esegui il seguente comando per installare efs-utils dai repository di Amazon:

   ```
   sudo yum -y install amazon-efs-utils
   ```

   b. Se stai usando altre distribuzioni Linux supportate, esegui il seguente comando:

   ```
   curl https://amazon-efs-utils.aws.com/efs-utils-installer.sh | sudo sh -s -- --
   install
   ```

   c. Per altre distribuzioni Linux, consulta il repository efs-utils su GitHub.
3. Crea una directory per il punto di montaggio del file system usando il seguente comando:

   ```
   sudo mkdir {path/to/mount}
   ```
4. Montate il file system S3:

   ```
   FS="{YOUR_FILE_SYSTEM_ID}"
   sudo mount -t s3files $FS:/ {path/to/mount}
   ```
5. Conferma che il file system è montato:

   ```
   df -h {path/to/mount}
   ```

Per visualizzare gli oggetti nel bucket S3 come file

Dopo aver completato le procedure precedenti, 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 il seguente comando:

```
ls {path/to/mount}
```

Object-based accedere

Puoi copiare file da e verso Amazon S3 utilizzando l'API S3 AWS CLI, gli AWS SDK o gli strumenti HTTP standard. Se disponi delle autorizzazioni richieste, puoi copiare un file da o verso Amazon S3 e la tua istanza utilizzando uno dei seguenti metodi.

wget

> **Note**
>
> Questo metodo funziona solo per oggetti pubblici. Se l'oggetto non è pubblico, riceverai un messaggio `ERROR 403: Forbidden`. Se ricevi questo errore, devi utilizzare la console Amazon S3, l' AWS API AWS CLI, l' AWS SDK o AWS Tools for Windows PowerShell, e devi disporre delle autorizzazioni richieste. Per ulteriori informazioni, consulta Identity and Access Management for Amazon S3 e Downloading an object nella Guida per l'utente di Amazon S3.

L'wgetutilità è un client HTTP e FTP che puoi utilizzare per scaricare oggetti pubblici da Amazon S3. Viene installata per impostazione di default in Amazon Linux e nella maggior parte delle altre distribuzione ed è disponibile per il download su Windows. Per scaricare un oggetto Amazon S3, utilizza il seguente comando, ricordando di sostituire l'URL dell'oggetto da scaricare.

```
[ec2-user ~]$ wget https://amzn-s3-demo-bucket.s3.amazonaws.com/path-to-file
```

PowerShell

Puoi usare AWS Tools for Windows PowerShell per spostare gli oggetti da e verso Amazon S3.

Usa il Copy-S3Object cmdlet per copiare un oggetto Amazon S3 nella tua istanza Windows come segue.

```
Copy-S3Object `
```

```
    -BucketName amzn-s3-demo-bucket `
    -Key path-to-file `
    -LocalFile my_copied_file.ext
```

In alternativa, puoi aprire la console Amazon S3 utilizzando un browser Web sull'istanza Windows.

AWS CLI

Puoi utilizzare AWS Command Line Interface (AWS CLI) per scaricare articoli soggetti a restrizioni da Amazon S3 e caricare articoli. Per ulteriori informazioni, ad esempio su come installare e configurare gli strumenti, consulta la pagina dei dettagli di AWS Command Line Interface.

Il comando aws s3 cp è simile al comando Unix cp. Puoi copiare file da Amazon S3 alla tua istanza, copiare file dalla tua istanza in Amazon S3 e copiare file da posizioni Amazon S3 diverse.

Usa il seguente comando per copiare un oggetto da Amazon S3 alla tua istanza:

```
aws s3 cp s3://amzn-s3-demo-bucket/my_folder/my_file.ext my_copied_file.ext
```

Usa il seguente comando per copiare nuovamente un oggetto dalla tua istanza in Amazon S3:

```
aws s3 cp my_copied_file.ext s3://amzn-s3-demo-bucket/my_folder/my_file.ext
```

Il comando aws s3 sync può sincronizzare un intero bucket Amazon S3 in una posizione di directory locale. Ciò può risultare utile per scaricare un set di dati e mantenere aggiornata la copia locale con il set remoto. Se disponi delle autorizzazioni adeguate per il bucket Amazon S3, puoi eseguire il push del backup della directory locale nel cloud quando sei pronto invertendo le posizioni di origine e di destinazione nel comando.

Usa il seguente comando per scaricare un intero bucket Amazon S3 in una directory locale sulla tua istanza:

```
aws s3 sync s3://amzn-s3-demo-source-bucket local_directory
```

Amazon S3 API

Puoi utilizzare un'API per accedere ai dati in Amazon S3. È possibile utilizzare questa API per sviluppare la tua applicazione e integrarla con altre API e SDK. Per ulteriori informazioni, consulta

Esempi di codice per Amazon S3 che utilizzano AWS SDK nell'API Reference di Amazon Simple Storage Service.

Utilizzo di Amazon EFS con le istanze Linux Amazon EC2

> **Note**
>
> Amazon EFS non è supportato sulle istanze Windows.

Amazon EFS fornisce lo storage di file scalabile da utilizzare con Amazon EC2. Puoi utilizzare un file system EFS come origine dati comune per carichi di lavoro e applicazioni in esecuzione su più istanze. Per ulteriori informazioni, consulta la pagina dei dettagli del prodotto Amazon Elastic File System.

Questo tutorial mostra come creare e collegare un Amazon EFS file system su un'istanza utilizzando la procedura di creazione rapida di Amazon EFS durante l'avvio dell'istanza. Per un tutorial su come creare un file system utilizzando la console Amazon EFS, consulta Nozioni di base su Amazon Elastic File System nella Guida per l'utente di Amazon Elastic File System.

> **Note**
>
> Quando si crea un file system EFS utilizzando la creazione rapida di EFS, il file system viene creato con le seguenti impostazioni consigliate per il servizio:
>
> - Backup automatici attivati.
> - Gestisci gli obiettivi di montaggio nel VPC selezionato.
> - Modalità prestazioni a scopo generale.
> - Modalità di throughput di bursting.
> - Crittografia dei dati inattivi abilitata utilizzando la chiave predefinita per Amazon EFS (`aws/elasticfilesystem`).
> - Gestione del ciclo di vita Amazon EFS abilitata con una policy di 30 giorni.

Processi

- Creazione di un file system EFS utilizzando la creazione rapida di Amazon EFS

- Testare il file system EFS
- Eliminare il file system EFS

Creazione di un file system EFS utilizzando la creazione rapida di Amazon EFS

Puoi creare un file system EFS e montarlo sull'istanza al momento dell'avvio utilizzando la funzionalità di creazione rapida di Amazon EFS della procedura guidata dell'istanza di Amazon EC2.

Per creare un file system EFS utilizzando la creazione rapida di Amazon EFS

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Launch Instance (Avvia istanza).
3. (Facoltativo) In Name and tags (Nome e tag), per Name (Nome) inserisci un nome descrittivo per identificare l'istanza.
4. In Application and OS Images (Amazon Machine Image) (Immagini di applicazioni e sistema operativo [Amazon Machine Image]), scegli un sistema operativo Linux, quindi per Amazon Machine Image (AMI) (Amazon Machine Image [AMI]), seleziona un'AMI Linux.
5. In Instance type (Tipo di istanza), per Instance type (Tipo di istanza), seleziona un tipo di istanza o mantieni il valore predefinito.
6. In Key pair (login) (Coppia di chiavi (login), per Key pair name (Nome della coppia di chiavi), scegliere una coppia di chiavi esistente o creane una nuova.
7. In Network settings (Impostazioni di rete), scegli Edit (Modifica) a destra, quindi seleziona una sottorete in Subnet (Sottorete).

   > **Note**
   >
   > Devi selezionare una sottorete prima di poter aggiungere un file system EFS.

8. In Configure storage (Configura lo storage), scegli Edit (Modifica) in basso a destra, quindi esegui le operazioni riportate di seguito:

   a. Assicurati che sia selezionato EFS per File system, quindi scegli Crea nuovo file system condiviso.

   b. Per Nome del file system, inserisci un nome per il file system Amazon EFS, quindi scegli Crea file system.

c. Per Punto di montaggio, specifica un punto di montaggio personalizzato o mantieni il valore predefinito.

d. Per consentire l'accesso al file system, seleziona Automatically create and attach security groups (Crea e allega automaticamente i gruppi di sicurezza). Selezionando questa casella di controllo, i seguenti gruppi di sicurezza verranno automaticamente creati e collegati all'istanza e alle destinazioni di montaggio del file system:

- Gruppo di sicurezza dell'istanza: include una regola in uscita che consente il traffico sulla porta NFS 2049, ma non include regole in entrata.
- Gruppo di sicurezza delle destinazioni di montaggio del file system: include una regola in entrata che consente il traffico sulla porta NFS 2049 dal gruppo di sicurezza dell'istanza (descritta sopra) e una regola in uscita che consente il traffico sulla porta NFS 2049.

> **Note**
>
> In alternativa, è possibile creare e collegare manualmente i gruppi di sicurezza. Se vuoi creare e allegare manualmente i gruppi di sicurezza, deseleziona Automatically create and attach the required security groups (Crea e allega automaticamente i gruppi di sicurezza richiesti).

e. Per montare automaticamente il file system condiviso all'avvio dell'istanza, seleziona Automatically mount shared file system by attaching required user data script (Monta automaticamente il file system condiviso allegando lo script di dati utente richiesto). Per visualizzare i dati utente generati automaticamente, espandi Advanced details (Dettagli avanzati) e scorri verso il basso fino a User data (Dati utente).

> **Note**
>
> Se sono stati aggiunti dati utente prima di selezionare questa casella di controllo, i dati utente originali vengono sovrascritti dai dati utente generati automaticamente.

9. Configura qualsiasi altra impostazione di configurazione dell'istanza in base alle esigenze.
10. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

Testare il file system EFS

Puoi connetterti alla tua istanza e verificare che il file system sia montato nella directory specificata (ad esempio,/mnt/efs).

Per verificare che il file system sia montato

1. Connettiti alla tua istanza. Per ulteriori informazioni, consulta Connessione a un'istanza Linux tramite SSH.
2. Dalla finestra del terminale dell'istanza esegui il comando df -T per verificare che il file system EFS sia montato.

```
$ df -T
Filesystem     Type              1K-blocks    Used          Available Use% Mounted
 on
/dev/xvda1     ext4                8123812 1949800            6073764  25% /
devtmpfs       devtmpfs            4078468      56            4078412   1% /dev
tmpfs          tmpfs               4089312       0            4089312   0% /dev/shm
efs-dns        nfs4       9007199254740992       0   9007199254740992   0% /mnt/efs
```

   Nota che il nome del file system, mostrato nell'output di esempio as*efs-dns*, ha la forma seguente.

```
file-system-id.efs.aws-region.amazonaws.com:/
```

3. (Facoltativo) Crea un file nel file system dall'istanza, quindi verifica di poter visualizzare il file da un'altra istanza.

   a. Dall'istanza, esegui il comando seguente per creare il file.

```
$ sudo touch /mnt/efs/test-file.txt
```

   b. Dall'altra istanza, esegui il comando seguente per visualizzare il file.

```
$ ls /mnt/efs
test-file.txt
```

Eliminare il file system EFS

Se il file system non è più necessario, puoi eliminarlo.

Per eliminare il file system

1. Apri la console di Amazon Elastic File System all'indirizzo https://console.aws.amazon.com/efs/.
2. Selezionare il file system da eliminare.
3. Scegliere Actions (Operazioni), Delete file system (Elimina file system).
4. Quando viene richiesta la conferma, immettere l'ID del file system e scegliere Delete file system (Elimina file system).

Utilizzo di Amazon FSx con istanze Amazon EC2

La famiglia di servizi Amazon FSx semplifica l'avvio, l'esecuzione e il dimensionamento dell'archivio condiviso basato su file system commerciali e open source più diffusi. Puoi utilizzare la nuova procedura guidata di avvio dell'istanza per collegare automaticamente i seguenti tipi di file system Amazon FSx alle istanze Amazon EC2 al momento dell'avvio:

- Amazon FSx for NetApp ONTAP fornisce uno storage condiviso completamente gestito nel AWS cloud con le popolari funzionalità di accesso e gestione dei dati di NetApp ONTAP.
- Amazon FSx for OpenZFS offre un archivio condiviso a costi contenuti completamente gestito con il popolare file system OpenZFS.

> **Note**
>
> - Questa funzionalità è disponibile solo nella procedura guidata di avvio dell'istanza. Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.
> - I file system Amazon FSx per Windows File Server e Amazon FSx per Lustre non possono essere montati all'avvio . È necessario montare questi file system manualmente dopo l'avvio.

È possibile scegliere di montare un file system esistente creato in precedenza oppure creare un nuovo file system da montare su un'istanza all'avvio.

Argomenti

- Script di dati utente e gruppi di sicurezza
- Montaggio di un file system Amazon FSx all'avvio

Script di dati utente e gruppi di sicurezza

Quando si monta un file system Amazon FSx su un'istanza utilizzando la procedura guidata di avvio dell'istanza, è possibile scegliere se creare e allegare automaticamente i gruppi di sicurezza necessari per abilitare l'accesso al file system e se includere automaticamente gli script di dati utente necessari per montare il file system e renderlo disponibile per l'uso.

Argomenti

- Gruppi di sicurezza
- Script di dati utente

Gruppi di sicurezza

Se si sceglie di creare automaticamente i gruppi di sicurezza necessari per abilitare l'accesso al file system, la procedura guidata di avvio dell'istanza crea e allega due gruppi di protezione: un gruppo di sicurezza è collegato all'istanza e l'altro è collegato al file system. Per ulteriori informazioni sui requisiti del gruppo di sicurezza, consulta FSx for ONTAP file system access control with Amazon VPC (Controllo degli accessi al file system FSx for ONTAP con Amazon VPC) e FSx for OpenZFS file system access control with Amazon VPC (Controllo degli accessi al file system FSx for OpenZFS).

Aggiungiamo il tag `Name=instance-sg-`*`1`* al gruppo di sicurezza creato e collegato all'istanza. Il valore del tag viene incrementato automaticamente ogni volta che la procedura guidata di avvio dell'istanza crea un nuovo gruppo di sicurezza per i file system Amazon FSx.

Il gruppo di sicurezza include le regole in uscita indicate di seguito, ma nessuna regola in entrata.

Regole in uscita

Tipo di protocollo	Numero della porta	Destinazione
UDP	111	*file system security group*
UDP	20001 - 20003	*file system security group*

Tipo di protocollo	Numero della porta	Destinazione
UDP	4049	*file system security group*
UDP	2049	*file system security group*
UDP	635	*file system security group*
UDP	4045 - 4046	*file system security group*
TCP	4049	*file system security group*
TCP	635	*file system security group*
TCP	2049	*file system security group*
TCP	111	*file system security group*
TCP	4045 - 4046	*file system security group*
TCP	20001 - 20003	*file system security group*
Tutti	Tutti	*file system security group*

Il gruppo di sicurezza creato e collegato al file system è contrassegnato con il tag `Name=fsx-sg-`*1*. Il valore del tag viene incrementato automaticamente ogni volta che la procedura guidata di avvio dell'istanza crea un nuovo gruppo di sicurezza per i file system Amazon FSx.

Il gruppo di sicurezza include le regole seguenti.

Regole in entrata

Tipo di protocollo	Numero della porta	Origine
UDP	2049	*instance security group*
UDP	20001 - 20003	*instance security group*
UDP	4049	*instance security group*
UDP	111	*instance security group*

Tipo di protocollo	Numero della porta	Origine
UDP	635	*instance security group*
UDP	4045 - 4046	*instance security group*
TCP	4045 - 4046	*instance security group*
TCP	635	*instance security group*
TCP	2049	*instance security group*
TCP	4049	*instance security group*
TCP	20001 - 20003	*instance security group*
TCP	111	*instance security group*

Regole in uscita

Tipo di protocollo	Numero della porta	Destinazione
Tutti	Tutti	0.0.0. 0/0

Script di dati utente

Se si sceglie di allegare automaticamente gli script di dati utente, la procedura guidata di avvio dell'istanza aggiunge i seguenti dati utente all'istanza. Questo script installa i pacchetti necessari, monta il file system e aggiorna le impostazioni dell'istanza in modo che il file system venga rimontato automaticamente ogni volta che l'istanza viene riavviata.

```
#cloud-config
package_update: true
package_upgrade: true
runcmd:
- yum install -y nfs-utils
- apt-get -y install nfs-common
- svm_id_1=svm_id
- file_system_id_1=file_system_id
- vol_path_1=/vol1
```

```
- fsx_mount_point_1=/mnt/fsx/fs1
- mkdir -p "${fsx_mount_point_1}"
- if [ -z "$svm_id_1" ]; then printf "\n${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
 0 0\n" >> /etc/fstab; else printf "\n${svm_id_1}.${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0\n" >> /etc/fstab; fi
- retryCnt=15; waitTime=30; while true; do mount -a -t nfs4 defaults; if [ $? = 0 ] ||
 [ $retryCnt -lt 1 ]; then echo File system mounted successfully; break; fi; echo File
 system not available, retrying to mount.; ((retryCnt--)); sleep $waitTime; done;
```

Montaggio di un file system Amazon FSx all'avvio

Come montare un file system Amazon FSx nuovo o esistente all'avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e quindi scegli Launch instance (Avvia istanza) per aprire la procedura guidata di avvio dell'istanza.
3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona l'AMI da utilizzare.
4. Nella sezione Instance type (Tipo di istanza), seleziona il tipo di istanza.
5. Nella sezione Key pair (Coppia di chiavi), seleziona una coppia di chiavi esistenti o creane una nuova.
6. Nella sezione Network settings (Impostazioni di rete), procedi nel seguente modo:

    a. Scegli Modifica.

    b. Se vuoi montare un file system esistente, in Subnet (Sottorete), scegli la sottorete preferita del file system. Ti consigliamo di avviare l'istanza nella stessa zona di disponibilità della sottorete preferita del file system per ottimizzare le prestazioni.

    Se vuoi creare un nuovo file system da montare su un'istanza, in Subnet (Sottorete), scegli la sottorete in cui avviare l'istanza.

> **Important**
>
> È necessario selezionare una sottorete per abilitare la funzionalità Amazon FSx nella nuova procedura guidata di avvio dell'istanza. Se non si seleziona una sottorete, non sarà possibile montare un file system esistente o crearne uno nuovo.

7. Nella sezione Storage (Archiviazione), procedi come segue:

   a. Configura i volumi secondo necessità.

   b. Espandi la sezione File systems (File system) e seleziona FSx.

   c. Scegli Add shared file system (Aggiungi file system condiviso).

   d. In File system, seleziona il file system da montare.

   > **Note**
   >
   > L'elenco mostra tutti i file system Amazon FSx for NetApp ONTAP e Amazon FSx for OpenZFS presenti nel tuo account nella regione selezionata.

   e. Per creare e collegare automaticamente i gruppi di sicurezza necessari per abilitare l'accesso al file system, seleziona Automatically create and attach security groups (Crea e collega automaticamente gruppi di sicurezza). Se preferisci creare manualmente i gruppi di sicurezza, deseleziona la casella di controllo. Per ulteriori informazioni, consulta Gruppi di sicurezza.

   f. Per collegare automaticamente gli script di dati utente necessari per montare il file system, seleziona Automatically mount shared file system by attaching required user data script (Monta automaticamente il file system condiviso collegando lo script di dati utente richiesto). Se preferisci fornire manualmente gli script di dati utente, deseleziona la casella di controllo. Per ulteriori informazioni, consulta Script di dati utente.

8. Nella sezione Advanced (Avanzate), configura le impostazioni aggiuntive dell'istanza in base alle esigenze.

9. Scegli Avvia.

Usa Amazon File Cache con le EC2 istanze Amazon

Amazon File Cache fornisce una cache ad alta velocità completamente gestita AWS che semplifica l'elaborazione dei dati dei file, indipendentemente da dove sono archiviati. Amazon File Cache funge da posizione di archiviazione temporanea e ad alte prestazioni per i dati archiviati in file system on-premises, file system AWS e bucket Amazon Simple Storage Service (Amazon S3). Puoi utilizzare questa funzionalità per rendere disponibili set di dati dispersi per applicazioni basate su file AWS con una vista unificata e a velocità elevate, con latenze inferiori al millisecondo e throughput elevato. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon File Cache.

Amazon File Cache funziona con i sistemi Linux AMIs più diffusi ed è compatibile con i tipi di istanza basati su x86 e i tipi di istanze Graviton. Puoi accedere alla cache dalle tue EC2 istanze Amazon utilizzando il client Lustre open source. Puoi montare la cache e quindi lavorare con i file e le directory in essa contenuti utilizzando i comandi Linux standard. EC2 Le istanze Amazon possono accedere alla cache da altre zone di disponibilità all'interno dello stesso cloud privato virtuale (VPC), a condizione che la configurazione di rete consenta l'accesso tra sottoreti all'interno del VPC. È anche possibile creare una cache in un VPC condiviso.

Per iniziare, consulta la sezione Guida introduttiva ad Amazon File Cache nella Guida per l'utente di Amazon File Cache.

Gestione delle risorse Amazon EC2.

Una risorsa è un'entità utilizzabile. Amazon EC2 crea risorse man mano che utilizzi le funzionalità del servizio. Ad esempio, le risorse di Amazon EC2 includono immagini, istanze, parchi, coppie di chiavi e gruppi di sicurezza. Tutti i tipi di risorse Amazon EC2 includono attributi che descrivono le risorse. Ad esempio, nomi, descrizioni, identificatori di risorse e Amazon Resource Name (ARN).

Le risorse Amazon EC2 sono specifiche della AWS regione o della zona in cui risiedono. Ad esempio, un'Amazon Machine Image (AMI) è specifica per una AWS regione, ma l'istanza avviata da un'AMI è specifica della zona in cui viene avviata. Puoi specificare una risorsa Amazon EC2 in una politica di autorizzazioni utilizzando il relativo ARN.

Hai delle Account AWS quote predefinite per Amazon EC2. Queste quote definiscono il numero massimo di risorse che è possibile creare. Ad esempio, esistono quote per il numero massimo di vCPU tra le istanze in esecuzione. Se l'avvio di un'istanza o l'avvio di un'istanza interrotta provocano il superamento della quota stabilita, l'operazione ha esito negativo.

Puoi cercare risorse specifiche nella tua Account AWS regione, utilizzando ID o tag delle risorse. Per cercare risorse o tipi di risorse specifici in più Regioni, usa Amazon EC2 Global View.

Indice

- Selezione di una regione per le risorse Amazon EC2
- Trova le risorse Amazon EC2
- Visualizza le risorse tra le regioni utilizzando AWS Global View
- Tagging delle risorse Amazon EC2.
- Service Quotas di Amazon EC2

Selezione di una regione per le risorse Amazon EC2

Le risorse Amazon EC2 sono specifiche della AWS regione o della zona in cui risiedono. Quando crei una risorsa Amazon EC2, selezioni la regione per la risorsa.

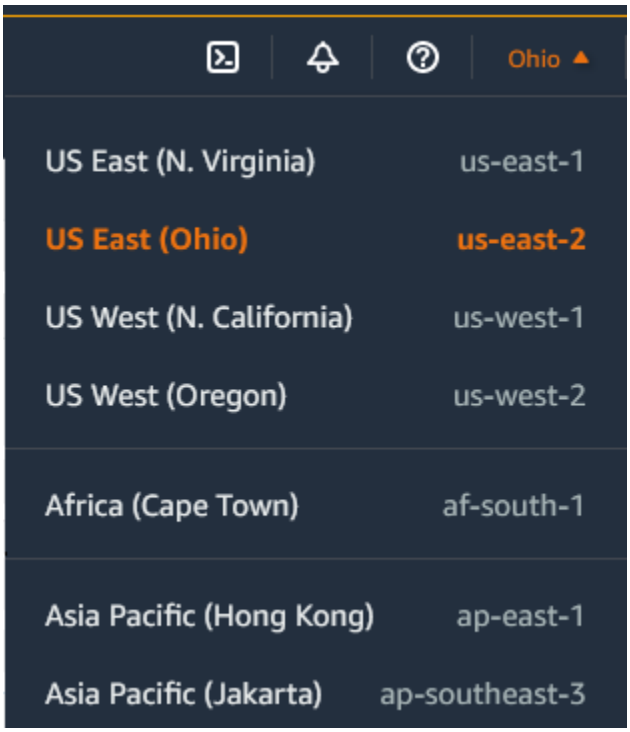
Considerazioni

- Alcune AWS risorse potrebbero non essere disponibili in tutte le regioni. Assicurati di poter creare tutte le AWS risorse di cui hai bisogno in una regione prima di iniziare a creare risorse in una regione.

- Alcune regioni sono disabilitate per impostazione predefinita. È necessario abilitare queste regioni prima di poterle utilizzare. Per ulteriori informazioni, consulta AWS Regions.

Per selezionare una regione per una risorsa tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, scegli il selettore Regions (Regioni) e seleziona la regione.



3. Il selettore Regioni include tutte le risorse disponibili per l'uso in Account AWS. Scegli il testo sottolineato nella parte inferiore dell'elenco per visualizzare le regioni che non sono abilitate per il tuo account.

Per selezionare una regione per una risorsa utilizzando AWS CLI

È possibile configurare l'uso AWS CLI di una regione predefinita. Se non specifichi una regione nel comando, viene utilizzata la regione predefinita. Per utilizzare una regione diversa per un comando specifico, aggiungi la seguente opzione.

```
--region us-east-1
```

Per selezionare una regione per una risorsa utilizzando gli Strumenti per PowerShell

È possibile configurare gli Strumenti per Windows in PowerShell modo che utilizzino una regione predefinita. Se non specifichi una regione in un comando, viene utilizzata la regione predefinita. Per utilizzare una regione diversa per un comando specifico, aggiungi il seguente parametro.

```
-Region us-east-1
```

Trova le risorse Amazon EC2

Puoi ottenere un elenco di alcuni tipi di risorse tramite la console Amazon EC2. Puoi ottenere un elenco di ciascun tipo di risorsa tramite il comando o l'operazione API corrispondente. Se disponi di molte risorse, puoi filtrare i risultati in modo da includere o escludere solo le risorse che corrispondono a determinati criteri.

Indice

- Elencare e filtrare le risorse utilizzando la console
- Elenca e filtra utilizzando la riga di comando
- Visualizza le risorse tra le regioni utilizzando AWS Global View

Elencare e filtrare le risorse utilizzando la console

Indice

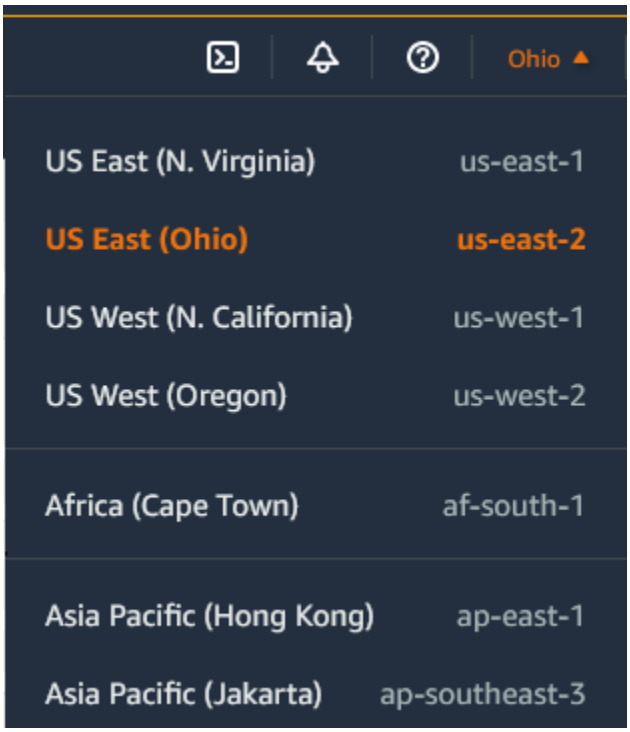
- Elencare le risorse mediante la console
- Filtrare le risorse mediante la console
  - Filtri supportati
- Salva i set di filtri mediante la console
  - Funzionalità principali
  - Crea un set di filtri
  - Modifica un set di filtri
  - Elimina un set di filtri

Elencare le risorse mediante la console

Puoi visualizzare i tipi di risorse Amazon EC2 più frequenti tramite la console. Per visualizzare risorse aggiuntive, utilizza l'interfaccia a riga di comando o le operazioni API.

Per elencare le risorse EC2 tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Le risorse Amazon EC2 sono specifiche di Regione AWS. Nella barra di navigazione, scegli una regione dal selettore Regioni.



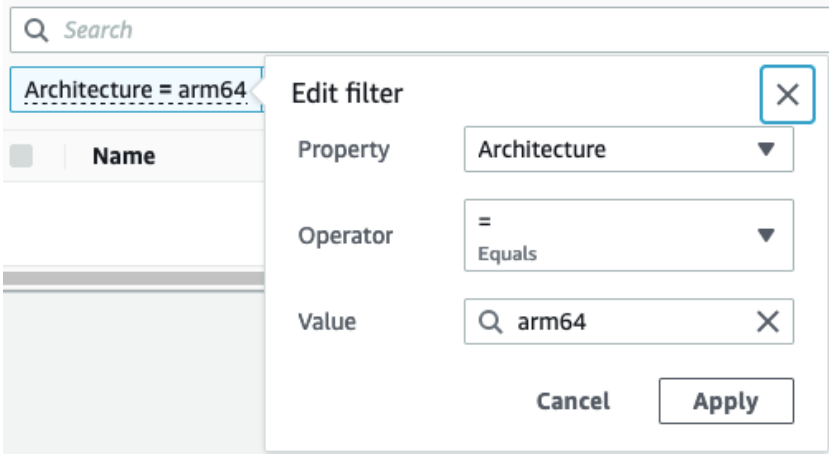
3. Nel riquadro di navigazione scegliere l'opzione corrispondente al tipo di risorsa. Ad esempio, per elencare tutte le istanze, scegliere Istanze.

Filtrare le risorse mediante la console

Per filtrare un elenco di risorse

1. Nel riquadro di navigazione selezionare un tipo di risorsa, ad esempio Instances (Istanze).
2. Selezionare il campo di ricerca.
3. Selezionare il filtro dall'elenco.
4. Selezionare un operatore, ad esempio = (uguale a). Per alcuni attributi è possibile selezionare più operatori. Nota: non tutte le schermate supportano la selezione di un operatore.
5. Seleziona un valore di filtro.

6. Per modificare un filtro selezionato, scegli il token del filtro (casella blu), apporta le modifiche richieste e quindi scegli Apply (Applica). Nota: non tutte le schermate supportano la modifica del filtro selezionato.



7. Al termine, rimuovere il filtro.

Filtri supportati

La console Amazon EC2 supporta due tipi di filtraggio.

- Il filtro API viene applicato sul lato server. Il filtro viene applicato alla chiamata API e riduce il numero di risorse restituite dal server. Consente un filtraggio rapido tra grandi insiemi di risorse e può ridurre i tempi e i costi di trasferimento dei dati tra il server e il browser. Il filtro API supporta gli operatori = (uguale a) e : (contiene) e fa sempre distinzione tra maiuscole e minuscole.
- Il filtro client avviene sul lato client. Consente di filtrare i dati già disponibili nel browser (in altre parole, i dati che sono già stati restituiti dall'API). Il filtro client funziona bene in combinazione con un filtro API per filtrare set di dati più piccoli nel browser. Oltre agli operatori = (uguale a) e : (contiene), il filtro client può anche supportare gli operatori di intervallo, come >= (maggiore o uguale a) e gli operatori di negazione (inverso) come != (non è uguale).

La console Amazon EC2 supporta i seguenti tipi di ricerche:

Ricerca per parola chiave

La ricerca per parola chiave è una ricerca a testo libero che consente di cercare un valore in tutti gli attributi o i tag delle risorse, senza specificare una chiave di attributo o di tag da cercare.

> **Note**
>
> Tutte le ricerche per parole chiave utilizzano il filtro client.

Per eseguire la ricerca per parola chiave, digita o incolla quello che stai cercando nel campo di ricerca, quindi scegli Enter (Invia). Ad esempio, la ricerca `123` corrisponde a tutte le istanze che hanno 123 in uno qualsiasi dei relativi attributi, ad esempio un indirizzo IP, un ID istanza, un ID VPC o un ID AMI, o in uno qualsiasi dei relativi tag, come il Nome. Se la ricerca a testo libero restituisce corrispondenze impreviste, applica filtri aggiuntivi.

Ricerca per attributo

La ricerca per attributo consente di cercare un attributo specifico in tutte le risorse.

> **Note**
>
> Le ricerche degli attributi utilizzano filtri API o filtri client, a seconda dell'attributo selezionato. Quando si esegue una ricerca di attributi, gli attributi vengono raggruppati di conseguenza.

Ad esempio puoi cercare nell'attributo Instance state (Stato istanza) tutte le istanze in modo da restituire solo le istanze che si trovano nello stato `stopped`. Per farlo:

1. Nel campo di ricerca nella schermata Instances (Istanze), inizia a immettere `Instance state`. Quando si immettono i caratteri, vengono visualizzati i due tipi di filtri per Instance state (Stato istanza): API filters (Filtri API) e Client filters (Filtri client).
2. Per eseguire la ricerca sul lato server, scegli Instance state (Stato istanza) in API filters (Filtri API). Per eseguire la ricerca sul lato client, scegli Instance state (client) (Stato istanza) (client) in Client filters (Filtri client).

   Viene visualizzato un elenco di possibili operatori per l'attributo selezionato.
3. Scegli l'operatore = (uguale a).

   Viene visualizzato un elenco di possibili valori per l'attributo e l'operatore selezionati.
4. Seleziona Stopped (Interrotto) dall'elenco.

Ricerca per tag

La ricerca per tag consente di filtrare le risorse nella tabella attualmente visualizzata in base a una chiave di tag o un valore di tag.

Le ricerche per tag utilizzano il filtro API o il filtro client, a seconda delle impostazioni nella finestra Preferences (Preferenze).

Per utilizzare il filtro API per i tag

1. Apri la finestra Preferenze.
2. Deseleziona la casella di spunta Usa corrispondenza espressioni regolari. Se questa casella di controllo è selezionata, viene applicato il filtro client.
3. Seleziona la casella di controllo Use case sensitive matching (Usa corrispondenza tra maiuscole e minuscole). Se questa casella di controllo è deselezionata, viene applicato il filtro client.
4. Scegli Conferma.

Quando si esegue una ricerca per tag, è possibile utilizzare i valori seguenti:

- (empty) (vuoto): trova tutte le risorse con la chiave di tag specificata, ma non deve essere presente alcun valore di tag.
- All values (Tutti i valori): trova tutte le risorse con la chiave di tag specificata e qualsiasi valore di tag.
- Senza tag: trova tutte le risorse che non hanno la chiave di tag specificata.
- Il valore visualizzato: trova tutte le risorse con la chiave di tag specificata e il valore di tag specificato.

È possibile utilizzare le seguenti tecniche per migliorare o perfezionare le ricerche:

Ricerca inversa

Le ricerche inverse consentono di cercare risorse che non corrispondono a un valore specificato. Nelle schermate Instances (Istanze) e AMI, le ricerche inverse vengono eseguite selezionando l'operatore != (non è uguale) o !: (non contiene) e successivamente selezionando un valore. In altre schermate, le ricerche inverse vengono eseguite aggiungendo un prefisso carattere punto esclamativo (!) alla parola chiave di ricerca.

> **Note**
>
> La ricerca inversa è supportata solo con le ricerche di parole chiave e attributi nei filtri client. Non è supportato con le ricerche di attributi nei filtri API.

Ad esempio puoi cercare nell'attributo Instance state (Stato istanza) tutte le istanze in modo da escludere le istanze che si trovano nello stato `terminated`. Per farlo:

1. Nel campo di ricerca nella schermata Instances (Istanze), inizia a immettere `Instance state`. Quando si immettono i caratteri, vengono visualizzati i due tipi di filtri per Instance state (Stato istanza): API filters (Filtri API) e Client filters (Filtri client).
2. In Client filters (Filtri client), scegli Instance state (client) (Stato istanza (client)). La ricerca inversa è supportata solo sui filtri client.

   Viene visualizzato un elenco di possibili operatori per l'attributo selezionato.
3. Scegli != (non è uguale), quindi scegli terminated (terminato).

Per filtrare le istanze in base a un attributo di stato dell'istanza, è inoltre possibile utilizzare le icone di ricerca
()
nella colonna Instance state (Stato istanza). L'icona di ricerca con un segno più (+) visualizza tutte le istanze corrispondenti a tale attributo. L'icona di ricerca con un segno meno (-) esclude tutte le istanze corrispondenti a tale attributo.

Ecco un altro esempio di utilizzo della ricerca inversa: per elencare tutte le istanze a cui non è assegnato il gruppo di sicurezza denominato `launch-wizard-1`, in Client filters, (Filtri client), esegui la ricerca in base all'attributo Security group name (Nome gruppo di sicurezza), scegli != e inserisci la parola chiave `launch-wizard-1` nella barra di ricerca.

Ricerca parziale

Con le ricerche parziali, è possibile cercare valori di stringa parziali. Per eseguire una ricerca parziale, immettere solo una parte della parola chiave da cercare. Nelle schermate Instances (Istanze) e AMI, le ricerche parziali possono essere eseguite solo con l'operatore : (contiene). In altre schermate, è possibile selezionare l'attributo del filtro client e inserire immediatamente solo una parte della parola chiave che si desidera cercare. Ad esempio, nella schermata Instance type (Tipo di istanza), per cercare tutte le istanze `t2.micro`, `t2.small` e `t2.medium` è possibile

eseguire la ricerca in base all'attributo Instance Type (Tipo di istanza) e inserire la parola chiave `t2`.

Ricerca di espressioni regolari

Per utilizzare le ricerche con espressioni regolari, è necessario selezionare la casella di controllo Usa corrispondenza espressioni regolari nella finestra Preferenze.

Le espressioni regolari sono utili quando devi far corrispondere i valori in un campo con un modello specifico. Ad esempio, per cercare un valore che inizia con `s`, cercare `^s`. Per cercare un valore che termina con `xyz`, cercare `xyz$`. Oppure per cercare un valore che inizia con un numero seguito da uno o più caratteri, cercare `[0-9]+.*`.

> **Note**
>
> La ricerca con espressioni regolari è supportata solo con ricerche per parole chiave e ricerche di attributi nei filtri client. Non è supportato con le ricerche di attributi nei filtri API.

Case-sensitive cerca

Per utilizzare le ricerche con distinzione tra maiuscole e minuscole, è necessario selezionare la casella di controllo Use case sensitive matching (Usa corrispondenza tra maiuscole e minuscole) nella finestra Preferences (Preferenze). Questa preferenza si applica solo ai filtri client e tag.

> **Note**
>
> I filtri API fanno sempre distinzione tra maiuscole e minuscole.

Ricerca con caratteri jolly

Utilizzare il carattere jolly `*` per abbinare zero o più caratteri. Utilizzare il carattere jolly `?` per corrispondere a zero o a un carattere. Ad esempio, se si dispone di un set di dati con i valori `prod`, `prods` e `production`, la ricerca di `prod*` corrisponde a tutti i valori, mentre `prod?` corrisponde solo a `prod` e `prods`. Per utilizzare i valori letterali, utilizzare il carattere escape barra rovesciata (\). Ad esempio, "`prod\*`" corrisponde a `prod*`.

> **Note**
>
> La ricerca con caratteri jolly è supportata solo con le ricerche di attributi e tag nei filtri API. Non è supportata con le ricerche per parole chiave e con le ricerche di attributi e tag nei filtri client.

Combinazione di ricerche

In generale, più filtri con lo stesso attributo vengono automaticamente uniti con `OR`. Ad esempio, la ricerca `Instance State : Running` e `Instance State : Stopped` restituisce tutte le istanze in esecuzione O arrestate. Per unire la ricerca con `AND`, cerca tra diversi attributi. Ad esempio, la ricerca `Instance State : Running` e `Instance Type : c4.large` restituisce solo le istanze di tipo `c4.large` E che si trovano in stato di esecuzione.

Salva i set di filtri mediante la console

Un set di filtri salvato è un gruppo personalizzato di filtri che puoi creare e riutilizzare per visualizzare in modo efficiente le tue risorse Amazon EC2. Questa funzionalità aiuta a semplificare il flusso di lavoro, consentendo un accesso rapido a visualizzazioni di risorse specifiche.

I set di filtri salvati sono supportati solo nella console Amazon EC2 e attualmente sono disponibili solo per la pagina Volumi.

Funzionalità principali

- Personalizzazione: crea set di filtri su misura per le tue esigenze. Ad esempio, puoi creare un set di filtri per visualizzare solo i volumi `gp3` creati dopo una data specificata.
- Filtro predefinito: imposta un set di filtri predefinito per una pagina e i filtri predefiniti vengono applicati automaticamente quando si accede alla pagina. Se non è impostato alcun valore predefinito, non viene applicato alcun filtro.
- Applicazione semplice: seleziona un set di filtri salvato per applicarlo immediatamente. Amazon EC2 visualizza quindi le risorse pertinenti, con i filtri attivi indicati da token blu.
- Flessibilità: crea, modifica ed elimina i set di filtri in base alle esigenze.

Crea un set di filtri

Per creare un nuovo set di filtri

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Volumes (Volumi).

> **Note**
>
> Attualmente i set di filtri salvati sono disponibili solo per i volumi.

3. Nel campo di ricerca, seleziona i filtri per il tuo set di filtri.
4. Scegli la freccia accanto al pulsante Cancella filtri e scegli Salva nuovo set di filtri.
5. Nella finestra Salva set di filtri, procedi come segue:
   a. Per Nome set di filtri, inserisci un nome per il set di filtri.
   b. (Facoltativo) Per Descrizione set di filtri, immetti una descrizione per il set di filtri.
   c. (Facoltativo) Per impostare il set di filtri come filtro predefinito, selezionate la casella Imposta come predefinito.

   > **Note**
   >
   > Il filtro predefinito viene applicato automaticamente ogni volta che apri la pagina della console.

   d. Scegli Save (Salva).

Modifica un set di filtri

Per modificare un set di filtri

1. Dall'elenco Set di filtri salvati, seleziona il filtro da modificare.
2. Per aggiungere un filtro, nel campo di ricerca, seleziona un filtro da aggiungere al set di filtri. Per eliminare un filtro dal set, scegli la X sul token del filtro.
3. Scegli la freccia accanto al pulsante Cancella filtri e scegli Modifica set di filtri.
4. Nella finestra Modifica set di filtri, effettua le seguenti operazioni:

a. (Facoltativo) Per impostare il set di filtri come filtro predefinito, selezionate la casella Imposta come predefinito.

> **Note**
>
> Il filtro predefinito viene applicato automaticamente ogni volta che apri la pagina della console.

b. Scegli Modifica.

Elimina un set di filtri

Per eliminare un set di filtri

1. Dall'elenco Set di filtri salvati, seleziona il filtro da eliminare.
2. Scegli la freccia accanto al pulsante Cancella filtri e scegli Elimina set di filtri.
3. Nella finestra Elimina set di filtri, controlla il filtro per confermare che si tratti del filtro che desideri eliminare, quindi scegli Elimina.

Elenca e filtra utilizzando la riga di comando

Ogni tipo di risorsa ha delle azioni API corrispondenti che puoi utilizzare per descrivere, elencare o ottenere risorse di quel tipo. Gli elenchi di risorse risultanti possono essere lunghi, quindi può essere più veloce e più utile filtrare i risultati in modo da includere solo le risorse corrispondenti a criteri specifici.

Considerazioni sui filtri

- Puoi specificare fino a 50 filtri e fino a 200 valori di filtro totali in una singola richiesta.
- Le stringhe di filtro possono contenere fino a 255 caratteri.
- Puoi anche utilizzare caratteri jolly con i valori di filtro. Un asterisco (*) corrisponde a 0 o più caratteri, mentre un punto interrogativo (?) corrisponde a 0 o un carattere.
- I valori di filtro fanno distinzione tra maiuscole e minuscole.
- La ricerca può includere i valori letterali dei caratteri jolly; basta inserirli come caratteri escape con una barra rovesciata prima del carattere. Ad esempio, un valore di `\*amazon\?\\` ricerca la stringa letterale `*amazon?\`.

- Non è possibile specificare un valore di filtro di null. Utilizza invece il filtro lato client. Ad esempio, il comando seguente utilizza l'opzione --query e restituisce gli ID delle istanze che sono state avviate senza una key pair.

```
aws ec2 describe-instances \
    --query 'Reservations[*].Instances[?!not_null(KeyName)].InstanceId' \
    --output text
```

AWS CLI

Example Esempio: specificare un singolo filtro

È possibile elencare le istanze Amazon EC2 utilizzando describe-instances. Senza filtri, la risposta contiene informazioni su tutte le tue risorse. Puoi utilizzare l'opzione seguente per includere solo le istanze in esecuzione nell'output.

```
--filters Name=instance-state-name,Values=running
```

Per elencare solo gli ID di istanza per le istanze in esecuzione, aggiungere l'opzione `--query` come indicato di seguito.

```
--query "Reservations[*].Instances[*].InstanceId"
```

Example Esempio: specificare più filtri o valori filtro

Se si specificano più filtri o più valori filtro, la risorsa deve corrispondere a tutti i filtri da includere nell'output.

Puoi utilizzare il comando seguente per elencare tutte le istanze il cui tipo è `m5.large` o `m5d.large`.

```
--filters Name=instance-type,Values=m5.large,m5d.large
```

Puoi utilizzare il comando seguente per elencare tutte le istanze interrotte il cui tipo è `t2.micro`.

```
--filters Name=instance-state-name,Values=stopped Name=instance-type,Values=t2.micro
```

Example Esempio: utilizzare caratteri jolly in un valore di filtro

Puoi utilizzare l'opzione seguente con describe-snapshots per restituire solo gli snapshot la cui descrizione è "database".

```
--filters Name=description,Values=database
```

Il carattere jolly * corrisponde a zero o più caratteri. Puoi utilizzare la seguente opzione per restituire solo gli snapshot la cui descrizione include la parola database.

```
--filters Name=description,Values=*database*
```

Il carattere jolly ? corrisponde esattamente a 1 carattere. Puoi utilizzare l'opzione seguente per restituire solo gli snapshot la cui descrizione è "database" o "database" seguito da un carattere.

```
--filters Name=description,Values=database?
```

Puoi utilizzare l'opzione seguente per restituire solo gli snapshot la cui descrizione è "database" seguito da un massimo di quattro caratteri. Questo esclude le descrizioni con "database" seguite da cinque o più caratteri.

```
--filters Name=description,Values=database????
```

Example Esempio: filtro in base alla data

Con AWS CLI, è possibile utilizzare JMESPath per filtrare i risultati utilizzando espressioni. Ad esempio, il describe-snapshots comando seguente visualizza gli ID di tutte le istantanee create dall'utente specificato Account AWS prima della data specificata. Se non si specifica il proprietario, i risultati includono tutti gli snapshot pubblici.

```
aws ec2 describe-snapshots \
    --filters Name=owner-id,Values=123456789012 \
    --query "Snapshots[?(StartTime<='2024-03-31')].[SnapshotId]" \
    --output text
```

L'esempio seguente visualizza gli ID di tutti gli snapshot creati nell'intervallo di date specificato.

```
aws ec2 describe-snapshots \
```

```
    --filters Name=owner-id,Values=123456789012 \
    --query "Snapshots[?(StartTime>='2024-01-01') && (StartTime<='2024-12-31')].
[SnapshotId]" \
    --output text
```

Esempio: filtro basato su tag

Per esempi su come filtrare un elenco di risorse in base ai relativi tag, consulta Filtra le risorse Amazon EC2 per tag.

PowerShell

Example Esempio: specificare un singolo filtro

È possibile elencare le istanze Amazon EC2 utilizzando Get-EC2Instance. Senza filtri, la risposta contiene informazioni su tutte le tue risorse. Puoi utilizzare il parametro seguente per includere solo le istanze in esecuzione nell'output.

```
-Filter @{Name="instance-state-name"; Values="running"}
```

L'esempio seguente elenca solo gli ID delle istanze in esecuzione.

```
(Get-EC2Instance -Filter @{Name="instance-state-name"; Values="stopped"}).Instances
 | Select InstanceId
```

Example Esempio: specificare più filtri o valori filtro

Se si specificano più filtri o più valori filtro, la risorsa deve corrispondere a tutti i filtri da includere nei risultati.

Puoi utilizzare il comando seguente per elencare tutte le istanze il cui tipo è `m5.large` o `m5d.large`.

```
-Filter @{Name="instance-type"; Values="m5.large", "m5d.large"}
```

Puoi utilizzare il comando seguente per elencare tutte le istanze interrotte il cui tipo è `t2.micro`.

```
-Filter @{Name="instance-state-name"; Values="stopped"}, @{Name="instance-type";
 Values="t2.micro"}
```

Visualizza le risorse tra le regioni utilizzando AWS Global View

AWS Global View ti consente di visualizzare e cercare risorse in una singola AWS regione o in più regioni contemporaneamente in un'unica console. Per ulteriori informazioni, consulta Visualizza le risorse tra le regioni utilizzando AWS Global View.

Visualizza le risorse tra le regioni utilizzando AWS Global View

AWS Global View ti consente di visualizzare alcune delle tue risorse in una singola AWS regione o in più regioni in un'unica console. AWS Global View offre anche una funzionalità di ricerca globale che consente di cercare risorse specifiche o tipi di risorse specifici in più regioni contemporaneamente.

AWS Global View non consente di modificare le risorse in alcun modo.

Risorse supportate

Utilizzando AWS Global View, puoi visualizzare un riepilogo globale delle seguenti risorse in tutte le regioni per le quali Account AWS è abilitato.

- Gruppi Auto Scaling
- Zone di disponibilità
- Prenotazioni della capacità e blocchi di capacità
- Cluster database
- Istanze DB
- Set opzioni DHCP
- Cluster Amazon Elastic Container Service (Amazon ECS)
- Servizi ECS
- Attività ECS
- Egress-only gateway Internet
- IP elastici
- Servizi endpoint
- Istanze
- Gateway Internet
- Elenchi di prefissi gestiti
- Gateway NAT

- Liste di controllo accessi (ACL) di rete
- Interfacce di rete
- Outposts
- Tabelle di instradamento
- Bucket S3
- Gruppi di sicurezza
- Sottoreti
- Volumi
- VPC
- Endpoint VPC
- Connessioni peering di VPC

Autorizzazioni richieste

Un utente deve disporre delle seguenti autorizzazioni per utilizzare AWS Global View.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "autoscaling:DescribeAutoScalingGroups",
      "ec2:DescribeRegions",
      "ec2:DescribeCapacityReservations",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeEgressOnlyInternetGateways",
      "ec2:DescribeAddresses",
      "ec2:DescribeVpcEndpointServices",
      "ec2:DescribeInstances",
      "ec2:DescribeInternetGateways",
      "ec2:DescribePrefixLists",
      "ec2:DescribeNatGateways",
      "ec2:DescribeNetworkAcls",
      "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeManagedPrefixLists",
        "ecs:ListClusters",
        "ecs:DescribeServices",
        "ecs:ListTasks",
        "outposts:ListOutposts",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
    }]
}
```

Per utilizzare AWS Global View

Accedi alla console AWS Global View.

> **Important**
>
> Non è possibile utilizzare una finestra privata in Firefox per accedere a AWS Global View.

La console include i seguenti elementi:

- Region explorer: questa pagina include le sezioni seguenti:
  - Riepilogo: fornisce una panoramica di alto livello delle risorse in tutte le Regioni.

    Espandi Mostra tutto il riepilogo delle risorse indica il numero di regioni per le quali Account AWS è abilitato. I campi rimanenti indicano il numero di risorse attualmente disponibili in tali Regioni. Scegli uno dei collegamenti per visualizzare le risorse di quel tipo in tutte le Regioni. Ad esempio, se il link sotto l'etichetta Instances (Istanze) è 29 in 10 Regioni, indica che attualmente

hai 29 istanze in 10 Regioni. Scegliere il collegamento per visualizzare un elenco di tutte le 29 istanze.

- Region explorer: elenca tutte le Regioni AWS (comprese quelle per le quali l'account non è abilitato) e fornisce i totali per ogni tipo di risorsa per ciascuna regione.

  Scegliere il nome di una regione per visualizzare tutte le risorse di tutti i tipi per la regione specifica. Ad esempio, scegli Africa (Città del Capo) af-south-1 per visualizzare tutti i VPC, le sottoreti, le istanze, i gruppi di sicurezza, i volumi e i gruppi con scalabilità automatica di tale regione. In alternativa, selezionare una regione e scegliere View resources for selected Region (Visualizza le risorse per la regione selezionata).

  Scegliere il valore per un tipo di risorsa specifico in una regione specifica per visualizzare solo le risorse di quel tipo in quella regione. Ad esempio, scegliere il valore di Istanze per Africa (Città del Capo) af-south-1 per visualizzare solo le istanze in quella regione.

- Global search: questa pagina consente di cercare risorse specifiche o tipi di risorse specifici in una singola regione o in più regioni. Consente inoltre di visualizzare i dettagli per una risorsa specifica.

  Per cercare le risorse, immettere i criteri di ricerca nel campo che precede la griglia. La ricerca può essere eseguita in base alla Regione, al tipo di risorsa e ai tag assegnati alle risorse.

  Per visualizzare i dettagli di una risorsa specifica, selezionala nella griglia. È possibile inoltre scegliere l'ID risorsa di una risorsa per aprirla nella console corrispondente. Ad esempio, scegli un ID istanza per aprire l'istanza nella console Amazon EC2 oppure scegli un ID sottorete per aprire la sottorete nella console Amazon VPC.

- Regioni e zone: questa pagina permette di visualizzare e gestire tutte le regioni, le zone locali e le zone Wavelength disponibili. Puoi passare dalla visualizzazione elenco alla visualizzazione mappa utilizzando l'interruttore Visualizzazione elenco/Visualizzazione mappa. La tua preferenza di visualizzazione persiste tra le sessioni.

  - Visualizzazione mappa: visualizza tutte le regioni e le zone su una mappa del mondo interattiva, colorata in base allo stato. Per visualizzare i dettagli di una località, posiziona il puntatore su di essa o sceglila. Scegli una località per agire: puoi abilitare una regione, abilitare una zona o aprirne la pagina dei dettagli. Puoi anche filtrare la mappa per mostrare solo stati specifici. La mappa e l'elenco dei dettagli rimangono sincronizzati: la selezione di una posizione su una la evidenzia sull'altra.
  - Visualizzazione a elenco: visualizza le regioni e le zone in una tabella. Dalla scheda Regioni, puoi visualizzare tutte le AWS regioni. La colonna Stato mostra le regioni abilitate per il tuo Account AWS.

In questa pagina, puoi selezionare una regione per:

- Visualizzare i dettagli della regione, come il codice regionale, la geografia e il numero di ogni tipo di zona.

  Puoi anche visualizzare l'elenco di zone di disponibilità, zone locali e zone Wavelength e l'elenco delle tue risorse nella regione.
- Abilita o disabilita la regione.

Da ogni scheda della zona, puoi visualizzare l'elenco di quel tipo di zona. Dalla scheda Zone locali, puoi attivare una zona locale.

> **Tip**
>
> Se utilizzi solo regioni o tipi di risorse specifici, puoi personalizzare AWS Global View per visualizzare solo tali regioni e tipi di risorse. Per personalizzare le regioni e i tipi di risorse visualizzati, nel pannello di navigazione, scegli Impostazioni, quindi nelle schede Risorse e regioni, seleziona le regioni e i tipi di risorse che non desideri vengano visualizzati nella visualizzazione AWS globale.

Tagging delle risorse Amazon EC2.

Per semplificare la gestione di istanze, immagini e altre risorse Amazon EC2 puoi decidere di assegnare metadati personalizzati a ogni risorsa sotto forma di tag. I tag consentono di classificare AWS le risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Questa caratteristicaè molto utile quando hai tante risorse dello stesso tipo in quanto puoi rapidamente individuare una risorsa specifica in base ai tag assegnati. Questo argomento descrive i tag e mostra come crearli.

> **Warning**
>
> Le chiavi di tag e i relativi valori vengono restituiti da numerose chiamate API diverse. Negando l'accesso a `DescribeTags` non viene automaticamente negato l'accesso ai tag restituiti da altre API. Come best practice, consigliamo di non includere dati sensibili nei tag.

Indice

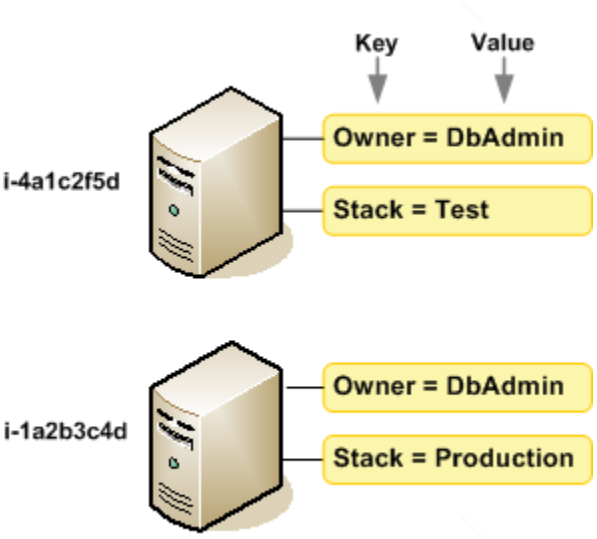
- Nozioni di base sui tag
- Assegnazione di tag alle risorse
- Limitazioni applicate ai tag
- Tag e gestione degli accessi
- Tagging delle risorse per la fatturazione
- Concessione dell'autorizzazione all'applicazione di tag Amazon EC2 per le risorse durante la creazione
- Aggiungi e rimuovi i tag per le risorse Amazon EC2
- Filtra le risorse Amazon EC2 per tag
- Visualizza i tag per le istanze EC2 utilizzando i metadati dell'istanza

Nozioni di base sui tag

Un tag è un'etichetta che assegni a una AWS risorsa. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili.

I tag consentono di classificare AWS le risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Ad esempio, puoi definire un set di tag per le istanze Amazon EC2 del tuo account e monitorare così ogni proprietario dell'istanza e il livello dello stack.

Lo schema seguente illustra il funzionamento del tagging. In questo esempio hai assegnato due tag a ciascuna istanza, un tag con la chiave `Owner` e un altro tag con la chiave `Stack`. A ogni tag è inoltre associato un valore.



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 AWS di etichettatura.

I tag non hanno alcun significato semantico per Amazon EC2 e vengono interpretati rigorosamente come una stringa di caratteri. Inoltre, i tag non vengono assegnati automaticamente alle risorse. Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Puoi impostare il valore di un tag su una stringa vuota, ma non su null. Se aggiungi un tag con la stessa chiave di un tag esistente a una risorsa specifica, il nuovo valore sovrascrive quello precedente. Se elimini una risorsa, verranno eliminati anche tutti i tag a essa associati.

> **Note**
>
> Dopo aver eliminato una risorsa, i relativi tag potrebbero rimanere visibili nell'output della console, dell'API e della CLI per un breve periodo. Questi tag saranno gradualmente dissociati dalla risorsa e verranno eliminati definitivamente.

Assegnazione di tag alle risorse

Quando utilizzi la console Amazon EC2, puoi applicare tag alle risorse utilizzando la scheda Tag nella schermata delle risorse pertinente oppure puoi utilizzare il Tags Editor nella console. AWS Resource Groups Alcune schermate relative alle risorse ti permettono di specificare i tag per una risorsa quando crei la risorsa, ad esempio un tag con la chiave `Name` e un valore specificato. Nella maggior parte dei casi, la console applica i tag subito dopo la creazione della risorsa, anziché durante il processo di creazione. La console può organizzare le risorse in base al relativo tag `Name` ma questo tag non ha un significato semantico per il servizio Amazon EC2.

Se utilizzi l'API Amazon EC2, o un AWS SDK AWS CLI, puoi utilizzare l'azione API `CreateTags` EC2 per applicare i tag alle risorse esistenti. Inoltre, alcune operazioni per la creazione di risorse ti consentono di specificare tag per una risorsa durante la sua creazione. Se i tag non possono essere applicati durante la creazione della risorsa, eseguiamo il rollback del processo di creazione della risorsa. Ciò fa sì che le risorse vengano create con i tag oppure che non vengano create affatto, nonché che nessuna risorsa sia mai sprovvista di tag. Il tagging delle risorse in fase di creazione ti permette di evitare di eseguire script di tagging personalizzati dopo la creazione delle risorse. Per ulteriori informazioni sull'abilitazione agli utenti affinché possano aggiungere tag alle risorse durante

la creazione, vedere Concessione dell'autorizzazione all'applicazione di tag Amazon EC2 per le risorse durante la creazione.

Puoi applicare autorizzazioni basate su tag a livello di risorsa nelle policy IAM alle operazioni dell'API Amazon EC2 che supportano il tagging in fase di creazione per implementare un controllo granulare sugli utenti e sui gruppi che associano tag alle risorse in fase di creazione. Le risorse vengono adeguatamente protette a partire dal momento della creazione, ovvero i tag vengono applicati subito alle risorse. Pertanto qualsiasi autorizzazione basata su tag a livello di risorsa che controlla l'uso delle risorse risulta immediatamente valida. Le risorse possono essere monitorate e segnalate con maggiore precisione. Puoi applicare l'uso del tagging alle nuove risorse e controllare quali chiavi e valori di tag sono impostati per le risorse.

Puoi inoltre applicare autorizzazioni a livello di risorsa alle operazioni `CreateTags` e `DeleteTags` dell'API Amazon EC2 nelle policy IAM per controllare quali chiavi e valori di tag sono impostati sulle risorse esistenti. Per ulteriori informazioni, consulta Esempio: aggiunta di tag alle risorse.

Per ulteriori informazioni sul tagging delle risorse per la fatturazione, consulta Utilizzo di tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing .

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 univoca 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
- Caratteri consentiti
  - Sebbene EC2 consenta l'uso di qualsiasi carattere nei suoi tag, altri AWS servizi sono più restrittivi. I caratteri consentiti in tutti i AWS servizi sono: lettere (`a-z`,`A-Z`), numeri (`0-9`) e spazi rappresentabili in UTF-8, e i seguenti caratteri:. `+ - = . _ : / @`
  - Se abiliti i tag delle istanze nei metadati delle istanze, per il tag dell'istanza keys puoi usare solo lettere (`a-z`, `A-Z`), numeri (`0-9`) e i seguenti caratteri: `+ - = . , _ : @`. Il tag dell'istanza keys non può contenere spazi o `/` e non può contenere solo `.` (un punto), `..` (due punti) o `_index`. Per ulteriori informazioni, consulta Visualizza i tag per le istanze EC2 utilizzando i metadati dell'istanza.

- 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 interrompere, arrestare o eliminare una risorsa solo sulla base dei relativi tag. Devi specificare il relativo identificatore. Ad esempio, per eliminare gli snapshot associato a una chiave di tag denominata `DeleteMe`, devi utilizzare l'operazione `DeleteSnapshots` con gli identificatori di risorsa degli snapshot, ad esempio `snap-1234567890abcdef0`.

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 tali tag. Per il controllo degli accessi alle risorse condivise basato su tag, ogni AWS account deve assegnare il proprio set di tag per controllare l'accesso alla risorsa.

Tag e gestione degli accessi

Se utilizzi AWS Identity and Access Management (IAM), puoi controllare quali utenti del tuo AWS account sono autorizzati a creare, modificare o eliminare i tag. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag Amazon EC2 per le risorse durante la creazione.

Puoi inoltre utilizzare i tag delle risorse per implementare il controllo basato sugli attributi (ABAC). Puoi creare le policy IAM che consentono operazioni basate sui tag per la risorsa. Per ulteriori informazioni, consulta Controllare l'accesso mediante l'accesso basato sugli attributi.

Tagging delle risorse per la fatturazione

Puoi utilizzare i tag per organizzare la AWS fattura in modo da riflettere la tua struttura dei costi. Per fare ciò, registrati per ricevere la fattura del tuo AWS account con i valori chiave dei tag inclusi. Per ulteriori informazioni sulla configurazione di un report di allocazione dei costi mediante i tag, consulta Report di allocazione dei costi mensili nella Guida per l'utente di AWS Billing . Per visualizzare il costo delle risorse combinate, puoi organizzare le informazioni di fatturazione in base alle risorse con gli stessi valori di chiave di tag. Puoi ad esempio applicare tag a numerose risorse con un nome di applicazione specifico, quindi organizzare le informazioni di fatturazione per visualizzare il costo totale dell'applicazione in più servizi. Per ulteriori informazioni, consulta Utilizzo dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing .

> **Note**
>
> Se hai appena abilitato la reportistica, i dati relativi al mese corrente saranno disponibili per la visualizzazione dopo 24 ore.

I tag di allocazione dei costi possono indicare quali risorse contribuiscono ai costi, ma eliminare o disattivare le risorse non sempre riduce i costi. Ad esempio, i dati di snapshot a cui fa riferimento un altro snapshot vengono conservati anche se viene eliminato lo snapshot contenente i dati originali. Per ulteriori informazioni, consulta Volumi e snapshot di Amazon Elastic Block Store nella Guida per l'utente di AWS Billing .

> **Note**
>
> Gli indirizzi IP elastici con tag non appaiono nel report di allocazione dei costi.

Concessione dell'autorizzazione all'applicazione di tag Amazon EC2 per le risorse durante la creazione

Alcune operazioni API Amazon EC2 per la creazione di risorse ti consentono di specificare tag quando crei le risorse. È possibile utilizzare i tag delle risorse per implementare il controllo basato sugli attributi (ABAC). Per ulteriori informazioni, consulta Assegnazione di tag alle risorse e Controllare l'accesso mediante l'accesso basato sugli attributi.

Per consentire agli utenti di applicare tag alle risorse durante la creazione, essi devono disporre delle autorizzazioni per utilizzare l'operazione che crea la risorsa, come `ec2:RunInstances` o `ec2:CreateVolume`. Se i tag vengono specificati nell'azione di creazione delle risorse, Amazon esegue autorizzazioni aggiuntive per l'azione `ec2:CreateTags` per verificare se gli utenti dispongono delle autorizzazioni per creare tag. Pertanto, gli utenti devono disporre anche di autorizzazioni esplicite a utilizzare l'azione `ec2:CreateTags`.

Nella definizione della policy IAM per l'operazione `ec2:CreateTags`, utilizzare l'elemento `Condition` con la chiave di condizione `ec2:CreateAction` per assegnare autorizzazioni di tagging all'operazione che crea la risorsa.

Ad esempio, la seguente policy consente gli utenti di avviare istanze e applicare tag a istanze e volumi durante l'avvio. Gli utenti non sono autorizzati ad applicare tag alle risorse esistenti (non possono chiamare l'operazione `ec2:CreateTags` direttamente).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

In modo analogo, la seguente policy consente gli utenti di creare volumi e applicare tag a tali volumi durante la creazione dei volumi stessi. Gli utenti non sono autorizzati ad applicare tag alle risorse esistenti (non possono chiamare l'operazione `ec2:CreateTags` direttamente).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "*"
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "CreateVolume"
          }
       }
    }
  ]
}
```

L'operazione `ec2:CreateTags` viene valutata solo se i tag vengono applicati durante l'operazione di creazione di risorse. Pertanto, un utente con le autorizzazioni per la creazione di una risorsa (presupponendo che non siano presenti condizioni di assegnazione di tag) non necessità delle autorizzazioni per utilizzare l'operazione `ec2:CreateTags` se nella richiesta non viene specificato alcun tag. Tuttavia, se l'utente tenta di creare una risorsa con tag, la richiesta ha esito negativo se non dispone delle autorizzazioni per utilizzare l'operazione `ec2:CreateTags`.

L'operazione `ec2:CreateTags` viene valutata anche se i tag sono forniti in un modello di avvio. Per un esempio di policy, consulta Tag in un modello di avvio.

Controllo dell'accesso a tag specifici

È possibile utilizzare condizioni aggiuntive nell'elemento `Condition` delle policy IAM per controllare le chiavi dei tag e i valori che possono essere applicati alle risorse.

Le seguenti chiavi di condizione possono essere utilizzate con gli esempi nella sezione precedente:

- `aws:RequestTag`: indica che una chiave di tag o una chiave e un valore di tag sono presenti in una richiesta. Anche gli altri tag devono essere specificati nella richiesta.
  - Da utilizzare assieme all'operatore di condizione `StringEquals` per applicare una combinazione specifica di chiave e valore di tag, ad esempio per applicare il tag `cost-center=cc123`:

    ```
    "StringEquals": { "aws:RequestTag/cost-center": "cc123" }
    ```

  - Da utilizzare assieme all'operatore di condizione `StringLike` per applicare una chiave di tag specifica nella richiesta, ad esempio per applicare la chiave di tag `purpose`:

```
"StringLike": { "aws:RequestTag/purpose": "*" }
```

- `aws:TagKeys`: applica le chiavi di tag utilizzate nella richiesta.
  - Da utilizzare assieme al modificatore `ForAllValues` per applicare chiavi di tag specifiche se vengono fornite nella richiesta (se i tag vengono specificati nella richiesta, solo le chiavi di tag specifiche sono consentite; non sono consentiti altri tag). Ad esempio, la chiave di tag `environment` o `cost-center` è consentita:

    ```
    "ForAllValues:StringEquals": { "aws:TagKeys": ["environment","cost-center"] }
    ```

  - Da utilizzare assieme al modificatore `ForAnyValue` per implementare la presenza di almeno una delle chiavi di tag specificate nella richiesta. Ad esempio, nella richiesta deve essere presente almeno una delle chiavi di tag `environment` o `webserver`:

    ```
    "ForAnyValue:StringEquals": { "aws:TagKeys": ["environment","webserver"] }
    ```

Queste chiavi di condizione possono essere applicate alle operazioni di creazione delle risorse che supportano il tagging, nonché alle operazioni `ec2:CreateTags` ed `ec2:DeleteTags`. Per sapere se un'operazione API Amazon EC2 supporta l'aggiunta di tag, consulta Operazioni, risorse e chiavi di condizione per Amazon EC2.

Per obbligare gli utenti a specificare i tag quando creano una risorsa, devi utilizzare la chiave di condizione `aws:RequestTag` o `aws:TagKeys` con il modificatore `ForAnyValue` nell'operazione di creazione delle risorse. L'operazione `ec2:CreateTags` non viene valutata se un utente non specifica i tag per l'operazione di creazione delle risorse.

Per le condizioni, la chiave di condizione non fa distinzione tra maiuscole e minuscole, mentre il valore della condizione fa distinzione tra maiuscole e minuscole. Pertanto, per applicare la distinzione tra maiuscole e minuscole per una chiave di tag, utilizza la chiave di condizione `aws:TagKeys`, specificando la chiave di tag come valore nella condizione.

Per esempi di policy IAM, consulta Policy di esempio da utilizzare all'API Amazon EC2. Per ulteriori informazioni, consulta Conditions with multiple context keys or values nella Guida per l'utente IAM.

Aggiungi e rimuovi i tag per le risorse Amazon EC2

Quando crei una risorsa Amazon EC2, ad esempio un'istanza Amazon EC2, puoi specificare i tag da aggiungere alla risorsa. Puoi anche utilizzare la console di Amazon EC2 per visualizzare i tag per una

risorsa Amazon EC2 specifica. Puoi anche aggiungere o rimuovere tag da una risorsa Amazon EC2 esistente.

Puoi utilizzare il Tag Editor nella AWS Resource Groups console per visualizzare, aggiungere o rimuovere tag in tutte le tue AWS risorse in tutte le regioni. Puoi applicare o rimuovere i tag da più tipi di risorse contemporaneamente. Per ulteriori informazioni, consulta la Guida per l'utente di Tagging AWS Resources.

Processi

- Aggiungere tag utilizzando la console
- Aggiungi tag usando il AWS CLI
- Aggiungi tag usando PowerShell
- Aggiungi tag usando CloudFormation

Aggiungere tag utilizzando la console

Puoi aggiungere tag a una risorsa esistente direttamente dalla pagina della risorsa stessa.

Come aggiungere tag a una risorsa esistente

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, seleziona la Regione in cui si trova la risorsa.
3. Nel riquadro di navigazione selezionare un tipo di risorsa, ad esempio Instances (Istanze).
4. Seleziona la risorsa dall'elenco.
5. Nella scheda Tag scegliere Gestisci tag.
6. Scegli Aggiungi nuovo tag, quindi specifica una chiave e un valore per il tag.
7. Scegli Save (Salva).

Aggiungi tag usando il AWS CLI

Puoi aggiungere tag durante la creazione di una risorsa o a una risorsa esistente.

Per aggiungere tag alla creazione di risorse

Utilizza l'opzione `-tag-specifications` per etichettare una risorsa al momento della creazione. Una specifica di tag richiede il tipo di risorsa da taggare, la chiave del tag e il valore del tag. Il seguente esempio crea un tag e lo aggiunge a una specifica di tag.

```
--tag-specifications 'ResourceType=instance,Tags=[{Key=stack,Value=production}]'
```

Per aggiungere un tag a una risorsa esistente

Gli esempi seguenti mostrano come aggiungere tag alle risorse esistenti utilizzando il comando create-tags.

Example Esempio: aggiunta di un tag a una risorsa

Questo esempio aggiunge il tag **Stack=production** all'immagine specificata o sovrascrive un tag esistente per l'AMI in cui la chiave tag è stack. Se il comando va a buon fine, non viene restituito alcun output.

```
aws ec2 create-tags \
    --resources ami-0abcdef1234567890 \
    --tags Key=stack,Value=production
```

Example Esempio: aggiunta di tag a più risorse.

Questo esempio aggiunge (o sovrascrive) due tag per un'AMI e un'istanza. Uno dei tag contiene solo una chiave (webserver), senza alcun valore (il valore viene impostato su una stringa vuota). L'altro tag comprende una chiave (stack) e un valore (**Production**). Se il comando va a buon fine, non viene restituito alcun output.

```
aws ec2 create-tags \
    --resources ami-0abcdef1234567890 i-1234567890abcdef0 \
    --tags Key=webserver,Value=  Key=stack,Value=Production
```

Example Esempio: aggiunta di tag con caratteri speciali

Questo esempio aggiunge il tag [Group]=test a un'istanza. Le parentesi quadre ([e]) sono caratteri speciali, per i quali occorre eseguire l'escape.

Se si utilizza Linux o OS X, per eseguire l'escape dei caratteri speciali, racchiudere l'elemento con il carattere speciale tra virgolette doppie (''), quindi racchiudere l'intera struttura chiave e valore tra virgolette singole (').

```
aws ec2 create-tags \
```

```
    --resources i-1234567890abcdef0 \
    --tags 'Key="[Group]",Value=test'
```

Se si utilizza Windows, per eseguire l'escape dei caratteri speciali, racchiudere l'elemento con caratteri speciali tra virgolette doppie ("), quindi anteporre ad ogni carattere virgolette doppie una barra rovesciata (****) come segue:

```
aws ec2 create-tags ^
    --resources i-1234567890abcdef0 ^
    --tags Key=\"[Group]\",Value=test
```

Se utilizzi Windows PowerShell, per evitare i caratteri speciali, racchiudi il valore che contiene caratteri speciali tra virgolette doppie (**"**), fai precedere ogni carattere tra virgolette doppie con una barra rovesciata (****) e quindi racchiudi l'intera struttura di chiavi e valori tra virgolette singole () come segue: **'**

```
aws ec2 create-tags `
    --resources i-1234567890abcdef0 `
    --tags 'Key=\"[Group]\",Value=test'
```

Aggiungi tag usando PowerShell

Puoi aggiungere tag durante la creazione di una risorsa o a una risorsa esistente.

Per aggiungere tag alla creazione di risorse

Utilizza il parametro `-TagSpecification` per etichettare una risorsa al momento della creazione. Una specifica di tag richiede il tipo di risorsa da taggare, la chiave del tag e il valore del tag. Il seguente esempio crea un tag e lo aggiunge a una specifica di tag.

```
$tag = @{Key="stack"; Value="production"}
$tagspec = new-object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "instance"
$tagspec.Tags.Add($tag)
```

L'esempio seguente specifica questo tag nel parametro `-TagSpecification`.

```
-TagSpecification $tagspec
```

Per aggiungere un tag a una risorsa esistente

Utilizza il cmdlet New-EC2Tag. Devi specificare la risorsa, la chiave del tag e il valore del tag.

```
New-EC2Tag `
    -Resource i-1234567890abcdef0 `
    -Tag @{Key="purpose"; Value="production"}
```

Aggiungi tag usando CloudFormation

Con i tipi di risorse Amazon EC2, è possibile specificare i tag utilizzando una proprietà `Tags` o `TagSpecifications`.

Gli esempi seguenti aggiungono il tag **`Stack=Production`** a AWS::EC2::Instance utilizzando la relativa proprietà `Tags`.

Example Esempio: Tag in YAML

```
Tags:
  - Key: "Stack"
    Value: "Production"
```

Example Esempio: Tag in JSON

```
"Tags": [
    {
        "Key": "Stack",
        "Value": "Production"
    }
]
```

Gli esempi seguenti aggiungono il tag **`Stack=Production`** ad AWS: :EC2:: LaunchTemplate LaunchTemplateData utilizzando la relativa `TagSpecifications` proprietà.

Example Esempio: TagSpecifications in YAML

```
TagSpecifications:
  - ResourceType: "instance"
    Tags:
    - Key: "Stack"
```

```
      Value: "Production"
```

Example Esempio: TagSpecifications in JSON

```
"TagSpecifications": [
    {
        "ResourceType": "instance",
        "Tags": [
            {
                "Key": "Stack",
                "Value": "Production"
            }
        ]
    }
]
```

Filtra le risorse Amazon EC2 per tag

Dopo aver aggiunto i tag, puoi filtrare le risorse Amazon EC2 in base alle chiavi e ai valori.

Console

Per filtrare le risorse per tag

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare un tipo di risorsa, ad esempio Instances (Istanze).
3. Selezionare il campo di ricerca.
4. Nell'elenco, in Tag, scegli la chiave del tag.
5. Scegliere il valore del tag corrispondente dall'elenco.
6. Al termine, rimuovere il filtro.

Per ulteriori informazioni sull'uso dei filtri nella console di Amazon EC2, consulta Trova le risorse Amazon EC2.

AWS CLI

Per descrivere risorse di un unico tipo con la chiave del tag specificata

Aggiungi il filtro seguente a un comando `describe` per descrivere le risorse di quel tipo con un tag Stack, indipendentemente dal valore del tag.

```
--filters Name=tag-key,Values=Stack
```

Per descrivere risorse di un unico tipo con il tag specificato

Aggiungi il seguente filtro a un comando `describe` per descrivere le risorse di quel tipo con il tag Stack=production.

```
--filters Name=tag:Stack,Values=production
```

Per descrivere risorse di un unico tipo con il valore del tag specificato

Aggiungi il filtro seguente a un comando `describe` per descrivere le risorse di quel tipo con un tag con il valore production, indipendentemente dalla chiave del tag.

```
--filters Name=tag-value,Values=production
```

Per descrivere tutte le risorse EC2 con il tag specificato

Aggiungi il seguente filtro al comando describe-tags per descrivere tutte le risorse EC2 con il tag Stack=test.

```
--filters Name=key,Values=Stack Name=value,Values=test
```

PowerShell

Per filtrare le risorse di un singolo tipo in base alla chiave del tag

Aggiungi il filtro seguente a un cmdlet `Get` per descrivere le risorse di quel tipo con un tag Stack, indipendentemente dal valore del tag.

```
-Filter @{Name="tag-key"; Values="Stack"}
```

Per filtrare le risorse di un singolo tipo in base al tag

Aggiungi il seguente filtro a un cmdlet `Get` per descrivere le risorse di quel tipo con il tag Stack=production.

```
-Filter @{Name="tag:Stack"; Values="production"}
```

Per filtrare le risorse di un singolo tipo in base al valore del tag

Aggiungi il filtro seguente a un cmdlet `Get` per descrivere le risorse di quel tipo con un tag con il valore production, indipendentemente dal valore della chiave del tag.

```
-Filter @{Name="tag-value"; Values="production"}
```

Per filtrare tutte le risorse EC2 per tag

Aggiungi il seguente filtro al Get-EC2Tag cmdlet per descrivere tutte le risorse EC2 con il tag. Stack=test

```
-Filter @{Name="tag:Stack"; Values="test"}
```

Visualizza i tag per le istanze EC2 utilizzando i metadati dell'istanza

È possibile accedere ai tag di un'istanza dai metadati dell'istanza. Accedendo ai tag dai metadati dell'istanza non è più necessario utilizzare Chiamate API `DescribeInstances` o `DescribeTags` per recuperare le informazioni sui tag, ciò riduce le transazioni API al secondo e consente al recupero dei tag di scalare il numero di istanze che si controllano. Inoltre, i processi locali in esecuzione su un'istanza possono visualizzare le informazioni sui tag dell'istanza direttamente dai metadati dell'istanza.

Per impostazione predefinita, i tag non sono disponibili dai metadati dell'istanza; è necessario consentire esplicitamente l'accesso. È possibile consentire l'accesso all'avvio dell'istanza o dopo l'avvio su un'istanza in esecuzione o interrotta. È inoltre possibile consentire l'accesso ai tag specificandolo in un modello di avvio. Le istanze avviate utilizzando il modello consentono l'accesso ai tag nei metadati dell'istanza.

Se aggiungi o rimuovi un tag di istanza, i metadati dell'istanza vengono aggiornati mentre l'istanza è in esecuzione, senza doverla arrestare e poi avviare.

Processi

- Abilita l'accesso ai tag nei metadati dell'istanza
- Recupero dei tag dai metadati dell'istanza
- Disabilita l'accesso ai tag nei metadati dell'istanza

Abilita l'accesso ai tag nei metadati dell'istanza

Per impostazione predefinita, non è possibile accedere ai tag dell'istanza nei metadati dell'istanza. Per ogni istanza, è necessario abilitare esplicitamente l'accesso.

> **Note**
>
> Se si consente l'accesso ai tag nei metadati delle istanze, le chiavi dei tag di istanza sono soggette a restrizioni specifiche. Non-compliance comporterà un avvio non riuscito per le nuove istanze o un errore per le istanze esistenti. Le restrizioni sono le seguenti:
>
> - Può includere solo lettere (`a-z`,`A-Z`), numeri (`0-9`) e i seguenti caratteri: `+ - = . , _ : @`.
> - Non può contenere spazi o `/`.
> - Non può essere composto solo da `.` (un periodo), `..` (due periodi) o`_index`.
>
> Per ulteriori informazioni, consulta Limitazioni applicate ai tag.

Console

Per consentire l'accesso ai tag nei metadati dell'istanza all'avvio

1. Segui la procedura per avviare un'istanza.
2. Espandi i dettagli avanzati e consenti i tag nei metadati, scegliendo Abilita.
3. Nel pannello Summary (Riepilogo), verifica la configurazione dell'istanza, quindi scegli Launch instance (Avvia istanza). Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.

Per consentire l'accesso ai tag nei metadati dell'istanza dopo l'avvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona la tua istanza e scegli Operazioni,Impostazioni istanza,Consenti tag nei metadati dell'istanza.
4. Per consentire l'accesso ai tag nei metadati dell'istanza, selezionare la casella di controllo Abilita.

5. Scegli Save (Salva).

AWS CLI

Per consentire l'accesso ai tag nei metadati dell'istanza all'avvio

Utilizza il comando run-instances e aggiungi la seguente opzione `--metadata-options`.

```
--metadata-options "InstanceMetadataTags=enabled"
```

Per consentire l'accesso ai tag nei metadati dell'istanza dopo l'avvio

Utilizza il comando modify-instance-metadata-options seguente.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --instance-metadata-tags enabled
```

Per verificare che l'accesso ai tag nei metadati dell'istanza sia abilitato

Utilizza il comando describe-instances e controlla il valore di `InstanceMetadataTags`.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[].MetadataOptions[].InstanceMetadataTags"
```

Di seguito è riportato un output di esempio. Il valore è `enabled` o `disabled`.

```
[
    "enabled"
]
```

PowerShell

Per consentire l'accesso ai tag nei metadati dell'istanza all'avvio

Utilizzare il New-EC2Instance cmdlet e aggiungere il seguente parametro. `-MetadataOptions_InstanceMetadataTags`

```
-MetadataOptions_InstanceMetadataTags enabled
```

Per consentire l'accesso ai tag nei metadati dell'istanza dopo l'avvio

Utilizza il cmdlet Edit-EC2InstanceMetadataOption.

```
Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -InstanceMetadataTags enabled
```

Per verificare che l'accesso ai tag nei metadati dell'istanza sia abilitato

Utilizzare il Get-EC2Instance cmdlet e verificare il valore di. `InstanceMetadataTags`

```
(Get-EC2Instance `
    -
InstanceId i-1234567890abcdef0).Instances.MetadataOptions.InstanceMetadataTags.Value
```

Di seguito è riportato un output di esempio. Il valore è `enabled` o `disabled`.

```
enabled
```

Recupero dei tag dai metadati dell'istanza

Dopo aver consentito l'accesso ai tag dell'istanza sono nei metadati, puoi accedere alla categoria `tags/instance` dai metadati dell'istanza. Per ulteriori informazioni, consulta Accesso ai metadati dell'istanza per un'istanza EC2.

IMDSv2

Linux

Esegui il seguente comando dall'istanza Linux per elencare tutte le chiavi dei tag per l'istanza.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/tags/instance
```

In questo esempio si ottiene il valore di una chiave recuperata nell'esempio precedente. La richiesta IMDSv2 utilizza il token memorizzato che è stato creato nel comando dell'esempio precedente, ipotizzando che non sia scaduto. Il token non deve essere scaduto.

```
curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
tags/instance/tag-key
```

Windows

Esegui il seguente cmdlet dall'istanza Windows per elencare tutte le chiavi dei tag per l'istanza.

```
$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/tags/instance
```

In questo esempio si ottiene il valore di una chiave recuperata nell'esempio precedente. La richiesta IMDSv2 utilizza il token memorizzato che è stato creato nel comando dell'esempio precedente, ipotizzando che non sia scaduto. Il token non deve essere scaduto.

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

IMDSv1

Linux

Esegui il seguente comando dall'istanza Linux per elencare tutte le chiavi dei tag per l'istanza.

```
curl http://169.254.169.254/latest/meta-data/tags/instance
```

In questo esempio si ottiene il valore di una chiave recuperata nell'esempio precedente.

```
curl http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

Windows

Esegui il seguente cmdlet dall'istanza Windows per elencare tutte le chiavi dei tag per l'istanza.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/tags/instance
```

In questo esempio si ottiene il valore di una chiave recuperata nell'esempio precedente.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

Disabilita l'accesso ai tag nei metadati dell'istanza

Puoi disabilitare l'accesso ai tag dell'istanza nei metadati dell'istanza. Non è necessario disabilitare l'accesso ai tag di istanza sui metadati delle istanze all'avvio perché è disattivato per impostazione predefinita.

Console

Per disabilitare l'accesso ai tag nei metadati dell'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare un'istanza e scegliere Actions (Operazioni),Instance settings (Impostazioni istanza),Allow tags in instance metadata (Consenti tag nei metadati dell'istanza).
4. Per disattivare l'accesso ai tag nei metadati dell'istanza, deselezionare la casella di controllo Abilita.
5. Scegli Save (Salva).

AWS CLI

Per disabilitare l'accesso ai tag nei metadati dell'istanza

Utilizza il comando modify-instance-metadata-options seguente.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --instance-metadata-tags disabled
```

PowerShell

Per disabilitare l'accesso ai tag nei metadati dell'istanza

Utilizza il cmdlet Edit-EC2InstanceMetadataOption.

```
Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -InstanceMetadataTag disabled
```

Service Quotas di Amazon EC2

Quando crei le tue Account AWS, impostiamo quote predefinite (note anche come limiti) per AWS le tue risorse in base alla regione. Se tenti di superare la quota per una risorsa, la richiesta ha esito negativo. Ad esempio, esiste un numero massimo di vCPU Amazon EC2 che puoi fornire per le istanze in una regione. On-Demand Se tenti di avviare un'istanza in una regione e questa richiesta fa sì che l'utilizzo superi questa quota, la richiesta ha esito negativo. In questo caso, puoi ridurre l'utilizzo delle risorse o richiedere un aumento delle quote.

La console Service Quotas è una posizione centrale in cui è possibile visualizzare e gestire le quote per AWS i servizi e richiedere un aumento della quota per molte delle risorse utilizzate. Utilizza le informazioni sulle quote che forniamo per gestire la tua AWS infrastruttura. Pianifica le richieste di incremento delle quote con un certo anticipo rispetto a quando ne avrai effettivamente bisogno.

Documentazione delle quote correlate

- Endpoint e quote Amazon EC2
- Quote dei tipi di istanza Amazon EC2
- Quote per Amazon EBS
- Quote Amazon VPC

Visualizzazione delle quote correnti

È possibile visualizzare le quote per ciascuna regione utilizzando la console Service Quotas.

Visualizzazione delle quote correnti utilizzando la console Service Quotas

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Nella barra di navigazione, nella parte superiore della schermata, seleziona una regione.
3. Nel pannello Gestisci quote, seleziona un servizio, ad esempio Amazon Elastic Compute Cloud (Amazon EC2). Scegli Visualizza quote.

4. Utilizza il campo di filtro per filtrare l'elenco in base al nome della risorsa. Ad esempio, inserisci per individuare **`On-Demand`** le quote per le istanze. On-Demand
5. Per visualizzare ulteriori informazioni, scegli il nome della quota per aprire la pagina dei dettagli della quota.

Richiesta di un aumento

È possibile richiedere un aumento della quota per ciascuna regione.

Per richiedere un aumento utilizzando la console Service Quotas

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Nella barra di navigazione, nella parte superiore della schermata, seleziona una regione.
3. Utilizza il campo di filtro per filtrare l'elenco in base al nome della risorsa. Ad esempio, immettete **`On-Demand`** per individuare le quote per On-Demand le istanze.
4. Se la quota è modificabile, seleziona la quota e quindi scegli Richiedi aumento della quota.
5. In Modifica valore quota, inserisci il nuovo valore della quota.
6. Scegli Richiedi.
7. Per visualizzare eventuali richieste in sospeso o risolte di recente nella console, scegli Pannello di controllo dal riquadro di navigazione. Per le richieste in sospeso, scegliere lo stato della richiesta per aprire la ricevuta della richiesta. Lo stato iniziale di una richiesta è Pending (In attesa). Dopo la modifica dello stato in Quota richiesta, vedrai il numero del caso con. Supporto Scegli il numero del caso per aprire il ticket della tua richiesta.

Per ulteriori informazioni, incluso come utilizzare AWS CLI o gli SDK per richiedere un aumento della quota, consulta Richiedere un aumento della quota nella Service Quotas User Guide.

Restrizione sull'e-mail inviata tramite la porta 25

Per impostazione predefinita, Amazon EC2 permette il traffico in uscita sulla porta 25 solo verso indirizzi IPv4 privati. Il traffico sulla porta 25 è bloccato verso gli indirizzi IPv4 pubblici e gli indirizzi IPv6.

È possibile richiedere la rimozione di questa restrizione. Per ulteriori informazioni, vedi Come rimuovo la restrizione sulla porta 25 dall'istanza Amazon EC2 o dalla funzione Lambda?

Questa restrizione non si applica al traffico in uscita sulla porta 25 destinato a:

- Indirizzi IP nel blocco CIDR primario del VPC in cui esiste l'interfaccia di rete di origine.
- Indirizzi IP nei CIDR definiti in RFC 1918, RFC 6598, e RFC 4193.

Monitoraggio delle risorse Amazon EC2

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle tue istanze Amazon EC2 e delle tue soluzioni. AWS È necessario raccogliere dati di monitoraggio da tutte le parti delle AWS soluzioni in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica.

AWS fornisce vari strumenti che puoi usare per monitorare Amazon EC2. Le dashboard di Amazon EC2 e CloudWatch della console forniscono una panoramica dello stato del tuo ambiente Amazon EC2. Inoltre, forniamo quanto segue:

- Controlli dello stato del sistema: monitora i AWS sistemi necessari per utilizzare la tua istanza per assicurarti che funzionino correttamente. Questi controlli rilevano i problemi dell'istanza che richiedono l' AWS intervento per la riparazione. Quando una verifica di stato del sistema ha esito negativo, puoi scegliere se attendere la risoluzione del problema da parte di AWS oppure puoi risolverlo direttamente (ad esempio, arrestando e riavviando o terminando e sostituendo un'istanza). Esempi di problemi che causano il mancato superamento dei controlli dello stato del sistema:
  - Perdita di connettività di rete
  - Perdita di alimentazione elettrica del sistema
  - Problemi di software sull'host fisico
  - Problemi hardware sull'host fisico che incidono sulla raggiungibilità della rete

  Per ulteriori informazioni, consulta Verifiche dello stato delle istanze Amazon EC2.
- Verifiche dello stato delle istanze: monitorano la configurazione del software e della rete della singola istanza. Tali verifiche rilevano i problemi per la cui risoluzione è richiesto il tuo intervento. Se l'esito della verifica dello stato di un'istanza è negativo, solitamente è necessario risolvere direttamente il problema (ad esempio, riavviando l'istanza o apportando modifiche al sistema operativo). Esempi di problemi che potrebbero causare il mancato superamento delle verifiche dello stato dell'istanza:
  - Verifiche dello stato del sistema non riuscite
  - Configurazione non corretta di rete o startup
  - Memoria esaurita
  - File system danneggiato
  - Kernel non compatibile

Per ulteriori informazioni, consulta Verifiche dello stato delle istanze Amazon EC2.

- CloudWatch Allarmi Amazon: monitora una singola metrica in un periodo di tempo specificato ed esegui una o più azioni in base al valore della metrica rispetto a una determinata soglia per diversi 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. Gli allarmi richiamano azioni solo per cambiamenti di stato prolungati. CloudWatch gli allarmi non richiamano azioni semplicemente perché si trovano in uno stato particolare; lo stato deve essere cambiato e mantenuto per un determinato numero di periodi. Per ulteriori informazioni, consulta Monitora le tue istanze utilizzando CloudWatch.
- EventBridge Eventi Amazon: automatizza i tuoi AWS servizi e rispondi automaticamente agli eventi di sistema. Gli eventi dei AWS servizi vengono trasmessi quasi EventBridge in tempo reale e puoi specificare azioni automatiche da intraprendere quando un evento corrisponde a una regola che scrivi. Per ulteriori informazioni, consulta the section called "Automatizza utilizzando EventBridge".
- AWS CloudTrail logs: acquisisce informazioni dettagliate sulle chiamate effettuate all'API Amazon EC2 e le archivia come file di registro in Amazon S3. Puoi utilizzare CloudTrail i log per determinare quali chiamate sono state effettuate, l'indirizzo IP di origine della chiamata, chi ha effettuato la chiamata e quando è stata effettuata la chiamata. Per ulteriori informazioni, consulta the section called "Registra le chiamate API utilizzando CloudTrail".
- CloudWatch agent: raccoglie registri e metriche a livello di sistema da host e ospiti sulle istanze EC2 e sui server locali. Per ulteriori informazioni, consulta Raccolta di metriche e log da istanze e On-Premises server Amazon EC2 con l'agente nella Amazon User Guide. CloudWatch CloudWatch

Monitoraggio dello stato delle istanze Amazon EC2

Puoi monitorare lo stato delle tue istanze visualizzando le relative verifiche dello stato e i relativi eventi pianificati.

Una verifica dello stato fornisce le informazioni risultanti dai controlli automatici eseguiti da Amazon EC2, che rilevano gli eventuali problemi specifici con le istanze. Le informazioni di controllo dello stato, insieme ai dati forniti da Amazon CloudWatch, offrono una visibilità operativa dettagliata su ciascuna delle tue istanze.

È anche possibile visualizzare lo stato di specifici eventi pianificati per le istanze. Lo stato degli eventi fornisce informazioni sulle prossime attività pianificate per le istanze, come il riavvio o il ritiro. Fornisce anche l'ora di inizio e di fine pianificata per ciascun evento.

Indice

- Verifiche dello stato delle istanze Amazon EC2
- Controlli dello stato delle applicazioni
- Eventi di modifica dello stato per le istanze Amazon EC2
- Eventi pianificati per le istanze Amazon EC2

Verifiche dello stato delle istanze Amazon EC2

Con i controlli di stato, puoi determinare rapidamente se ci sono problemi che potrebbero impedire alle tue istanze di eseguire le tue applicazioni. Amazon EC2 offre quattro tipi di controlli di stato: sistema, istanza, EBS collegato e applicazione. I controlli di stato del sistema, delle istanze e degli EBS collegati sono gestiti da Amazon EC2 ed eseguiti automaticamente su ogni istanza. I controlli sullo stato delle applicazioni sono facoltativi e monitorano le risposte HTTP o HTTPS delle applicazioni in esecuzione sulle tue istanze. Puoi visualizzare i risultati di tutti i controlli di stato nella console Amazon EC2, nel AWS CLI, o negli SDK. AWS

Le verifiche dello stato vengono eseguite ogni minuto e restituiscono un risultato positivo o negativo. Se vengono superate tutte le verifiche, lo stato complessivo dell'istanza sarà OK. Se invece una o più verifiche non vengono superate, lo stato complessivo sarà impaired (danneggiata). I controlli di stato del sistema, delle istanze e degli EBS allegati sono gestiti da Amazon EC2 e non possono essere disabilitati o eliminati. I controlli dello stato delle applicazioni sono facoltativi; li crei, li associ e li gestisci tu stesso.

Quando un controllo dello stato ha esito negativo, la CloudWatch metrica corrispondente per i controlli di stato viene incrementata. Per ulteriori informazioni, consulta Parametri di controllo dello stato. Puoi utilizzare questi parametri per creare allarmi CloudWatch che vengono attivati in base al risultato delle verifiche dello stato. Ad esempio, puoi creare un allarme che ti avvisi se il risultato delle verifiche dello stato di una specifica istanza è negativo. Per ulteriori informazioni, consulta Crea CloudWatch allarmi per le istanze Amazon EC2 che non superano i controlli di stato.

Puoi anche creare un CloudWatch allarme Amazon che monitora un'istanza Amazon EC2 e ripristina automaticamente l'istanza se viene danneggiata a causa di un problema sottostante. Per ulteriori informazioni, consulta Ripristino automatico dell'istanza.

Indice

- Tipi di verifica dello stato
- Visualizzazione delle verifiche dello stato delle istanze Amazon EC2

- Crea CloudWatch allarmi per le istanze Amazon EC2 che non superano i controlli di stato

Tipi di verifica dello stato

Esistono quattro tipi di controlli di stato.

- Verifiche dello stato del sistema
- Verifiche dello stato delle istanze
- Controlli dello stato dei volumi EBS collegati
- Controlli dello stato delle applicazioni

Verifiche dello stato del sistema

I controlli dello stato del sistema monitorano i AWS sistemi su cui viene eseguita l'istanza. Tali verifiche rilevano i problemi sottostanti della tua istanza per la cui risoluzione è richiesto l'intervento di AWS . Quando un controllo dello stato del sistema fallisce, puoi scegliere di AWS attendere la risoluzione del problema oppure puoi risolverlo tu stesso. Puoi arrestare e avviare manualmente le istanze supportate da Amazon EBS, operazione che nella maggior parte dei casi comporta la migrazione dell'istanza a un nuovo host. Per le istanze sostenute dall'archivio dell'istanza (supportate soltanto per le istanze Linux), puoi terminare e sostituire l'istanza. Si noti che i volumi dell'instance store sono effimeri e tutti i dati vengono persi quando l'istanza viene arrestata.

Di seguito sono riportati esempi di problemi che possono causare il mancato superamento delle verifiche dello stato del sistema:

- Perdita di connettività di rete
- Perdita di alimentazione elettrica del sistema
- Problemi di software sull'host fisico
- Problemi hardware sull'host fisico che incidono sulla raggiungibilità della rete

Se un controllo dello stato del sistema fallisce, aumentiamo la metrica StatusCheckFailed _System.

Istanze Bare Metal

Se si esegue un riavvio su un'istanza bare metal, il controllo dello stato del sistema potrebbe temporaneamente restituire uno stato di errore. Quando l'istanza diventa disponibile, il controllo dello stato del sistema deve restituire uno stato di riuscita.

Verifiche dello stato delle istanze

Verifiche dello stato delle istanze monitorano la connettività del software e della rete della singola istanza. Amazon EC2 verifica lo stato di integrità dell'istanza inviando una richiesta ARP (Address Resolution Protocol) all'interfaccia di rete (NIC). Tali verifiche rilevano i problemi per la cui risoluzione è richiesto il tuo intervento. Se l'esito della verifica dello stato di un'istanza è negativo, solitamente devi risolvere direttamente il problema (ad esempio riavviando l'istanza o modificandone la configurazione).

> **Note**
>
> Le distribuzioni Linux recenti che utilizzano `systemd-networkd` per la configurazione di rete potrebbero creare report sui controlli dell'integrità in modo diverso rispetto alle distribuzioni precedenti. Durante il processo di avvio, questo tipo di rete può iniziare prima e potenzialmente concludere prima di altre attività di avvio, e ciò può influire anche sullo stato dell'istanza. Le verifiche dello stato che dipendono dalla disponibilità di rete possono creare report sullo stato di integrità prima del completamento di altre attività.

Di seguito sono riportati esempi di problemi che possono causare il mancato superamento delle verifiche dello stato delle istanze:

- Verifiche dello stato del sistema non riuscite
- Configurazione errata di rete o startup
- Memoria esaurita
- File system danneggiato
- Kernel non compatibile
- Durante un riavvio, un controllo dello stato dell'istanza può segnalare un errore fino a quando l'istanza non diventa nuovamente disponibile.

Se un controllo dello stato dell'istanza ha esito negativo, incrementiamo la metrica StatusCheckFailed _Instance.

Istanze Bare Metal

Se esegui un riavvio su un'istanza bare metal, il controllo dello stato dell'istanza potrebbe temporaneamente restituire uno stato di errore. Quando l'istanza diventa disponibile, il controllo dello stato dell'istanza deve restituire uno stato di riuscita.

Controlli dello stato dei volumi EBS collegati

I controlli di stato EBS allegati monitorano se i volumi Amazon EBS collegati a un'istanza sono raggiungibili e in grado di completare le operazioni. I/O La `StatusCheckFailed_AttachedEBS` metrica è un valore binario che indica un deterioramento se uno o più volumi EBS collegati all'istanza non sono in grado di completare le operazioni. I/O Questi controlli dello stato rilevano problemi di fondo con l'infrastruttura di calcolo o Amazon EBS. Quando la metrica di controllo dello stato EBS allegata ha esito negativo, è possibile attendere la risoluzione del problema oppure intraprendere azioni, AWS ad esempio la sostituzione dei volumi interessati o l'arresto e il riavvio dell'istanza.

Di seguito sono riportati esempi di problemi che possono causare il mancato superamento dei controlli dello stato dei volumi EBS collegati:

- Problemi hardware o software sui sottosistemi di archiviazione alla base dei volumi EBS
- Problemi hardware sull'host fisico che incidono sulla raggiungibilità dei volumi EBS
- Problemi di connettività tra l'istanza e i volumi EBS

È possibile utilizzare il parametro `StatusCheckFailed_AttachedEBS` per migliorare la resilienza di un carico di lavoro. Puoi utilizzare questa metrica per creare CloudWatch allarmi Amazon che vengono attivati in base al risultato del controllo dello stato. Ad esempio, è possibile eseguire il failover su una zona di disponibilità o su un'istanza secondaria quando si rileva un impatto prolungato. In alternativa, puoi monitorare le I/O prestazioni di ciascun volume collegato utilizzando le CloudWatch metriche EBS per rilevare e sostituire il volume danneggiato. Se il controllo dello stato di EBS indica un problema e il carico di lavoro non si dirige I/O verso i volumi EBS collegati, interrompi e avvia l'istanza per spostarla su un nuovo host. In questo modo puoi risolvere i problemi sottostanti all'host che influiscono sulla raggiungibilità dei volumi EBS. Per ulteriori informazioni, consulta Amazon Metrics for Amazon EBS CloudWatch .

È anche possibile configurare i gruppi di Amazon EC2 Auto Scaling per rilevare gli errori di verifiche dello stato dei volumi EBS collegati e quindi sostituire l'istanza interessata con una nuova. Per ulteriori informazioni, consulta Monitorare e sostituire le istanze di Auto Scaling con volumi Amazon EBS danneggiati nella Guida per l'utente di Amazon EC2 Auto Scaling.

> **Note**
>
> Il parametro di controllo dello stato dei volumi EBS collegati è disponibile solo per le istanze Nitro.

Controlli dello stato delle applicazioni

Utilizza i controlli dello stato delle applicazioni per monitorare la raggiungibilità e la disponibilità della rete delle applicazioni in esecuzione sulle tue istanze Amazon EC2. Con i controlli dello stato delle applicazioni, puoi monitorare le risposte HTTP e HTTPS a livello di applicazione. I controlli dello stato delle applicazioni vengono eseguiti solo sulle istanze a cui sono associate.

È possibile configurare ogni controllo dello stato dell'applicazione per richiedere un percorso HTTP sull'endpoint dell'applicazione e definire i codici di risposta che indicano una risposta corretta.

È possibile sopprimere i controlli sullo stato delle applicazioni durante i riavvii o le distribuzioni per evitare errori falsi positivi durante i tempi di inattività previsti. Per ulteriori informazioni, consulta Gestione della distribuzione, dell'applicazione di patch sul posto e delle sostituzioni.

Di seguito sono riportati alcuni esempi di problemi che possono causare il fallimento dei controlli dello stato delle applicazioni:

- Il processo di candidatura si è bloccato o ha smesso di rispondere
- L'applicazione ha restituito un codice di risposta HTTP che indica un errore interno del servizio applicativo o un altro problema
- Porta dell'applicazione non raggiungibile
- Un problema software o hardware sottostante ha causato il fallimento dell'istanza e la mancata risposta

Se il controllo dello stato dell'applicazione ha esito negativo, incrementiamo la `StatusCheckFailed_Application` metrica.

Per informazioni sulla configurazione dei controlli dello stato delle applicazioni, vedere. Controlli dello stato delle applicazioni

Visualizzazione delle verifiche dello stato delle istanze Amazon EC2

Se l'esito della verifica dello stato di un'istanza è negativo, solitamente devi risolvere direttamente il problema (ad esempio riavviando l'istanza o modificandone la configurazione). Per risolvere direttamente i problemi inerenti l'esito negativo delle verifiche dello stato di sistema o delle istanze, consulta Risoluzione dei problemi relativi alle istanze Amazon EC2 Linux con esito negativo delle verifiche dello stato.

Console

Per visualizzare i controlli di stato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Nella pagina Instances (Istanze), la colonna Status check (Verifiche dello stato) elenca lo stato operativo di ogni istanza.
4. Per visualizzare lo stato di una specifica istanza, seleziona l'istanza, quindi la scheda Stato e allarmi.
5. Per esaminare le CloudWatch metriche per i controlli di stato, nella scheda Stato e allarmi, espandi Metriche per visualizzare i grafici relativi alle seguenti metriche:
   - Verifica stato non riuscita per il sistema
   - Verifica stato non riuscita per l'istanza
   - Verifica dello stato non riuscita per EBS collegato
   - Controllo dello stato non riuscito per l'applicazione

   Per ulteriori informazioni, consulta the section called "Parametri di controllo dello stato".

AWS CLI

Per visualizzare i controlli di stato

Utilizzare il comando describe-instance-status

Esempio: ottieni lo stato di tutte le istanze in esecuzione

```
aws ec2 describe-instance-status
```

Esempio: ottieni lo stato di tutte le istanze

```
aws ec2 describe-instance-status --include-all-instances
```

Esempio: ottieni lo stato di una singola istanza in esecuzione

```
aws ec2 describe-instance-status --instance-ids i-1234567890abcdef0
```

Esempio: ottieni tutte le istanze con uno stato di `impaired`

```
aws ec2 describe-instance-status \
--filters Name=instance-status.status,Values=impaired
```

PowerShell

Per visualizzare i controlli di stato

Utilizza il comando Get-EC2InstanceStatus.

Esempio: ottieni lo stato di tutte le istanze in esecuzione

```
Get-EC2InstanceStatus
```

Esempio: ottieni lo stato di tutte le istanze

```
Get-EC2InstanceStatus -IncludeAllInstance $true
```

Esempio: ottieni lo stato di una singola istanza in esecuzione

```
Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0
```

Esempio: ottieni tutte le istanze con uno stato di `impaired`

```
Get-EC2InstanceStatus \
-Filter @{Name="instance-status.status"; Values="impaired"}
```

Crea CloudWatch allarmi per le istanze Amazon EC2 che non superano i controlli di stato

Puoi utilizzare le metriche di controllo dello stato per creare CloudWatch allarmi che ti notifichino quando una verifica dello stato di un'istanza non è riuscita.

Le verifiche dello stato e gli allarmi di verifica dello stato possono assumere temporaneamente lo stato dati insufficienti se vi sono punti dati dei parametri mancanti. Nonostante sia una circostanza rara, può verificarsi in caso di un'interruzione del sistema di report dei parametri, anche quando un'istanza è integra. Consigliamo di considerare questo stato come avviso di dati mancanti e non come un errore della verifica dello stato o un utilizzo fuori limite dell'allarme. Ciò è particolarmente importante quando si risponde con interventi che prevedono azioni di arresto, terminazione, riavvio o recupero sull'istanza.

Console

Questo esempio configura un allarme che invia una notifica quando un'istanza non supera una verifica dello stato. Facoltativamente, puoi arrestare, terminare o ripristinare l'istanza.

Per creare un allarme di verifica dello stato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Selezionare l'istanza, scegliere la scheda Status Checks (Verifiche dello stato), quindi Actions (Operazioni), Create status check alarm (Crea un allarme di verifica stato).
4. Nella pagina Gestisci CloudWatch allarmi, in Aggiungi o modifica allarme, scegli Crea un avviso.
5. Per la Alarm notification (Notifica allarme), attivare l'opzione per configurare le notifiche Amazon Simple Notification Service (Amazon SNS). Selezionare un argomento Amazon SNS esistente o immettere un nome per creare un nuovo argomento.

   Se aggiungi un indirizzo e-mail all'elenco dei destinatari o hai creato un nuovo argomento, Amazon SNS invia un'e-mail di conferma a ciascun nuovo indirizzo. Ciascun destinatario deve scegliere il link di conferma contenuto nell'e-mail. Solo gli indirizzi confermati ricevono notifiche di avviso.
6. Per Alarm action (Operazione allarme), attivare l'interruttore per specificare un'azione da eseguire quando viene attivato l'allarme. Selezionare l'azione.
7. Per Alarm thresholds (Soglie di allarme), selezionare il parametro e i criteri per l'allarme.

Puoi lasciare le impostazioni di default per Raggruppa campioni per (Media) e per Tipo di dati da campionare (Verifica stato non riuscito: una delle due voci), o modificarle in base alle proprie esigenze.

In Consecutive period (Periodo consecutivo), impostare il numero di periodi che si desidera valutare e, in Period (Periodo), immettere la durata del periodo di valutazione prima di attivare l'allarme e inviare un'e-mail.

8. (Facoltativo) Per Sample metric data (Dati dei parametri di esempio), scegliere Add to dashboard (Aggiungi al pannello di controllo).
9. Scegli Crea.

Se necessario, puoi apportare delle modifiche a un allarme di stato delle istanze.

Per modificare un allarme di verifica dello stato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e scegli Azioni, Monitoraggio, Gestisci CloudWatch allarmi.
4. Nella pagina Gestisci CloudWatch allarmi, in Aggiungi o modifica allarme, scegli Modifica un allarme.
5. Per Search for alarm (Cerca allarme), scegli l'allarme da modificare.
6. Una volta completate le modifiche, scegliere Update (Aggiorna).

AWS CLI

Nell'esempio seguente, l'allarme pubblica una notifica in un argomento SNS, , quando l'istanza non supera la verifica di stato dell'istanza o del sistema per almeno due periodi consecutivi. La CloudWatch metrica utilizzata è. `StatusCheckFailed`

Per creare un allarme di verifica dello stato

1. Selezionare un argomento SNS esistente o crearne uno nuovo. Per ulteriori informazioni, consulta Accessing Amazon SNS in the AWS CLI nella guida per l'utente AWS Command Line Interface .
2. Utilizza il seguente comando list-metrics per visualizzare le CloudWatch metriche Amazon disponibili per Amazon EC2.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. Utilizzare il seguente comando put-metric-alarm per creare l'allarme.

```
aws cloudwatch put-metric-alarm \
    --alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 \
    --metric-name StatusCheckFailed \
    --namespace AWS/EC2 \
    --statistic Maximum \
    --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
    --unit Count \
    --period 300 \
    --evaluation-periods 2 \
    --threshold 1 \
    --comparison-operator GreaterThanOrEqualToThreshold \
    --alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

Il periodo è l'intervallo di tempo, in secondi, in cui vengono raccolte le metriche di Amazon. CloudWatch Questo esempio utilizza 300, ossia 60 secondi moltiplicati per 5 minuti. Il periodo di valutazione è il numero di periodi consecutivi in cui il valore del parametro deve essere paragonato alla soglia. Questo esempio usa 2. Le operazioni di allarme sono le operazioni da eseguire quando l'allarme viene attivato.

PowerShell

Per creare un allarme di verifica dello stato

Utilizza il Write-CWMetricAlarm cmdlet come segue per pubblicare notifiche su un argomento SNS quando l'istanza non supera i controlli di stato per almeno due periodi consecutivi.

```
Write-CWMetricAlarm `
    -AlarmName "StatusCheckFailed-Alarm-for-i-1234567890abcdef0" `
    -MetricName "StatusCheckFailed" `
    -Namespace "AWS/EC2" `
    -Statistic "Maximum" `
    -Dimension @{Name="InstanceId"; Values="i-1234567890abcdef0"} `
    -Unit "Count" `
    -Period 300 `
    -EvaluationPeriod 2 `
    -Threshold 1 `
```

```
    -ComparisonOperator "GreaterThanOrEqualToThreshold" `
    -AlarmAction "arn:aws:sns:us-west-2:111122223333:my-sns-topic"
```

Il periodo è l'intervallo di tempo, in secondi, in cui vengono raccolte le CloudWatch metriche di Amazon. Questo esempio utilizza 300, ossia 60 secondi moltiplicati per 5 minuti. Il periodo di valutazione è il numero di periodi consecutivi in cui il valore del parametro deve essere paragonato alla soglia. Questo esempio usa 2. Le operazioni di allarme sono le operazioni da eseguire quando l'allarme viene attivato.

Controlli dello stato delle applicazioni

I controlli dello stato delle applicazioni ti aiutano a monitorare le prestazioni e lo stato delle applicazioni in esecuzione su Amazon EC2. Con i controlli dello stato delle applicazioni, puoi rilevare e rispondere ai problemi di salute delle applicazioni monitorando le applicazioni attraverso percorsi e porte configurabili. Ad esempio, è possibile utilizzare i controlli dello stato delle applicazioni per confermare che il server Web è in ascolto sulla porta prevista e accetta nuove connessioni.

I controlli dello stato delle applicazioni monitorano le risposte HTTP e HTTPS delle applicazioni su percorsi e porte configurabili. Vengono eseguiti ogni 60 secondi e si integrano con Amazon EC2 Auto Scaling, in modo da poter sostituire automaticamente le istanze le cui applicazioni sono danneggiate.

Indice

- Come funzionano i controlli dello stato delle applicazioni
- Inizia con i controlli dello stato delle applicazioni
- Opzioni di configurazione
- Impostazioni predefinite
- Integrazione con Amazon EC2 Auto Scaling
- Gestione della distribuzione, dell'applicazione di patch sul posto e delle sostituzioni
- Test di una nuova verifica dello stato dell'applicazione
- Rete avanzata
- Best practice
- Risoluzione dei problemi
- Monitora i controlli sullo stato delle applicazioni
- Sicurezza e autorizzazioni
- Prezzi

- Quote

Come funzionano i controlli dello stato delle applicazioni

I controlli dello stato delle applicazioni inviano richieste HTTP o HTTPS a un endpoint in ascolto su una porta di rete dell'istanza ogni 60 secondi. AWS confronta il codice di risposta con il matcher del codice di stato configurato. Il controllo viene contrassegnato come compromesso dopo un numero di richieste consecutive non riuscite e viene ripristinato dopo un numero di richieste consecutive riuscite. Entrambi i conteggi sono predefiniti e sono configurabili. Per ulteriori informazioni, consulta Soglie di valutazione.

> **Note**
>
> I controlli sullo stato dell'applicazione inviano la richiesta di controllo dello stato di salute. HTTP/2
>
> Il controllo del protocollo HTTPS non convalida il certificato del server.

Durante un riavvio, i controlli dello stato dell'applicazione segnalano un errore fino a quando l'istanza non diventa nuovamente disponibile perché l'applicazione non è in grado di rispondere alle richieste di controllo dello stato durante il riavvio del sistema operativo.

Architettura di rete

I controlli sullo stato delle applicazioni provengono dal servizio di controllo dello stato delle applicazioni di Amazon EC2. Per raggiungere le tue istanze, AWS crea un'interfaccia di rete elastica gestita (ENI) nel tuo VPC. AWS crea un ENI per combinazione di sottorete di origine e gruppo di sicurezza a cui sono associate istanze. AWS crea l'ENI gestito quando un controllo dello stato dell'applicazione richiede per la prima volta tale combinazione e lo rimuove quando nessun controllo dello stato dell'applicazione rimanente lo richiede. L'ENI gestito non viene conteggiato nel limite ENI dell'istanza, ma viene conteggiato nella quota delle interfacce di rete per regione per l'account, applicata per zona di disponibilità. Per ulteriori informazioni, consulta la pagina relativa alle quote di Amazon VPC.

Per impostazione predefinita, Amazon EC2 nasconde queste interfacce di rete gestite dalla console e dalle operazioni dell'elenco delle API per gli account che non disponevano di risorse gestite prima che questa impostazione diventasse disponibile. Per modificarne la visibilità, consulta Impostazioni di visibilità delle risorse gestite.

AWS crea un'interfaccia di rete gestita per ogni combinazione di sottorete di origine e gruppo di sicurezza tra le istanze associate. Il numero di interfacce gestite aumenta con il numero di combinazioni distinte di sottorete e gruppi di sicurezza utilizzate dalle istanze monitorate. Il consolidamento delle istanze monitorate in un minor numero di combinazioni di sottorete e gruppi di sicurezza riduce il numero di interfacce gestite. Ad esempio, 200 istanze distribuite su 2 sottoreti che utilizzano tutte un singolo gruppo di sicurezza producono 2 interfacce gestite. Le stesse 200 istanze che utilizzano 3 gruppi di sicurezza in queste 2 sottoreti producono fino a 6 interfacce gestite. Ogni interfaccia corrisponde a una combinazione di sottorete e gruppo di sicurezza.

I controlli dello stato delle applicazioni raggiungono le tue istanze da un punto di vista privato all'interno del tuo VPC. L'ambito descrive l'origine del controllo, non una proprietà dell'indirizzo IP dell'istanza. AWS crea l'ENI gestito in una sottorete all'interno del tuo VPC e raggiunge l'istanza tramite il percorso di rete privato.

Con i percorsi di rete AWS gestiti, il traffico di controllo dello stato proviene da istanze Amazon EC2 AWS gestite nella stessa zona di disponibilità dell'istanza di destinazione (o nella zona di disponibilità principale per i target delle zone locali). Il traffico viaggia sulla rete AWS interna e non attraversa la rete Internet pubblica. Per ulteriori informazioni, consulta le domande frequenti su Amazon VPC sul sito Web di Amazon Web Services.

Con i percorsi di rete gestiti dal cliente, scegli le sottoreti di origine, in modo da poter eseguire controlli da una zona di disponibilità diversa da quella di destinazione. Per ulteriori informazioni, consulta the section called “Cross-Availability Monitoraggio delle zone”.

AWS percorsi di rete gestiti e gestiti dal cliente

I controlli dello stato delle applicazioni supportano due modalità di onboarding che determinano chi seleziona le sottoreti e i gruppi di sicurezza di origine per il controllo dello stato ENI e le sottoreti e i gruppi di sicurezza di destinazione per le istanze di destinazione.

AWS percorsi di rete gestiti

AWS seleziona le sottoreti e i gruppi di sicurezza di origine per il controllo dello stato dell'ENI e le sottoreti e i gruppi di sicurezza di destinazione per le istanze di destinazione.

Customer-managed percorsi di rete

Si specificano le sottoreti e i gruppi di sicurezza di origine per il controllo dello stato dell'ENI e le sottoreti e i gruppi di sicurezza di destinazione per le istanze di destinazione.

Utilizza i percorsi di rete gestiti dal cliente quando devi controllare da quali sottoreti e gruppi di sicurezza proviene il traffico di controllo dello stato, ad esempio quando il tuo VPC è soggetto a rigide segmentazioni di rete, regole firewall o requisiti di conformità che limitano le fonti che possono raggiungere gli endpoint delle applicazioni.

Puoi scegliere la modalità includendo o omettendo il parametro nel comando create. `--health-check-paths` Se si omette il `--health-check-paths` parametro, AWS vengono selezionate le sottoreti e i gruppi di sicurezza di origine e destinazione (AWS percorsi di rete gestiti). Se includi il `--health-check-paths` parametro, li gestisci (percorsi di rete gestiti dal cliente).

Versione IP

Ogni controllo dello stato dell'applicazione è associato a una singola versione IP (IPv4 o IPv6). Per monitorare un'istanza sia su IPv4 che su IPv6, create due controlli di stato dell'applicazione separati e associateli entrambi all'istanza.

I controlli arrivano all'istanza dall'interno del tuo VPC sia per IPv4 che per IPv6.

Controlla i valori di stato

Ogni singolo controllo riporta uno dei seguenti stati:

- `passed`: il controllo è stato completato con successo
- `failed`: il controllo non è riuscito. La risposta include il codice di stato HTTP restituito dall'applicazione. Per indicazioni sull'interpretazione e la correzione, vedereRisoluzione dei problemi.
- `initializing`: il controllo non ha ancora completato la sua prima valutazione
- `insufficient-data`: il controllo non ha ricevuto dati sufficienti per determinare un risultato
- `not-applicable`: il controllo non è associato all'istanza

Lo stato complessivo dell'applicazione riportato per l'istanza aggrega tutti i risultati dei singoli controlli. Lo stato complessivo è uno dei seguenti:

- `ok`: tutti i controlli sono stati superati
- `impaired`: uno o più controlli non riusciti
- `initializing`: uno o più controlli non hanno ancora completato la prima valutazione
- `insufficient-data`: uno o più controlli riportano dati insufficienti

- `not-applicable`: tutti i controlli sullo stato delle applicazioni associati sono esclusi dall'aggregazione
- `suppressed`: la valutazione del controllo dello stato dell'applicazione viene soppressa per l'istanza

Aggregazione

È possibile contrassegnare ogni controllo dello stato dell'applicazione come incluso o escluso dallo stato generale dell'istanza. Per impostazione predefinita, un segno di spunta è`included`.

`included`

Il controllo contribuisce allo stato generale dell'istanza e Amazon EC2 Auto Scaling lo utilizza.

`excluded`

Il controllo riporta lo stato individuale ma non contribuisce allo stato generale dell'istanza e Amazon EC2 Auto Scaling non lo utilizza. Usa questa impostazione per convalidare un nuovo check-in in produzione senza influire sullo stato generale o attivare le sostituzioni di Amazon EC2 Auto Scaling. Questo è il flusso di lavoro consigliato quando si aggiunge un assegno a un carico di lavoro di produzione esistente; vedi. Test di una nuova verifica dello stato dell'applicazione

Inizia con i controlli dello stato delle applicazioni

Prerequisiti

Prima di creare un controllo dello stato dell'applicazione, assicurati di disporre di quanto segue:

- Un VPC con le istanze che desideri monitorare.
- Un endpoint applicativo su ogni istanza in grado di rispondere alle richieste HTTP o HTTPS sulla porta e sul percorso HTTP che configurerai.
- Un gruppo di sicurezza su ogni istanza di destinazione che consente il traffico in entrata sulla porta di controllo proveniente dal gruppo di sicurezza di origine utilizzato dal controllo dello stato dell'applicazione. Consulta Sicurezza e autorizzazioni.

Fase 1: configurazione dell'applicazione

Configura l'endpoint dell'applicazione per rispondere alle richieste HTTP o HTTPS sulla porta e sul percorso HTTP che specificherai al momento della creazione del controllo. Restituisci un codice di risposta incluso nel codice di stato per indicare che l'applicazione è integra.

Assicurati che il gruppo di sicurezza dell'istanza di destinazione consenta il traffico in entrata sulla porta di controllo proveniente dal gruppo di sicurezza di origine utilizzato dal controllo dello stato dell'applicazione. Per i percorsi di rete gestiti, AWS fornisce il gruppo di sicurezza di origine al momento della creazione del controllo. Per i percorsi di rete gestiti dal cliente, si specifica il gruppo di sicurezza di origine al momento della creazione del controllo.

Passaggio 2: creare una definizione di controllo

Usa la AWS CLI per creare un controllo dello stato dell'applicazione.

Console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, in Istanze, scegli Controlli dello stato dell'applicazione.
3. Scegli Crea controllo dello stato dell'applicazione.
4. In Health check logic, configura quanto segue:
   - Protocollo: scegli HTTP o HTTPS.
   - Porta: inserisci la porta su cui l'applicazione è in ascolto.
   - Percorso (opzionale): inserisci il percorso HTTP da richiedere, ad esempio `/healthcheck`.
   - Versione IP: scegli IPv4 o IPv6.
   - Indice dei dispositivi: l'indice dei dispositivi di interfaccia di rete da controllare. Il valore predefinito è "`0`".
5. In Controlli e soglie, imposta il Timeout e, facoltativamente, il Matcher del codice di stato, la soglia di errore, la soglia di successo e il periodo di tolleranza per l'inizializzazione. L'intervallo di controllo è fissato a 60 secondi.
6. In Aggregazione, scegli Incluso perché il controllo contribuisca allo stato generale dell'applicazione e gestisca Amazon EC2 Auto Scaling, oppure Escluso per segnalare il controllo senza influire sullo stato generale.
7. In Percorsi di controllo dello stato, seleziona Non specificare i percorsi di rete (recommended/default) per consentire ad Amazon EC2 di inserire le interfacce di rete di controllo dello stato nelle sottoreti dell'istanza, oppure scegli Specifica i percorsi di rete (avanzato) per definire tu stesso la sottorete di origine, il gruppo di sicurezza e le destinazioni.
8. (Facoltativo) Aggiungi un tag con il nome e altri tag.

9. Scegli Crea controllo dello stato dell'applicazione.

AWS CLI

Per utilizzare percorsi di rete AWS gestiti, omettete il `--health-check-paths` parametro e lasciate AWS selezionare le sottoreti e i gruppi di sicurezza di origine e destinazione.

```
aws ec2 create-application-status-check \
        --protocol https \
        --port 443 \
        --path "/health" \
        --status-code-matcher "200"
```

Per utilizzare percorsi di rete gestiti dal cliente, includete il parametro. `--health-check-paths` Ogni percorso di controllo dello stato contiene un'origine (sottorete e gruppo di sicurezza per il controllo dello stato ENI) e una o più destinazioni (sottorete e gruppo di sicurezza per le istanze di destinazione).

```
aws ec2 create-application-status-check \
        --protocol https \
        --port 443 \
        --path "/health" \
        --status-code-matcher "200" \
        --health-check-paths '[{"Source":
{"SubnetId":"subnet-111","SecurityGroupId":"sg-aaa"},"Destinations":
[{"SubnetId":"subnet-222","SecurityGroupId":"sg-bbb"}]}]'
```

Fase 3: Associare il controllo alle istanze

Associa il controllo alle istanze che desideri monitorare, per ID dell'istanza o per tag.

Console

1. Nel riquadro di navigazione, in Istanze, scegli Controlli dello stato dell'applicazione e seleziona il controllo.
2. Scegli Gestisci le associazioni per il controllo dello stato, quindi scegli Gestisci le associazioni per ID risorsa o Gestisci le associazioni per tag.

3. Per associarti a tutte le istanze di un gruppo Auto Scaling, scegli Gestisci le associazioni per tag e inserisci `aws:autoscaling:groupName` come chiave del tag e il nome del tuo gruppo Auto Scaling come valore.
4. Selezionare Associate (Associa).

AWS CLI

Per ID dell'istanza:

```
aws ec2 associate-application-status-check \
        --application-status-check-id asc-1234567890abcdef0 \
        --instance-ids i-0123456789abcdef0
```

Per tag:

```
aws ec2 associate-application-status-check \
        --application-status-check-id asc-1234567890abcdef0 \
        --target-tag-associations Key=Environment,Value=production
```

Per associarti a tutte le istanze di un gruppo Auto Scaling, usa il tag di `aws:autoscaling:groupName` sistema:

```
aws ec2 associate-application-status-check \
        --application-status-check-id asc-1234567890abcdef0 \
        --target-tag-associations Key=aws:autoscaling:groupName,Value=my-asg
```

Le operazioni di associazione e dissociazione restituiscono risultati positivi e negativi per istanza. Se alcune istanze non possono essere associate (ad esempio, perché il controllo è già associato), tali istanze vengono visualizzate nei risultati non riusciti con un motivo.

Fase 4: Visualizza i risultati

Visualizza lo stato di integrità dell'applicazione per istanza.

Console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).

3. Seleziona l'istanza, quindi scegli la scheda Stato e allarmi.
4. In Controlli dello stato dell'applicazione, controlla lo stato generale e lo stato individuale di ogni controllo associato.

AWS CLI

```
aws ec2 describe-application-status \
        --instance-ids i-0123456789abcdef0
```

La risposta include lo stato generale dell'applicazione e, per ogni controllo associato, lo stato del controllo e, per i controlli non riusciti, il codice di stato HTTP restituito dall'applicazione.

Risposta di esempio:

```
{
        "ApplicationStatuses": [
            {
                "InstanceId": "i-0123456789abcdef0",
                "ApplicationStatus": {
                    "Status": "ok",
                    "Details": [
                        {
                            "ApplicationStatusCheckId": "asc-1234567890abcdef0",
                            "Status": "passed",
                            "Reason": {
                                "Code": "ResponseCodeMatched",
                                "StatusCode": 200,
                                "Protocol": "HTTP"
                            }
                        }
                    ]
                }
            }
        ]
    }
```

Per visualizzare le definizioni dei controlli (non lo stato per istanza), usa describe-application-status-checks. Questo comando restituisce la configurazione dei controlli di stato dell'applicazione, incluse le impostazioni del protocollo, della porta, del percorso HTTP e del codice di stato.

Opzioni di configurazione

I controlli dello stato dell'applicazione accettano diversi parametri di configurazione. Questa sezione spiega i parametri in cui il comportamento non è evidente dal nome del parametro. Per l'elenco completo dei parametri e delle regole di convalida, consulta CreateApplicationStatusCheck e AssociateApplicationStatusCheck nella sezione Amazon EC2 API Reference.

Soglie di valutazione

`FailureThreshold`

Il numero di richieste consecutive non riuscite prima del controllo è contrassegnato come ridotto. Default: 2

`SuccessThreshold`

Il numero di richieste consecutive riuscite prima del controllo viene nuovamente contrassegnato come integro. Default: 2

`Timeout`

Il numero di secondi di attesa per una risposta prima che la richiesta venga registrata come non riuscita. Viene applicato come timeout forzato; se l'applicazione non risponde entro questa finestra, la richiesta viene registrata come un errore indipendentemente dall'eventuale risposta. Predefinito: 6. Intervallo valido: 1-30.

Periodo di tolleranza all'avvio

`InitializationGracePeriodSeconds`

Il numero di secondi di attesa dopo l'avvio di un'istanza prima di AWS iniziare a valutare il controllo. Utilizzate questo parametro per dare alle applicazioni il tempo di iniziare ad ascoltare prima dell'inizio dei controlli. Se il periodo di tolleranza è troppo breve, Amazon EC2 Auto Scaling potrebbe sostituire nuove istanze prima che l'applicazione sia pronta. Impostazione predefinita: 300. Intervallo valido: da 1 a 600.

Ambito IP

`IpScope`

I controlli sullo stato dell'applicazione utilizzano l'`private`ambito; il controllo viene eseguito dall'interno del tuo VPC. Per IPv4, corrisponde all'indirizzo IP privato dell'istanza. Per IPv6, AWS non classifica l'indirizzo come pubblico o privato; il controllo accetta qualsiasi indirizzo IPv6 e lo valuta dall'interno del VPC.

Indice dei dispositivi

`DeviceIndex`

L'indice del dispositivo di rete sull'istanza che AWS viene valutato per il controllo dello stato. Modificalo quando il dispositivo di rete principale della tua istanza non è quello che desideri controllare. Impostazione predefinita: 0.

L'aggregazione, la versione IP e i percorsi di controllo dello stato (sottoreti di origine e destinazione e gruppi di sicurezza) sono trattati nelle rispettive sezioni precedenti di questa pagina.

Impostazioni predefinite

Con i percorsi di rete AWS gestiti, i controlli dello stato delle applicazioni utilizzano le seguenti impostazioni predefinite.

Impostazione	Predefinita
Intervallo di controllo	60 secondi (fisso; non configurabile)
Soglia di errore	2 guasti consecutivi
Soglia di successo	2 successi consecutivi
Timeout	6 secondi
Codice di stato corrispondente	200
Percorso HTTP	/
Versione IP	ipv4

Impostazione	Predefinita
Ambito IP	private
Indice del dispositivo	0
Periodo di tolleranza per l'inizializzazione	300 secondi
Aggregazione	incluso
Sottoreti di origine e gruppi di sicurezza	Gestito da AWS

Integrazione con Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling termina e sostituisce automaticamente le istanze il cui stato complessivo dell'applicazione viene riportato`impaired`, purché il controllo sia incluso nell'aggregazione. Non è richiesta alcuna configurazione del gruppo Auto Scaling oltre all'associazione del controllo dello stato dell'applicazione alle istanze del gruppo.

Amazon EC2 Auto Scaling utilizza lo stato generale dell'istanza, non lo stato di controllo individuale. I controlli contrassegnati `excluded` non determinano le azioni di Amazon EC2 Auto Scaling. I controlli nello `suppressed` stato non determinano le azioni di Amazon EC2 Auto Scaling.

Utilizza il `InitializationGracePeriodSeconds` parametro sul controllo per consentire l'avvio di nuove istanze prima che inizino i controlli sullo stato dell'applicazione. Se il periodo di tolleranza è troppo breve, le nuove istanze potrebbero essere terminate e sostituite da Amazon EC2 Auto Scaling prima che l'applicazione sia pronta a servire il traffico.

Il controllo `InitializationGracePeriodSeconds` imposta il tempo trascorso dall'avvio di un'istanza prima che il controllo inizi a valutare l'applicazione. Impostalo in modo che copra il tempo di avvio dell'applicazione, in modo che il controllo non venga segnalato `impaired` mentre l'applicazione è ancora in fase di avvio. Il periodo di tolleranza per il controllo dello stato di salute del gruppo Auto Scaling è separato. Imposta il tempo trascorso dall'entrata in servizio di un'istanza prima che Amazon EC2 Auto Scaling la interrompa per un controllo di integrità fallito.

Per ulteriori informazioni su come Amazon EC2 Auto Scaling utilizza i controlli di integrità, consulta i controlli dello stato delle istanze in un gruppo Auto Scaling e Use application status checks with an Auto Scaling group nella Amazon EC2 Auto Scaling User Guide.

Gestione della distribuzione, dell'applicazione di patch sul posto e delle sostituzioni

Le implementazioni, l'applicazione di patch sul posto e altre operazioni di manutenzione possono arrestare o riavviare temporaneamente l'applicazione. Durante questo periodo, i controlli sullo stato dell'applicazione segnalano un errore perché l'applicazione non è in grado di rispondere alle richieste di controllo dello stato. Se le istanze fanno parte di un gruppo Auto Scaling con controlli sullo stato delle applicazioni inclusi nell'aggregazione, Amazon EC2 Auto Scaling potrebbe terminare e sostituire queste istanze anche se è prevista l'interruzione.

Opzione A: Sopprimere il controllo

Usa la soppressione per finestre di manutenzione limitate di cui conosci la durata. La soppressione viene applicata a livello di istanza. Specificate una durata o la omettete per sopprimere il controllo finché non disattivate la soppressione.

AWS CLI

```
aws ec2 enable-application-status-check-suppression \
        --instance-ids i-0123456789abcdef0 \
        --duration-seconds 3600
```

La risposta restituisce, per ogni istanza, quando è iniziata la soppressione e quando terminerà. È possibile un successo parziale; alcune istanze potrebbero non essere soppresse e apparire nella risposta con una motivazione.

Per riprendere i controlli prima della scadenza del periodo di soppressione:

```
aws ec2 disable-application-status-check-suppression \
        --instance-ids i-0123456789abcdef0
```

Quando viene soppressa, viene riportato lo stato generale dell'applicazione per l'istanza. `suppressed` Amazon EC2 Auto Scaling non agisce sulle istanze. `suppressed`

Opzione B: escludi l'assegno dall'aggregazione

Se desideri che il controllo continui a valutare e riportare il suo stato individuale ma non influenzi lo stato generale né attivi le azioni di Amazon EC2 Auto Scaling, imposta l'impostazione di aggregazione dell'assegno su. `excluded` Ciò è utile per scenari più duraturi, come l'implementazione di una nuova versione di controllo o la convalida di una modifica senza rischiare la sostituzione e per i casi in cui desideri che la telemetria continui senza impatto operativo.

Per ulteriori informazioni, consulta Aggregazione.

Opzione C: dissociare il controllo

Usa la dissociazione per una rimozione più duratura o indefinita.

```
aws ec2 disassociate-application-status-check \
        --application-status-check-id asc-1234567890abcdef0 \
        --instance-ids i-0123456789abcdef0
```

Se l'hai associato tramite tag, rimuovi il tag dall'istanza da dissociare. Dopo la dissociazione, viene riportato lo stato generale dell'applicazione per l'istanza. `not-applicable`

Linee guida per l'implementazione

Le implementazioni sono lo scenario di manutenzione più comune che richiede la soppressione. Usa la soppressione quando il tuo strumento di distribuzione ha un hook pre-distribuzione e un hook post-distribuzione in modo da poter sopprimere il controllo prima dell'inizio della distribuzione e disabilitare la soppressione al termine della distribuzione.

Lo schema generale è:

1. Nell'hook di pre-distribuzione, chiama enable-application-status-check-suppression per l'istanza, con una durata che copra la finestra di distribuzione prevista.
2. Esegui la distribuzione.
3. Nell'hook successivo alla distribuzione, chiama https://docs.aws.amazon.com/cli/latest/reference/ec2/disable-application-status-check-suppression.html disable-application-status-check-suppression per l'istanza.

Se il tuo strumento di distribuzione non dispone di hook, attiva la soppressione dalla pipeline che richiama la distribuzione. CI/CD

Test di una nuova verifica dello stato dell'applicazione

È possibile convalidare un nuovo controllo dello stato dell'applicazione in produzione prima che inizi a contribuire al monitoraggio a livello di istanza. Imposta l'impostazione di aggregazione su `excluded` quando crei il controllo, quindi conferma che riporti lo stato previsto e i codici di risposta HTTP. Quando sei pronto, modifica l'impostazione `included` in modo che il controllo contribuisca allo stato generale dell'istanza e si integri con Amazon EC2 Auto Scaling.

1. Crea il controllo con l'impostazione di aggregazione impostata su. `excluded`

```
aws ec2 create-application-status-check \
        --protocol https \
        --port 443 \
        --path "/health" \
        --status-code-matcher "200" \
        --aggregation excluded
```

2. Associa il controllo a un'istanza di test o a un sottoinsieme del tuo parco di produzione.
3. Attendi almeno due intervalli di controllo (circa due minuti) per consentire al controllo di completare una valutazione iniziale.
4. Utilizza describe-application-status per verificare che il controllo riporti lo stato previsto e il codice di risposta HTTP.

```
aws ec2 describe-application-status \
        --instance-ids i-0123456789abcdef0
```

5. Se il controllo viene riportato come previsto, aggiorna l'impostazione di aggregazione per `included` fare in modo che il controllo contribuisca allo stato generale dell'istanza e promuova le azioni di Amazon EC2 Auto Scaling.

```
aws ec2 modify-application-status-check \
        --application-status-check-id asc-1234567890abcdef0 \
        --aggregation included
```

Rete avanzata

I controlli dello stato dell'applicazione provengono da un ENI gestito nella sottorete di origine e nel gruppo di sicurezza specificati (o che AWS seleziona automaticamente). Per i carichi di lavoro che richiedono una disponibilità più elevata rispetto a quella fornita da una configurazione a fonte singola o per i carichi di lavoro eseguiti in zone locali o avamposti, considera i seguenti modelli.

Cross-Availability Monitoraggio delle zone

Per la ridondanza della zona di disponibilità, è possibile eseguire controlli di integrità da più di una zona di disponibilità. Con i percorsi di rete gestiti dal cliente, si definiscono percorsi di controllo dello stato le cui origini si trovano in due diverse zone di disponibilità che raggiungono le stesse istanze di destinazione, utilizzando il parametro. `--health-check-paths` Il monitoraggio da due zone

di disponibilità mantiene continui i report sullo stato delle istanze anche se una zona di disponibilità diventa non disponibile.

L'esempio seguente crea un controllo con due percorsi di controllo dello stato le cui origini si trovano in zone di disponibilità diverse, che raggiungono entrambi le stesse istanze di destinazione.

```
aws ec2 create-application-status-check \
        --protocol https \
        --port 443 \
        --path "/health" \
        --status-code-matcher "200" \
        --health-check-paths '[{"Source":{"SubnetId":"subnet-source-
az1","SecurityGroupId":"sg-healthcheck"},"Destinations":[{"SubnetId":"subnet-
app-az1","SecurityGroupId":"sg-app"}]},{"Source":{"SubnetId":"subnet-source-
az2","SecurityGroupId":"sg-healthcheck"},"Destinations":[{"SubnetId":"subnet-app-
az2","SecurityGroupId":"sg-app"}]}]'
```

Local Zones

Per le istanze eseguite in zone AWS locali, l'interfaccia di rete elastica gestita (ENI) risiede nella AWS regione padre, non nella zona locale. Il traffico di Health Check tra la regione madre e le istanze della zona locale attraversa il collegamento del servizio Local Zone, il che potrebbe comportare costi aggiuntivi per il trasferimento dei dati.

Best practice

- Progetta il tuo endpoint di integrità in modo che rifletta lo stato dell'applicazione in esecuzione su quell'istanza. Quando l'endpoint restituisce lo stato di integrità in base all'applicazione stessa, Amazon EC2 Auto Scaling sostituisce solo le istanze effettivamente compromesse. Se la risposta dell'endpoint dipende anche da una risorsa condivisa come un database o un servizio downstream, un problema relativo a tale risorsa può non essere verificato su più istanze contemporaneamente. Ciò può innescare una sostituzione a livello di parco veicoli. Per indicazioni sulla scrittura degli endpoint per il controllo dello stato di salute, consulta Implementazione dei controlli di integrità nella libreria di Amazon Builders.
- Proteggiti dai guasti correlati. Un assegno incluso determina la sostituzione di Amazon EC2 Auto Scaling. Un controllo che fallisce in più istanze contemporaneamente può innescare un'ondata di sostituzioni. Imposta una politica di manutenzione delle istanze nel tuo gruppo Auto Scaling per limitare il numero di istanze che vengono sostituite contemporaneamente. Per ulteriori informazioni, consulta la politica di manutenzione delle istanze nella Amazon EC2 Auto Scaling User Guide.

- Allarme sul numero di istanze danneggiate. Crea un CloudWatch allarme Amazon sulla `StatusCheckFailed_Application` metrica della tua flotta. Un aumento improvviso in molte istanze indica una dipendenza condivisa piuttosto che i guasti delle singole istanze e ti dà il tempo di rispondere prima che le sostituzioni si verifichino a cascata. Per ulteriori informazioni, consulta the section called "Monitora i controlli sullo stato delle applicazioni".
- Rimani entro la quota dell'interfaccia di rete. I controlli dello stato delle applicazioni creano interfacce di rete gestite che vengono conteggiate nella quota delle interfacce di rete per regione. AWS applica questa quota per zona di disponibilità. Monitora il tuo utilizzo in modo che una flotta in crescita non raggiunga la quota. In caso affermativo, AWS non è possibile creare nuove interfacce. Per le relative indicazioni relative agli allarmi relativi alle quote, vederethe section called "Quote".
- Considera le autorizzazioni di controllo dello stato come controllate dalle modifiche. Le azioni IAM che creano, modificano, eliminano, associano, dissociano e sopprimono i controlli di stato delle applicazioni possono influire sulla disponibilità delle istanze. Queste azioni determinano i motivi alla base della sostituzione di Amazon EC2 Auto Scaling. Considera azioni come`ec2:CreateApplicationStatusCheck`, `ec2:AssociateApplicationStatusCheck``ec2:ModifyApplicationStatusCheck`, e controllate dalle modifiche anziché concederle `ec2:EnableApplicationStatusCheckSuppression` come parte dell'accesso generale ad Amazon EC2. Per l'elenco completo delle azioni, consulta l'API Reference di Amazon EC2.

Risoluzione dei problemi

Quando il controllo dello stato dell'applicazione risulta compromesso ma prevedi che l'applicazione sia integra, verifica quanto segue:

1. Raggiungibilità dell'istanza. Conferma che i controlli dello stato dell'istanza e del sistema dell'istanza lo sia`ok`.
2. Regola in entrata del gruppo di sicurezza. Il gruppo di sicurezza dell'istanza di destinazione deve consentire il traffico in entrata sulla porta di controllo dal gruppo di sicurezza di origine utilizzato dal controllo dello stato dell'applicazione. Per i percorsi di rete AWS gestiti, AWS fornisce il gruppo di sicurezza di origine; per i percorsi di rete gestiti dal cliente, utilizza il gruppo di sicurezza specificato come origine.
3. Firewall host. Qualsiasi firewall a livello di host (iptables, Windows Firewall, firewall host di terze parti) sull'istanza deve consentire il traffico in entrata sulla porta di controllo.

4. Endpoint dell'applicazione. L'applicazione deve essere in ascolto sulla porta e sul percorso configurati. Conferma con una richiesta locale dall'istanza (`curl http://localhost:PORT/PATH`).
5. Mancata corrispondenza del protocollo. Se il controllo è configurato come HTTPS ma l'endpoint serve solo HTTP (o viceversa), tutte le chiamate avranno esito negativo.
6. Matcher del codice di stato. Verifica che il codice di risposta effettivo della tua applicazione sia incluso nel codificatore del codice di stato configurato.
7. Percorso di rete. Se hai configurato percorsi di rete gestiti dal cliente, verifica che la sottorete di origine e il gruppo di sicurezza siano connessi alla sottorete di destinazione. Usa VPC Reachability Analyzer per tracciare il percorso di rete.
8. Quota ENI disponibile. AWS crea un'interfaccia di rete elastica gestita (ENI) nel tuo account per ogni combinazione di sottorete di origine e gruppo di sicurezza. Verifica che il tuo account non abbia raggiunto la quota di interfacce di rete per regione, applicata per zona di disponibilità. Se il tuo account ha raggiunto questa quota, AWS non può creare l'ENI gestito e il controllo non può essere eseguito. Per ulteriori informazioni, consulta la pagina relativa alle quote di Amazon VPC.

Codici dei motivi

La risposta describe-application-status include un motivo per ogni controllo. Il motivo contiene il codice di stato HTTP restituito dall'applicazione (sotto forma di numero), insieme al protocollo utilizzato per il controllo. Viene contrassegnato un segno di spunta `passed` se il codice di stato restituito è incluso nel codificatore del codice di stato e in `failed` caso contrario.

Il motivo include anche un codice motivo e, per HTTP-level i risultati, il protocollo e il codice di stato HTTP restituito. Il motivo contiene i seguenti campi:

`Code`

Il codice del motivo del risultato del controllo dello stato della domanda. Uno dei seguenti valori:

- `ResponseCodeMatched`: il codice di stato HTTP restituito dal controllo di integrità corrisponde a quello configurato`StatusCodeMatcher`.
- `ResponseCodeMismatch`: il codice di stato HTTP restituito dal controllo di integrità non corrispondeva a quello configurato`StatusCodeMatcher`.
- `ConnectionTimeout`: la connessione alla destinazione è scaduta.
- `ResponseTimeout`: il controllo sanitario è scaduto in attesa di una risposta dal bersaglio.

- `ConnectionRefused`: il bersaglio ha rifiutato la connessione per il controllo dello stato di salute.
- `ConnectionReset`: la connessione di controllo dello stato è stata ripristinata prima della ricezione di una risposta.

Per `ResponseCodeMatched` e`ResponseCodeMismatch`, il `StatusCode` campo contiene il codice di stato HTTP restituito e il `Protocol` campo contiene il protocollo utilizzato per il controllo dello stato. Per gli errori di connessione`ConnectionTimeout`, ad esempio`ResponseTimeout`,`ConnectionRefused`, e`ConnectionReset`, i `Protocol` campi `StatusCode` and non sono presenti.

`Protocol`

Il protocollo utilizzato per il controllo dello stato di salute. Uno dei `HTTP` nostri`HTTPS`.

`StatusCode`

Il codice di stato HTTP restituito dal controllo dello stato.

Utilizza il codice di stato HTTP restituito per identificare il motivo per cui un controllo non è riuscito. Alcuni esempi comuni:

Codice di stato HTTP	Significato tipico	Soluzione correttiva comune
`200`	L'applicazione ha restituito una risposta positiva.	Nessuna. Si tratta in genere di uno stato integro.
`301`, `302`	L'applicazione ha restituito un reindirizzamento. Le chiamate di controllo dello stato non seguono i reindirizzamenti.	Indirizza il percorso di controllo dello stato alla destinazione del reindiriz zamento o aggiungi il codice di reindirizzamento al tuo codice di stato se lo ritieni valido.
`401`, `403`	L'applicazione richiede l'autenti cazione o l'accesso negato al percorso di controllo dello stato.	Configura il percorso di controllo dello stato in modo che non sia autenticato o esegui i controlli di integrità su un percorso che non richiede credenziali.

Codice di stato HTTP	Significato tipico	Soluzione correttiva comune
`404`	Il percorso di controllo dello stato configurato non è stato trovato nell'applicazione.	Verifica che il percorso corrisponda a quello utilizzato dall'applicazione.
`500`	L'applicazione ha restituito un errore interno del server.	Analizza i log dell'applicazione sull'istanza.
`502`, `503`, `504`	L'applicazione è raggiungibile ma segnala problemi relativi all'upstream o alla capacità.	Analizza lo stato, le dipendenze e la capacità delle applicazioni. Se l'applicazione restituisce questi codici durante l'avvio, `InitializationGracePeriodSeconds` aumentali.

Per la `ApplicationStatusReason` struttura completa, consulta ApplicationStatusReason l'API Reference di Amazon EC2.

Errori comuni

- Il gruppo di sicurezza non consente il traffico in entrata dalla fonte del controllo dello stato sulla porta di controllo.
- L'applicazione è associata all'interfaccia di rete `127.0.0.1` e non è in ascolto.
- Il percorso di controllo dello stato restituisce un reindirizzamento (301, 302) anziché una risposta positiva e lo status code matcher non include il codice di reindirizzamento.
- Il controllo è configurato per HTTPS ma l'applicazione serve solo HTTP o viceversa.
- L'avvio dell'applicazione richiede più tempo rispetto al `InitializationGracePeriodSeconds` valore e Amazon EC2 Auto Scaling sostituisce l'istanza prima che sia pronta.

Monitora i controlli sullo stato delle applicazioni

È possibile monitorare i controlli dello stato delle applicazioni in tre modi:

- Amazon CloudWatch. La `StatusCheckFailed_Application` metrica riflette lo stato complessivo dell'applicazione per l'istanza e può generare allarmi. La metrica viene aggregata

per istanza tra i controlli associati la cui impostazione di aggregazione è. `included` CloudWatch pubblica inoltre una metrica per controllo per ogni controllo associato, denominata. `StatusCheckFailed_Application_`*`application-status-check-id`*

- https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instance-status.htmldescribe-instance-status. Restituisce lo stato generale dell'applicazione insieme alle altre informazioni sullo stato dell'istanza.
- https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-application-status.htmldescribe-application-status. Restituisce risultati dettagliati per istanza, incluso lo stato individuale di ogni controllo associato e il codice di stato HTTP restituito dall'applicazione.

Usa la CloudWatch metrica per l'automazione basata sugli allarmi. Usala `describe-instance-status` quando la richiedi già per verificare lo stato dell'istanza. Usalo `describe-application-status` per una visibilità dettagliata per ogni controllo.

Sicurezza e autorizzazioni

AWS crea e gestisce le interfacce di rete utilizzate per i controlli dello stato delle applicazioni tramite un ruolo collegato al servizio. Non è richiesta alcuna configurazione IAM per consentire al servizio di creare questi ENI. Il ruolo collegato al servizio utilizza la `EC2ApplicationStatusChecksServiceRolePolicy` AWS policy gestita.

Per creare, associare, descrivere, eliminare ed eliminare autonomamente i controlli sullo stato delle applicazioni, l'utente o il ruolo IAM necessita delle autorizzazioni Amazon EC2 corrispondenti. Consulta l'API Reference di Amazon EC2 per l'elenco completo delle azioni.

Il gruppo di sicurezza della tua istanza deve consentire il traffico in entrata dal gruppo di sicurezza di origine di Health Check sulla porta che hai configurato. Con i percorsi di rete AWS gestiti, AWS fornisce il gruppo di sicurezza di origine; con i percorsi di rete gestiti dal cliente, utilizza il gruppo di sicurezza specificato come origine.

Prezzi

I controlli sullo stato delle applicazioni vengono fatturati sui seguenti componenti:

- Una tariffa oraria di 0,01 USD per ogni interfaccia di rete elastica gestita (ENI), per zona di disponibilità.
- CloudWatch I prezzi standard di Amazon si applicano alle metriche di controllo dello stato delle applicazioni.

Quote

I controlli sullo stato delle applicazioni sono soggetti a quote AWS di servizio. Per i nomi delle quote, i valori predefiniti e le descrizioni, consulta gli endpoint e le quote di Amazon EC2 nella Guida generale. AWS

Oltre alle quote di AWS servizio che influiscono sulle interfacce di rete gestite, i controlli dello stato delle applicazioni hanno le seguenti quote di servizio. È possibile visualizzare l'utilizzo e richiedere aumenti dalla console Service Quotas.

In queste quote, un obiettivo è una singola istanza monitorata da un controllo dello stato. Se più di un controllo dello stato monitora un'istanza, ogni associazione tra istanza e controllo dello stato viene conteggiata come destinazione separata. Un'associazione è una singola regola di tag o un ID di singola istanza che si associa a un controllo dello stato. Ogni regola o ID di istanza conta come un'associazione, indipendentemente dal numero di istanze in cui viene risolta.

Quota	Predefinita	Adattabile
Controlli dello stato di salute per account	50	Sì, automaticamente
Associazioni per controllo sanitario	50	Sì, automaticamente
Associazioni per account	200	Sì, automaticamente
Obiettivi per account	5.000	Sì, su richiesta

La maggior parte degli aumenti delle quote viene approvata automaticamente. L'aumento degli obiettivi per account richiede una richiesta e un'approvazione manuale.

> **Important**
>
> Se il numero di obiettivi nel tuo account supera la quota Obiettivi per account, gli obiettivi che superano il limite non vengono monitorati e non segnalano lo stato della domanda. Per evitare lacune nel monitoraggio, mantieni il numero degli obiettivi entro la quota o richiedi un aumento.

Ti consigliamo di creare un CloudWatch allarme Amazon in caso di verifica dello stato della domanda di utilizzo delle quote, in modo da ricevere una notifica prima del raggiungimento di una quota. Service Quotas pubblica le metriche di utilizzo nel `AWS/Usage` namespace in CloudWatch cui puoi creare l'allarme.

Eventi di modifica dello stato per le istanze Amazon EC2

Amazon EC2 invia un `EC2 Instance State-change Notification` evento ad Amazon EventBridge quando lo stato di un'istanza cambia.

Di seguito vengono riportati dati di esempio per questo evento. In questo esempio, l'istanza è entrata nello stato `pending`.

```
{
   "id":"7bf73129-1428-4cd3-a780-95db273d1602",
   "detail-type":"EC2 Instance State-change Notification",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"2021-11-11T21:29:54Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
   ],
   "detail":{
      "instance-id":"i-1234567890abcdef0",
      "state":"pending"
   }
}
```

I valori possibili per `state` sono:

- `pending`
- `running`
- `stopping`
- `stopped`
- `shutting-down`
- `terminated`

Quando avvii un'istanza, il relativo stato diventa `pending` e quindi `running`. Quando arresti un'istanza, il relativo stato diventa `stopping` e quindi `stopped`. Quando termini un'istanza, il relativo stato diventa `shutting-down` e quindi `terminated`. Per ulteriori informazioni, consulta Cambio di stato di un'istanza Amazon EC2.

Creare un allarme che invii un'e-mail quando un'istanza Amazon EC2 cambia stato

Per ricevere notifiche e-mail quando l'istanza cambia stato, crea un argomento Amazon SNS e quindi crea una EventBridge regola per l'`EC2 Instance State-change Notification`evento.

Creazione di un argomento SNS

1. Apri la console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Nel pannello di navigazione, scegli Argomenti.
3. Scegli Create topic (Crea argomento).
4. Per Tipo, scegliere Standard.
5. In Name (Nome) inserisci un nome per l'argomento.
6. Scegli Create topic (Crea argomento).
7. Scegli Crea iscrizione.
8. Per Protocollo, scegli E-mail.
9. In Endpoint inserisci l'indirizzo e-mail utilizzabile che riceve le notifiche.
10. Scegli Crea iscrizione.
11. Riceverai un messaggio e-mail con l'oggetto seguente: AWS Notification - Subscription Confirmation. Segui le istruzioni per confermare la tu sottoscrizione.

Per creare una regola EventBridge

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Scegli Crea regola.
3. In Name (Nome) inserisci un nome per la regola.
4. Per Tipo di regola, scegli Regola con un modello di eventi.
5. Scegli Avanti.
6. Per Event pattern (Modello eventi), procedi come segue:

    a. In Event source (Origine eventi), selezionare Servizi AWS.

b. Per Servizio AWS, scegli EC2.

c. Per il tipo di evento, scegli State-change Notifica di istanza EC2.

d. Per impostazione predefinita, riceverai una notifica per qualsiasi modifica dello stato di qualsiasi istanza. Se preferisci, puoi selezionare stati o istanze specifiche.

7. Scegli Avanti.
8. Specifica un obiettivo come segue:

a. Per Target types (Tipi di target), scegli Servizio AWS.

b. Per Select a target (Seleziona un target), scegli SNS topic (Argomento SNS).

c. In Topic (Argomento), scegli l'argomento SNS creato nella procedura precedente.

9. Scegli Avanti.
10. (Facoltativo) Aggiungi tag alla regola.
11. Scegli Avanti.
12. Scegli Crea regola.
13. Per testare la regola, avvia un cambio di stato. Ad esempio, avvia un'istanza arrestata, arresta un'istanza in esecuzione o avvia una nuova istanza. Riceverai messaggi e-mail con l'oggetto seguente: AWS Notification Message. Il corpo dell'e-mail contiene i dati relativi all'evento.

Eventi pianificati per le istanze Amazon EC2

Per garantire l'affidabilità e le prestazioni dell'infrastruttura, AWS puoi pianificare eventi per riavviare, arrestare e ritirare le istanze. Questi eventi non si verificano di frequente.

Se una delle tue istanze sarà interessata da un evento pianificato, ti AWS avviserà in anticipo via e-mail, utilizzando l'indirizzo email associato al tuo account. AWS L'e-mail fornisce dettagli sull'evento, inclusa la data di inizio e di fine. A seconda del tipo di evento, potresti essere in grado di intervenire per controllarne la tempistica. AWS invia anche un AWS Health evento, che puoi monitorare e gestire utilizzando Amazon EventBridge. Per ulteriori informazioni, consulta Monitoraggio degli eventi AWS Health in Amazon EventBridge.

Gli eventi programmati sono gestiti da AWS. Non puoi pianificare gli eventi pianificati per le tue istanze. Tuttavia, puoi:

- Visualizzare gli eventi pianificati per le istanze
- Personalizzare le notifiche di eventi pianificati per includere tag nella notifica e-mail.

- Ripianificare determinati eventi pianificati.
- Creare finestre di eventi personalizzate per gli eventi pianificati.
- Agire quando è pianificato il riavvio, l'arresto o il ritiro di un'istanza.

Per assicurarti di ricevere notifiche sugli eventi pianificati, verifica le tue informazioni di contatto nella pagina Account.

> **Note**
>
> Quando un'istanza è interessata da un evento pianificato e fa parte di un gruppo con scalabilità automatica, il Amazon EC2 Auto Scaling alla fine la sostituisce come parte dei controlli dell'integrità, senza ulteriori operazioni necessarie da parte tua. Per ulteriori informazioni sui controlli dell'integrità eseguiti da Amazon EC2 Auto Scaling, consultare Controlli dell'integrità per le istanze di un gruppo Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.

Tipi di eventi pianificati

Amazon EC2 può creare i seguenti tipi di eventi pianificati per le istanze, dove l'evento si verifica in un orario pianificato:

Tipo di evento	Codice dell'evento	Azione di eventi
Arresto dell'istanza	`instance-stop`	L'istanza viene arrestata all'orario pianificato. Quando la avvii nuovamente, l'istanza viene migrata a un nuovo host. Si applica solo alle istanze con un volume root Amazon EBS.
Ritiro dell'istanza	`instance-retirement`	L'istanza è arrestata all'orari o pianificato se dispone di un volume root Amazon EBS o terminata se dispone di un volume root Amazon EBS.

Tipo di evento	Codice dell'evento	Azione di eventi
Riavvio dell'istanza	`instance-reboot`	L'istanza è riavviata all'orari o pianificato. L'istanza rimane sull'host e, durante il riavvio, l'host è sottopost o a manutenzione. Questa operazione è nota come riavvio sul posto.
Riavvio del sistema	`system-reboot`	All'orario pianificato, l'istanza è riavviata e migrata a un nuovo host. Questa operazion e è nota come migrazione al riavvio.
Manutenzione sistema	`system-maintenance`	All'orario pianificato, l'istanza potrebbe essere temporane amente interessata dalle operazioni di manutenzione della rete o dell'alimentazione elettrica.

Determinazione del tipo di evento

Puoi verificare il tipo di evento pianificato per la tua istanza.

Console

Determinare il tipo di evento

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione seleziona Events (Eventi).
3. Nella tabella, il codice dell'evento appare nella colonna Tipo di evento.
4. Per filtrare la tabella in modo da mostrare solo gli eventi per le istanze, nel campo di ricerca scegli Tipo di risorsa: istanza dall'elenco dei filtri.

AWS CLI

Determinare il tipo di evento per un'istanza

Utilizzare il comando describe-instance-status Se all'istanza è associato un evento pianificato, l'output fornisce informazioni sull'evento pianificato.

```
aws ec2 describe-instance-status \
    --instance-ids i-1234567890abcdef0 \
    --query InstanceStatuses[].Events
```

Di seguito è riportato un output di esempio. Il codice dell'evento pianificato è `system-reboot`.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2020-03-14T22:00:00.000Z",
            "NotBefore": "2020-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2020-04-05T11:00:00.000Z"
        }
    ]
]
```

PowerShell

Determinare il tipo di evento per un'istanza

Utilizza il cmdlet Get-EC2InstanceStatus. Se all'istanza è associato un evento pianificato, l'output fornisce informazioni sull'evento pianificato.

```
(Get-EC2InstanceStatus `
    -InstanceId i-1234567890abcdef0).Events
```

Di seguito è riportato un output di esempio. Il codice dell'evento pianificato è `system-reboot`.

```
Code              : system-reboot
Description       : The instance is scheduled for a reboot
```

```
InstanceEventId   : instance-event-0d59937288b749b32
NotAfter          : 2020-03-14T22:00:00.000Z
NotBefore         : 2020-03-14T20:00:00.000Z
NotBeforeDeadline : 2020-04-05T11:00:00.000Z
```

Indice

- Gestisci le istanze Amazon EC2 pianificate per l'arresto o il ritiro
- Gestione delle istanze Amazon EC2 per le quali è pianificato il riavvio
- Gestisci le istanze Amazon EC2 pianificate per le operazioni di manutenzione
- Visualizzare gli eventi pianificati che influiscono sulle istanze Amazon EC2
- Personalizzazione delle notifiche per gli eventi pianificati per le istanze EC2
- Ripianifica un evento pianificato per un'istanza EC2
- Creare finestre di eventi personalizzate per eventi pianificati che influiscono sulle istanze Amazon EC2

Gestisci le istanze Amazon EC2 pianificate per l'arresto o il ritiro

Quando AWS rileva un errore irreparabile dell'host sottostante dell'istanza, pianifica l'arresto o la chiusura dell'istanza, a seconda del tipo di volume principale dell'istanza.

- Se l'istanza ha un volume root Amazon EBS, è pianificato l'arresto della stessa.
- Se l'istanza ha un volume root dell'archivio dell'istanza, è pianificata la terminazione dell'istanza.

Per ulteriori informazioni, consulta Ritiro dell'istanza.

> **Important**
>
> Tutti i dati archiviati nei volumi instance store vengono persi quando un'istanza viene arrestata, ibernata o terminata. Ciò include i volumi dell'archivio dell'istanza collegati a un'istanza che ha un volume root EBS. Accertati di salvare i dati contenuti nei volumi instance store di cui potresti aver bisogno successivamente prima che l'istanza venga arrestata o terminata.

Azioni che puoi intraprendere

Azioni che puoi intraprendere per le istanze con un volume root EBS

Quando ricevi una notifica di un evento `instance-stop` pianificato, puoi scegliere tra una delle seguenti azioni:

- Attendi un arresto pianificato: puoi attendere che l'istanza si arresti entro la finestra di manutenzione pianificata.
- Esegui arresto e avvio manuali: puoi arrestare e avviare manualmente l'istanza nel momento che preferisci, comportandone la migrazione in un nuovo host. Non è come riavviare l'istanza. Per ulteriori informazioni, consulta Avvio e arresto di un'istanza Amazon EC2.
- Arresto e avvio automatici: puoi automatizzare un arresto e un avvio immediato in risposta a un evento di arresto `instance-stop` pianificato. Per ulteriori informazioni, consulta Esecuzione di operazioni automaticamente sulle istanze EC2 in risposta a eventi in AWS Health nella Guida per l'utente di AWS Health .

Azioni che puoi intraprendere per le istanze con un volume root dell'archivio dell'istanza

Quando ricevi una notifica di un evento `system-retirement` pianificato e desideri mantenere i tuoi dati, puoi intraprendere le seguenti azioni:

1. Avviare un'istanza sostitutiva dall'AMI più recente.
2. Migrare tutti i dati necessari nell'istanza sostituiva prima della terminazione pianificata dell'istanza.
3. Termina l'istanza originale o attendi che sia terminata come pianificato.

Per ulteriori informazioni sulle azioni che puoi intraprendere, consulta Ritiro dell'istanza.

Gestione delle istanze Amazon EC2 per le quali è pianificato il riavvio

Quando è AWS necessario eseguire attività come l'installazione degli aggiornamenti o la manutenzione dell'host sottostante, può pianificare il riavvio dell'istanza. Durante il riavvio pianificato, l'istanza rimane sullo stesso host o migra su un host diverso, a seconda dell'evento, come segue:

- Evento `instance-reboot`.
  - Durante il riavvio, l'istanza rimane sull'host. Questa operazione è nota come riavvio sul posto.
  - L'host corrente è sottoposto a manutenzione.

  - In genere si completa in pochi secondi.
- Evento `system-reboot`.
  - Durante il riavvio, l'istanza è migrato su un nuovo host. Questa operazione è nota come migrazione al riavvio.
  - In genere è completata in pochi minuti.

Per verificare il tipo di evento pianificato per la tua istanza, consultaDeterminazione del tipo di evento.

Azioni che puoi intraprendere

Quando ricevi una notifica di un evento `instance-reboot` o `system-reboot` pianificato, puoi scegliere tra una delle seguenti azioni:

- Attendi un riavvio pianificato: puoi attendere che si verifichi il riavvio dell'istanza entro la finestra di manutenzione pianificata.
- Ripianifica il riavvio: puoi ripianificare il riavvio dell'istanza a una data e un'ora adatte alle tue esigenze.
- Esegui un riavvio avviato dall'utente: puoi riavviare manualmente l'istanza nel momento che preferisci. Tuttavia, l'esito dipende dall'evento:
  - Evento `instance-reboot`: l'istanza rimane sull'hardware corrente (riavvio sul posto), non è eseguita alcuna manutenzione dell'host e l'evento rimane aperto.
  - Evento `system-reboot`.
    - Se la migrazione al riavvio è abilitata sull'istanza, un riavvio avviato dall'utente tenta di migrare l'istanza su un nuovo hardware. In caso di esito positivo, l'evento è cancellato. In caso di esito negativo, si verifica un riavvio sul posto e l'evento rimane pianificato.
    - Se la migrazione al riavvio è disabilitata sull'istanza, un riavvio avviato dall'utente mantiene l'istanza sullo stesso hardware (riavvio sul posto), non è effettuata alcuna manutenzione dell'host e l'evento rimane pianificato. Quando alla fine si verificherà l'evento pianificato, AWS sposterà l'istanza su un nuovo hardware (migrazione al riavvio).

Dopo aver AWS riavviato l'istanza

Quanto segue si applica dopo il AWS riavvio dell'istanza:

- L'evento pianificato è cancellato.
- La descrizione dell'evento è aggiornata.

- Per un evento `instance-reboot`:
  - La manutenzione dell'host sottostante è completa.
- Per un evento `system-reboot`:
  - L'istanza si sposta su un nuovo host.
  - L'istanza mantiene il suo indirizzo IP e il nome DNS.
  - Eventuali dati sui volumi dell'archivio dell'istanza locale saranno conservati.
- Puoi utilizzare l'istanza dopo averla avviata completamente.

Opzioni alternative

Se non puoi ripianificare l'evento di riavvio o abilitare la migrazione al riavvio per un riavvio avviato dall'utente, ma desideri mantenere il normale funzionamento durante la finestra di manutenzione pianificata, puoi effettuare le seguenti operazioni:

- Per un'istanza con un volume root EBS
  - Arresta e avvia manualmente l'istanza per migrarla su un nuovo host. Non è la stessa cosa che riavviare manualmente l'istanza, in cui l'istanza rimane sullo stesso host.
  - Facoltativamente, automatizza un arresto e un avvio immediati dell'istanza in risposta all'evento di riavvio pianificato. Per ulteriori informazioni, consulta Esecuzione di operazioni automaticamente sulle istanze EC2 in risposta a eventi in AWS Health nella Guida per l'utente di AWS Health .

> **Important**
>
> Quando l'istanza è arrestata, i dati nei volumi dell'archivio dell'istanza sono persi. Per ulteriori informazioni, consulta Avvio e arresto di un'istanza Amazon EC2.

- Per un'istanza con un volume root dell'archivio dell'istanza
  1. Avviare un'istanza sostitutiva dall'AMI più recente.
  2. Migra tutti i dati necessari nell'istanza sostituiva prima della finestra di manutenzione pianificata.
  3. Termina l'istanza originale.

Abilitazione o disabilitazione della migrazione al riavvio

Quando un'istanza è pianificata per un evento `system-reboot`, puoi riavviarla prima dell'evento. Il risultato di un riavvio avviato dall'utente dipende dall'impostazione di migrazione al riavvio dell'istanza:

- Abilitato: un riavvio avviato dall'utente tenta di migrare l'istanza su un nuovo hardware (migrazione al riavvio). In caso di esito positivo, l'evento è cancellato. In caso di esito negativo, si verifica un riavvio sul posto e l'evento rimane pianificato. Tieni presente che, anche se abilitata, la migrazione al riavvio può avvenire solo se l'istanza soddisfa i requisiti di migrazione al riavvio.
- Disabilitato: un riavvio avviato dall'utente mantiene l'istanza sullo stesso hardware (riavvio sul posto), non è effettuata alcuna manutenzione dell'host e l'evento rimane pianificato. Quando alla fine si verificherà l'evento pianificato, l'istanza AWS verrà spostata su un nuovo hardware (migrazione al riavvio).

Un riavvio con migrazione richiede più tempo di un riavvio sul posto:

- In-place riavvio: circa 30 secondi
- Riavvio con migrazione: alcuni minuti

> **Note**
>
> Per impostazione predefinita, le istanze che ricevono una notifica di un evento `system-reboot` sono abilitate per la migrazione al riavvio avviata dall'utente.

Requisiti per abilitare la migrazione al riavvio

La migrazione al riavvio può essere abilitata nelle istanze che soddisfano i seguenti criteri:

Tipi di istanza

Non tutti i tipi di istanza supportano l'abilitazione della migrazione al riavvio. Puoi visualizzare i tipi di istanza che supportano l'abilitazione della migrazione al riavvio.

Console

Per visualizzare i tipi di istanza che supportano l'abilitazione della migrazione al riavvio

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione a sinistra, scegli Instance Types (Tipi di istanza).
3. Nella barra del filtro, inserisci Supporto per la migrazione al riavvio: supportato. Quando immetti i caratteri e viene visualizzato il nome del filtro, potrai selezionarlo.

   La tabella Tipi di istanze mostra tutti i tipi di istanza che supportano l'abilitazione della migrazione al riavvio.

AWS CLI

Per visualizzare i tipi di istanza che supportano l'abilitazione della migrazione al riavvio

Utilizza il comando describe-instance-types con il filtro `reboot-migration-support`.

```
aws ec2 describe-instance-types \
    --filters Name=reboot-migration-support,Values=supported \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Per visualizzare i tipi di istanza che supportano l'abilitazione della migrazione al riavvio

Utilizzare il Get-EC2InstanceType cmdlet con il filtro. `reboot-migration-support`

```
Get-EC2InstanceType `
    -Filter @{Name="reboot-migration-support";Values="true"} | `
    Select InstanceType | Sort-Object InstanceType
```

Tenancy

- Condiviso
- Dedicated Instance

Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2.

Limitazioni

La migrazione al riavvio non è supportata per le istanze con le seguenti caratteristiche:

- Piattaforma: istanze eseguite in modo nativo sull'hypervisor Xen
- Dimensione dell'istanza: istanze `metal`
- Tenancy: host dedicato. Per gli host dedicati, usa il ripristino automatico dell'host dedicato.
- Archiviazione: istanze con volumi di archivio dell'istanza
- Rete: istanze che utilizzano un Elastic Fabric Adapter
- Dimensionamento automatico: istanze appartenenti a un gruppo Auto Scaling

Passaggi per abilitare o disabilitare la migrazione al riavvio

Quando un'istanza riceve un evento `system-reboot`, per impostazione predefinita è abilitata la migrazione al riavvio. Pupi disabilitare la migrazione al riavvio in modo che durante un riavvio avviato dall'utente, l'istanza rimanga sullo stesso hardware (riavvio sul posto).

La configurazione `default` non consente la migrazione al riavvio per un'istanza non supportata. Per ulteriori informazioni, consulta Requisiti per abilitare la migrazione al riavvio.

Puoi disabilitare o abilitare la migrazione al riavvio su un'istanza in esecuzione o arrestata.

AWS CLI

Per disabilitare la migrazione al riavvio

Utilizza il comando modify-instance-metadata-options e imposta il parametro `--reboot-migration` su `disabled`.

```
aws ec2 modify-instance-maintenance-options \

    --instance-id i-0abcdef1234567890 \

    --reboot-migration disabled
```

Per abilitare la migrazione al riavvio

Utilizza il comando modify-instance-metadata-options e imposta il parametro `--reboot-migration` su `default`.

```
aws ec2 modify-instance-maintenance-options \
```

```
    --instance-id i-0abcdef1234567890 \

    --reboot-migration default
```

PowerShell

Per disabilitare la migrazione al riavvio

Utilizza il cmdlet Edit-EC2InstanceMaintenanceOption.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId  `
    -RebootMigration Disabled
```

Per abilitare la migrazione al riavvio

Utilizza il cmdlet Edit-EC2InstanceMaintenanceOption.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId i-1234567890abcdef0 `
    -RebootMigration Enabled
```

Gestisci le istanze Amazon EC2 pianificate per le operazioni di manutenzione

Quando AWS deve mantenere l'host sottostante per un'istanza, pianifica la manutenzione dell'istanza. Esistono due tipi di eventi di manutenzione: della rete e dell'alimentazione elettrica.

- Durante la manutenzione della rete, le istanze per le quali è pianificato l'evento perdono la connettività di rete per un breve periodo di tempo. La normale connettività di rete dell'istanza viene ripristinata al completamento della manutenzione.
- Durante la manutenzione dell'alimentazione elettrica, le istanze per le quali è pianificato l'evento vengono impostate sulla modalità offline per un breve periodo di tempo, quindi vengono riavviate. Tutte le impostazioni di configurazione dell'istanza vengono mantenute anche dopo il riavvio.

Una volta riavviata l'istanza (solitamente l'operazione richiede alcuni minuti), verifica che la tua applicazione funzioni come previsto. A questo punto, all'istanza non dovrebbero più essere associati eventi pianificati oppure, se ciò avvenisse, la descrizione dell'evento pianificato inizia con [Completed]

([Completato]). Talvolta può essere necessaria anche un'ora perché la descrizione dello stato dell'istanza venga aggiornata. Gli eventi di manutenzione completati vengono visualizzati nel pannello di controllo della console di Amazon EC2 per un massimo di una settimana.

Azioni che puoi intraprendere

Azioni che puoi intraprendere per le istanze con un volume root EBS

Quando ricevi una notifica di un evento `system-maintenance`, puoi scegliere tra una delle seguenti azioni:

- Attendi la manutenzione pianificata: puoi attendere che la manutenzione sia eseguita come pianificato
- Esegui arresto manuale e arresta: puoi arrestare e avviare l'istanza, comportandone la migrazione in un nuovo host. Non è come riavviare l'istanza. Per ulteriori informazioni, consulta Avvio e arresto di un'istanza Amazon EC2.
- Arresto e avvio automatizzati: puoi automatizzare un arresto e un avvio immediato in risposta a un evento di manutenzione pianificato. Per ulteriori informazioni, consulta Esecuzione di operazioni automaticamente sulle istanze EC2 in risposta a eventi in AWS Health nella Guida per l'utente di AWS Health .

Azioni che puoi intraprendere per le istanze con un volume root dell'archivio dell'istanza

Quando ricevi una notifica di un evento `system-maintenance`, puoi scegliere tra una delle seguenti azioni:

- Attendi la manutenzione pianificata: puoi attendere che la manutenzione sia eseguita come pianificato
- Avvia un'istanza sostitutiva: se desideri mantenere il normale funzionamento durante la finestra di manutenzione programmata:
  1. Avviare un'istanza sostitutiva dall'AMI più recente.
  2. Migra tutti i dati necessari nell'istanza sostituiva prima della finestra di manutenzione pianificata.
  3. Termina l'istanza originale.

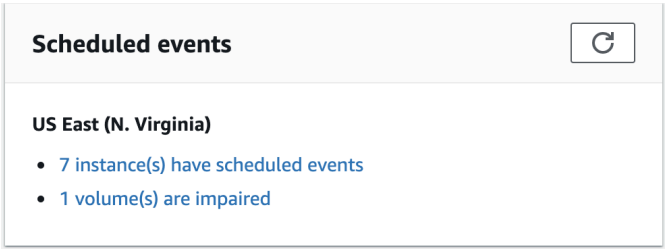
Visualizzare gli eventi pianificati che influiscono sulle istanze Amazon EC2

Oltre a ricevere una notifica e-mail relativa agli eventi pianificati, puoi verificare gli eventi pianificati.

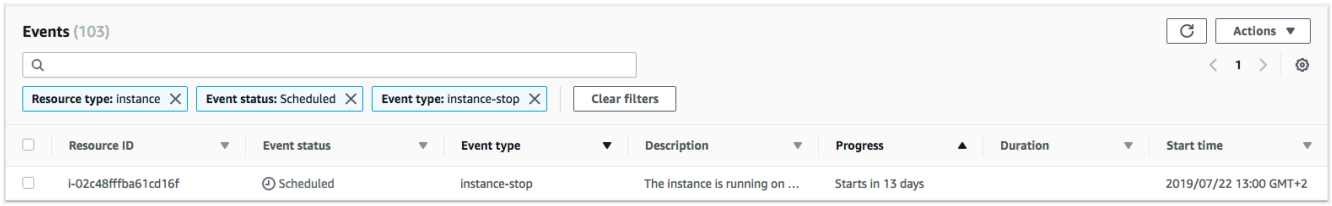
Console

Per visualizzare gli eventi pianificati per le istanze

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. La dashboard visualizza in Eventi pianificati qualsiasi risorsa a cui è associato un evento.



3. Per maggiori dettagli, scegli Eventi nel pannello di navigazione. Vengono visualizzate le risorse a cui è associato un evento. Puoi filtrare per caratteristiche come il tipo di evento, il tipo di risorsa e la zona di disponibilità.



AWS CLI

Per visualizzare gli eventi pianificati per le istanze

Utilizzare il comando describe-instance-status

```
aws ec2 describe-instance-status \
    --instance-ids i-1234567890abcdef0 \
    --query "InstanceStatuses[].Events"
```

Il seguente esempio di output mostra un evento di riavvio.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2019-03-15T22:00:00.000Z",
```

```
            "NotBefore": "2019-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
         }

    ]
]
```

Di seguito è riportato un output di esempio che mostra un evento di ritiro di un'istanza.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0e439355b779n26",

            "Code": "instance-stop",
            "Description": "The instance is running on degraded hardware",
            "NotBefore": "2015-05-23T00:00:00.000Z"
        }
    ]
]
```

PowerShell

Per visualizzare gli eventi pianificati per le istanze

Utilizza il seguente comando Get-EC2InstanceStatus.

```
(Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0).Events
```

Di seguito è riportato un output di esempio che mostra un evento di ritiro di un'istanza.

```
Code         : instance-stop
Description  : The instance is running on degraded hardware
NotBefore    : 5/23/2015 12:00:00 AM
```

Instance metadata

Per visualizzare gli eventi pianificati per le istanze utilizzando i metadati dell'istanza

È possibile recuperare informazioni sugli eventi di manutenzione attivi per le istanze, dai metadati dell'istanza utilizzando Servizio di metadati dell'istanza Versione 2 o Servizio di metadati dell'istanza Versione 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

Segue un esempio di output con informazioni su un evento di riavvio del sistema pianificato, in formato JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "active"
  }
]
```

Per visualizzare la cronologia degli eventi completati o annullati per le istanze che utilizzano i metadati dell'istanza

È possibile recuperare informazioni sugli eventi completati o cancellati per le istanze dai metadati dell'istanza utilizzando Servizio di metadati dell'istanza Versione 2 o Servizio di metadati dell'istanza Versione 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/history
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/
history
```

Segue un output di esempio con informazioni su un evento di riavvio del sistema che è stato cancellato e un evento di riavvio del sistema che è stato completato, in formato JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Canceled] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "canceled"
  },
  {
    "NotBefore" : "29 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Completed] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "29 Jan 2019 09:17:23 GMT",
    "State" : "completed"
  }
]
```

AWS Health

Puoi usare il Dashboard AWS Health per conoscere gli eventi che possono influire sulla tua istanza. Health Dashboard Organizza i problemi in tre gruppi: problemi aperti, modifiche pianificate e altre notifiche. Il gruppo delle modifiche programmate contiene elementi in corso o prossimi.

Per ulteriori informazioni, consulta Nozioni di base su Dashboard AWS Health nella Guida per l'utente di AWS Health .

Personalizzazione delle notifiche per gli eventi pianificati per le istanze EC2

Puoi personalizzare le notifiche di eventi pianificati per includere tag nella notifica e-mail. Questo semplifica l'identificazione della risorsa interessata (istanze o Host dedicati) e l'assegnazione delle priorità alle operazioni per il prossimo evento.

Quando personalizzi le notifiche di eventi per includere i tag, puoi scegliere di includere:

- Tutti i tag associati alla risorsa interessata
- Solo tag specifici associati alla risorsa interessata

Ad esempio, supponi di assegnare i tag `application`, `costcenter`, `project` e `owner` a tutte le istanze. Puoi scegliere di includere tutti i tag nelle notifiche di eventi. In alternativa, se desideri visualizzare solo i tag `owner` e `project` nelle notifiche di eventi, puoi scegliere di includere solo tali tag.

Dopo aver selezionato i tag da includere, le notifiche di eventi includeranno l'ID risorsa (ID istanza o ID Host dedicato) e le coppie valore e chiave tag associate alla risorsa interessata.

Processi

- Inclusione dei tag nelle notifiche di eventi
- Rimozione di tag da notifiche di eventi
- Visualizzazione dei tag da includere nelle notifiche di eventi

Inclusione dei tag nelle notifiche di eventi

I tag che scegli di includere si applicano a tutte le risorse (istanze e Host dedicati) nell'area selezionata. Per personalizzare le notifiche di eventi in altre regioni, seleziona innanzitutto la regione richiesta e quindi esegui le fasi seguenti.

Console

Per includere tag nelle notifiche di eventi

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Scegliere Actions (Operazioni), Manage event notifications (Gestisci notifiche eventi).
4. Attiva Inclusione dei tag nelle notifiche di eventi.
5. Eseguire una delle seguenti operazioni, a seconda dei tag che si desidera includere nelle notifiche di eventi:
   - Per includere tutti i tag associati all'istanza interessata o Host dedicato, selezionare Includi tutti i tag delle risorse.

- Per selezionare i tag da includere, seleziona Scegli i tag da includere, quindi seleziona o inserisci le chiavi di tag.

6. Selezionare Salva.

AWS CLI

Per includere tutti i tag nelle notifiche di eventi

Utilizza il comando register-instance-event-notification-attributes e impostare il parametro `IncludeAllTagsOfInstance` su `true`.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=true"
```

Per includere tag specifici nelle notifiche di eventi

Utilizza il comando register-instance-event-notification-attributes e specifica i tag da includere utilizzando il parametro `InstanceTagKeys`.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

PowerShell

Per includere tutti i tag nelle notifiche di eventi

Utilizza il cmdlet Register-EC2InstanceEventNotificationAttribute.

```
Register-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_IncludeAllTagsOfInstance $true
```

Per includere tag specifici nelle notifiche di eventi

Utilizza il cmdlet Register-EC2InstanceEventNotificationAttribute.

```
Register-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_InstanceTagKey tag_key_1, tag_key_2, tag_key_3
```

Rimozione di tag da notifiche di eventi

Puoi rimuovere di tag da notifiche di eventi

Console

Per rimuovere tag dalle notifiche di eventi

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Scegliere Actions (Operazioni), Manage event notifications (Gestisci notifiche eventi).
4. Per rimuovere tutti i tag dalle notifiche di eventi, disattiva Includi tag delle risorse nelle notifiche di eventi.
5. Per rimuovere tag specifici dalle notifiche degli eventi, scegli la X) per le chiavi di tag corrispondenti.
6. Selezionare Salva.

AWS CLI

Per rimuovere tutti i tag dalle notifiche di eventi

Utilizza il comando deregister-instance-event-notification-attributes e imposta il parametro `IncludeAllTagsOfInstance` su `false`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=false"
```

Per rimuovere tag dalle notifiche di eventi

Utilizza il comando deregister-instance-event-notification-attributes e specifica i tag da rimuovere utilizzando il parametro `InstanceTagKeys`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_3"]'
```

PowerShell

Per rimuovere tutti i tag dalle notifiche di eventi

Utilizza il cmdlet Unregister-EC2InstanceEventNotificationAttribute.

```
Unregister-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_IncludeAllTagsOfInstance $false
```

Per rimuovere tag dalle notifiche di eventi

Utilizza il cmdlet Unregister-EC2InstanceEventNotificationAttribute.

```
Unregister-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_InstanceTagKey tag_key_3
```

Visualizzazione dei tag da includere nelle notifiche di eventi

Puoi visualizzare i tag da includere nelle notifiche degli eventi.

Console

Per visualizzare i tag da includere nelle notifiche di eventi

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Scegliere Actions (Operazioni), Manage event notifications (Gestisci notifiche eventi).

AWS CLI

Per visualizzare i tag da includere nelle notifiche degli eventi

Utilizza il comando describe-instance-event-notification-attributes.

```
aws ec2 describe-instance-event-notification-attributes
```

PowerShell

Per visualizzare i tag da includere nelle notifiche degli eventi

Utilizza il cmdlet Get-EC2InstanceEventNotificationAttribute.

```
Get-EC2InstanceEventNotificationAttribute
```

Ripianifica un evento pianificato per un'istanza EC2

È possibile riprogrammare un evento in modo che si verifichi in una data e un'ora specifiche. Dopo aver riprogrammato un evento, potrebbero essere necessari uno o due minuti prima che sia visualizzata la data aggiornata.

Limitazioni

- Solo gli eventi che possiedono una data di scadenza dell'evento possono essere ripianificati. L'evento può essere ripianificato fino alla data di scadenza dell'evento medesimo. La data di scadenza dell'evento è indicata nella colonna Scadenza (console) e nel campo `NotBeforeDeadline` (AWS CLI).
- Solo gli eventi non ancora iniziati possono essere ripianificati. L'ora di inizio è indicata nella colonna Ora di inizio (console) e nel campo `NotBefore` (AWS CLI). Gli eventi pianificati per l'avvio nei prossimi 5 minuti non possono essere ripianificati.
- La nuova ora di inizio dell'evento deve essere almeno 60 minuti dopo l'ora corrente.
- In caso di ripianificazione di più eventi mediante la console, la data di scadenza dell'evento è determinata dalla data di scadenza dell'evento più vicina.

Console

Per riprogrammare un evento

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Scegliere Resource type: instance (Tipo di risorsa: istanza) dall'elenco dei filtri.
4. Selezionare una o più istanze, quindi selezionare Actions (Operazioni), Schedule Event (Pianificazione evento).

   Solo gli eventi che possiedono una data di scadenza dell'evento, indicata da un valore per Deadline (Scadenza), possono essere ripianificati. Se uno degli eventi selezionati non ha una data di scadenza, Actions (Operazioni), Schedule event (Pianificazione evento) è disabilitato.
5. In New start time (Nuova ora di inizio), inserire una nuova data e ora per il riavvio. La nuova data e ora deve essere precedente alla Event Deadline (Scadenza evento).
6. Selezionare Salva.

Potrebbero essere necessari 1-2 minuti affinché l'ora di inizio dell'evento aggiornata sia visibile nella console.

AWS CLI

Per riprogrammare un evento

Utilizza il comando modify-instance-event-start-time.

```
aws ec2 modify-instance-event-start-time \
    --instance-id i-1234567890abcdef0 \
    --instance-event-id instance-event-0d59937288b749b32 \
    --not-before 2020-03-25T10:00:00.000
```

PowerShell

Per riprogrammare un evento

Utilizza il cmdlet Edit-EC2InstanceEventStartTime.

```
Edit-EC2InstanceEventStartTime `
    -InstanceId i-1234567890abcdef0 `
    -InstanceEventId instance-event-0d59937288b749b32 `
    -NotBefore 2020-03-25T10:00:00.000
```

Creare finestre di eventi personalizzate per eventi pianificati che influiscono sulle istanze Amazon EC2

Puoi definire finestre di eventi personalizzate con ricorrenza settimanale per eventi pianificati che riavviano, arrestano o terminano le istanze Amazon EC2. Puoi associare una o più istanze a una finestra di eventi. Se per tali istanze è programmato un evento pianificato, AWS programmerà gli eventi all'interno della finestra di eventi associata.

Puoi utilizzare le finestre di eventi per aumentare al massimo la disponibilità del carico di lavoro specificando le finestre di eventi che si verificano durante i periodi non di picco per il carico di lavoro. È inoltre possibile allineare le finestre di eventi alle pianificazioni di manutenzione interne.

Puoi definire una finestra di eventi specificando un insieme di intervalli di tempo. La durata minima per un intervallo di tempo è di 2 ore. Gli intervalli di tempo combinati devono essere pari ad almeno 4 ore.

È possibile associare una o più istanze a una finestra di eventi utilizzando ID istanza o tag istanza. Puoi inoltre associare host dedicati a una finestra di evento utilizzando l'ID host.

> **Warning**
>
> Le finestre di eventi sono applicabili solo agli eventi pianificati che arrestano, riavviano o terminano le istanze.
> Le finestre di eventi non sono applicabili a:
>
> - Eventi pianificati accelerati ed eventi di manutenzione della rete.
> - Manutenzione non pianificata, come ripristino automatico dell'istanza e riavvii non pianificati.

Utilizzo delle finestre di eventi

- Considerazioni
- Creazione di una finestra di eventi
- Associazione di una destinazione a una finestra di eventi
- Dissociazione dei tag di istanza da una finestra di eventi
- Modifica di una finestra di eventi
- Eliminazione di una finestra di eventi

Considerazioni

- Tutti gli orari delle finestre di eventi sono in UTC.
- Una finestra di eventi può contenere più intervalli di tempo. Sebbene ogni singolo intervallo debba essere di almeno 2 ore, la durata totale in tutti gli intervalli deve essere di almeno 4 ore.
- A una finestra di eventi è possibile associare un solo tipo di destinazione (ID istanza, ID host dedicato o tag istanza).
- A una finestra di eventi è possibile associare un solo tipo di destinazione (ID istanza, ID host dedicato o tag istanza).

- A una finestra di eventi è possibile associare un massimo di 100 ID istanza o 50 ID host dedicati o 50 tag istanza. I tag istanza possono essere associati a qualsiasi numero di istanze.
- È possibile creare un massimo di 200 finestre di eventi per AWS regione.
- Più istanze associate alle finestre di eventi possono potenzialmente avere eventi pianificati nello stesso momento.
- Se AWS ha già pianificato un evento, la modifica di una finestra dell'evento non cambierà l'ora dell'evento pianificato. Se l'evento ha una data di scadenza, puoi riprogrammare l'evento.
- Puoi arrestare e avviare un'istanza prima dell'evento pianificato. In questo modo l'istanza migra su un nuovo host e l'evento è cancellato.

Creazione di una finestra di eventi

È possibile creare una o più finestre di eventi. Per ogni finestra di eventi, è necessario specificare uno o più blocchi temporali. Ad esempio, puoi creare una finestra di eventi con blocchi temporali che si verificano ogni giorno alle 4 del mattino per 2 ore. Oppure puoi creare una finestra di eventi con blocchi temporali che si verificano la domenica dalle 2 alle 4 e il mercoledì dalle 3 alle 5.

Le finestre di eventi vengono ripetute settimanalmente finché non vengono eliminate.

Console

Per creare una finestra di eventi

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Seleziona Operazioni, Gestisci finestre di eventi.
4. Seleziona Crea finestra di eventi dell'istanza.
5. Per Nome finestra di eventi inserisci un nome descrittivo per la finestra.
6. Per Pianificazione della finestra di eventi, scegli di specificare i blocchi temporali nella finestra di eventi utilizzando il generatore di pianificazione cron o specificando gli intervalli di tempo.
   - Se si sceglie Generatore di pianificazione cron, specifica quanto segue:
     1. Per Giorni (UTC) specifica i giorni della settimana in cui viene visualizzata la finestra di eventi.
     2. Per Ora di inizio (UTC), specifica l'ora in cui inizia la finestra di evento.

3. Per Durata, specifica la durata dei blocchi temporali nella finestra di eventi. La durata minima per un blocco temporale è di 2 ore. La durata minima della finestra di eventi deve essere pari o superiore a 4 ore in totale. Tutti gli orari sono in UTC.

- Se scegli Intervalli di tempo, seleziona Aggiungi un nuovo intervallo di tempo e specifica il giorno e l'ora di inizio e il giorno e l'ora di fine. Ripeti l'operazione per ogni intervallo di tempo. La durata minima per un intervallo di tempo è di 2 ore. La durata minima per tutti gli intervalli di tempo combinati deve essere pari o superiore a 4 ore in totale.

7. (Facoltativo) Per i Dettagli destinazioni, associa una o più istanze alla finestra di eventi. Utilizza gli ID delle istanze o i tag di istanza per associare le istanze. Utilizza gli ID host per associare host dedicati. Quando la manutenzione di queste destinazioni è pianificata, l'evento si verificherà durante questa finestra dell'evento.

   Tieni presente che è possibile creare la finestra di eventi senza associare una destinazione alla finestra. Successivamente, potrai modificare la finestra per associare una o più destinazioni.
8. (Facoltativo) Per Tag della finestra di eventi, seleziona Aggiungi tag e inserisci la chiave e il valore per il tag. Ripetere per ogni tag.
9. Seleziona Crea finestra di eventi.

AWS CLI

Per creare una finestra di eventi con un intervallo temporale

Utilizza il comando create-instance-event-window.

```
aws ec2 create-instance-event-window \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Di seguito è riportato un output di esempio.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
```

```
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Per creare una finestra di eventi con un'espressione cron

Utilizza il comando create-instance-event-window.

```
aws ec2 create-instance-event-window \
    --cron-expression "* 21-23 * * 2,3" \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Di seguito è riportato un output di esempio.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

PowerShell

Per creare una finestra di eventi con un intervallo temporale

Utilizza il cmdlet New-EC2InstanceEventWindow.

```
$timeRange = New-Object Amazon.EC2.Model.InstanceEventWindowTimeRangeRequest
$timeRange.StartWeekDay = "monday"
$timeRange.EndWeekDay = "wednesday"
$timeRange.StartHour = 2
$timeRange.EndHour = 8
$tag = @{Key="key1"; Value="value1"}
$tagspec = New-Object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "instance-event-window"
$tagspec.Tags.Add($tag)
New-EC2InstanceEventWindow `
    -Name my-event-window `
    -TagSpecification $tagspec `
    -TimeRange @($timeRange)
```

Di seguito è riportato un output di esempio.

```
AssociationTarget     :
CronExpression        :
InstanceEventWindowId : iew-0abcdef1234567890
Name                  : my-event-window
State                 : creating
Tags                  : {key1}
TimeRanges            : {Amazon.EC2.Model.InstanceEventWindowTimeRange}
```

Per creare una finestra di eventi con un'espressione cron

Utilizza il cmdlet New-EC2InstanceEventWindow.

```
$tag = @{Key="key1"; Value="value1"}
$tagspec = New-Object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "instance-event-window"
$tagspec.Tags.Add($tag)
New-EC2InstanceEventWindow `
    -Name my-event-window `
    -TagSpecification $tagspec`
    -CronExpression "* 21-23 * * 2,3"
```

Di seguito è riportato un output di esempio.

```
AssociationTarget     :
CronExpression        : * 21-23 * * 2,3
InstanceEventWindowId : iew-0abcdef1234567890
Name                  : my-event-window
State                 : creating
Tags                  : {key1}
TimeRanges            : {}
```

Associazione di una destinazione a una finestra di eventi

Dopo aver creato una finestra dell'evento, puoi associare le destinazioni alla finestra dell'evento. Puoi associare un solo tipo di destinazione a una finestra di eventi. Puoi specificare ID istanza, ID host dedicati o tag istanza.

Console

Per associare ulteriori destinazioni a una finestra di eventi

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione seleziona Events (Eventi).
3. Seleziona la finestra dell'evento da modificare.
4. Scegli Azioni, Modifica la finestra degli eventi dell'istanza.

AWS CLI

Per associare i tag di istanza a una finestra di eventi

Utilizza il comando associate-instance-event-window.

```
aws ec2 associate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Di seguito è riportato un output di esempio.

```
{
    "InstanceEventWindow": {
```

```
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [
                {
                    "Key": "k2",
                    "Value": "v2"
                },
                {
                    "Key": "k1",
                    "Value": "v1"
                }
            ],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Per associare gli ID istanza a una finestra di eventi

Utilizza il comando associate-instance-event-window.

```
aws ec2 associate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Di seguito è riportato un output di esempio.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-1234567890abcdef0",
                "i-0598c7d356eba48d7"
            ],
            "Tags": [],
            "DedicatedHostIds": []
```

```
        },
        "State": "creating"
    }
}
```

Per associare un host dedicato a una finestra di eventi

Utilizza il comando associate-instance-event-window.

```
aws ec2 associate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

Di seguito è riportato un output di esempio.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": [
                "h-029fa35a02b99801d"
            ]
        },
        "State": "creating"
    }
}
```

PowerShell

Per associare i tag di istanza a una finestra di eventi

Utilizza il cmdlet Register-EC2InstanceEventWindow.

```
$tag1 = @{Key="key1"; Value="value1"}
$tag2 = @{Key="key2"; Value="value2"}
Register-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceTag @($tag1,$tag2)
```

Per associare gli ID istanza a una finestra di eventi

Utilizza il cmdlet Register-EC2InstanceEventWindow.

```
Register-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceId i-1234567890abcdef0, i-0598c7d356eba48d7
```

Per associare un host dedicato a una finestra di eventi

Utilizza il cmdlet Register-EC2InstanceEventWindow.

```
Register-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_DedicatedHostId h-029fa35a02b99801d
```

Dissociazione dei tag di istanza da una finestra di eventi

Console

Per dissociare le destinazioni da una finestra di eventi

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione seleziona Events (Eventi).
3. Seleziona la finestra dell'evento da modificare.
4. Scegli Azioni, Modifica la finestra degli eventi dell'istanza.

AWS CLI

Per dissociare i tag di istanza da una finestra di eventi

Utilizza il comando disassociate-instance-event-window.

```
aws ec2 disassociate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Di seguito è riportato un output di esempio.

```
{
```

```
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Per dissociare i tag di istanza da una finestra di eventi

Utilizza il comando disassociate-instance-event-window.

```
aws ec2 disassociate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Di seguito è riportato un output di esempio.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Per dissociare un host dedicato da una finestra di eventi

Utilizza il comando disassociate-instance-event-window.

```
aws ec2 disassociate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
```

```
    --association-target DedicatedHostIds=h-029fa35a02b99801d
```

Di seguito è riportato un output di esempio.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

PowerShell

Per dissociare i tag di istanza da una finestra di eventi

Utilizza il cmdlet Unregister-EC2InstanceEventWindow.

```
$tag1 = @{Key="key1"; Value="value1"}
$tag2 = @{Key="key2"; Value="value2"}
Unregister-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceTag @($tag1, $tag2)
```

Per dissociare i tag di istanza da una finestra di eventi

Utilizza il cmdlet Unregister-EC2InstanceEventWindow.

```
Unregister-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceId i-1234567890abcdef0, i-0598c7d356eba48d7
```

Per dissociare un host dedicato da una finestra di eventi

Utilizza il cmdlet Unregister-EC2InstanceEventWindow.

```
Unregister-EC2InstanceEventWindow `
```

```
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_DedicatedHostId h-029fa35a02b99801d
```

Modifica di una finestra di eventi

È possibile modificare tutti i campi di una finestra di eventi tranne il relativo ID. Ad esempio, quando inizia l'ora legale, è possibile modificare la pianificazione della finestra di eventi. Per le finestre di eventi esistenti, potrebbe essere necessario aggiungere o rimuovere destinazioni.

Durante la modifica della finestra di eventi, è possibile modificare un intervallo temporale o un'espressione cron, ma non entrambi.

Console

Per modificare una finestra di eventi

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Seleziona Operazioni, Gestisci finestre di eventi.
4. Selezionare la finestra degli eventi da modificare, quindi seleziona Operazioni, Modifica finestra di eventi per l'istanza.
5. Modifica i campi nella finestra di eventi e seleziona Modifica finestra di eventi.

AWS CLI

Per modificare l'intervallo temporale di una finestra di eventi

Utilizza il comando modify-instance-event-window.

```
aws ec2 modify-instance-event-window
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

Di seguito è riportato un output di esempio.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
```

```
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Per modificare un insieme di intervalli temporali di una finestra di eventi

Utilizza il comando modify-instance-event-window.

```
aws ec2 modify-instance-event-window
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay":
 "wednesday", "EndHour": 8},
   {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday",
 "EndHour": 8}]'
```

Di seguito è riportato un output di esempio.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
```

```
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            },
            {
                "StartWeekDay": "thursday",
                "StartHour": 2,
                "EndWeekDay": "friday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Per modificare l'espressione cron di una finestra di eventi

Utilizza il comando modify-instance-event-window.

```
aws ec2 modify-instance-event-window
    --instance-event-window-id iew-0abcdef1234567890 \
    --cron-expression "* 21-23 * * 2,3"
```

Di seguito è riportato un output di esempio.

```
{
```

```
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

PowerShell

Per modificare l'intervallo temporale di una finestra di eventi

Utilizza il cmdlet Edit-EC2InstanceEventWindow.

```
$timeRange1 = New-Object Amazon.EC2.Model.InstanceEventWindowTimeRangeRequest
$timeRange1.StartWeekDay = "monday"
$timeRange1.EndWeekDay = "wednesday"
$timeRange1.StartHour = 2
$timeRange1.EndHour = 8
$timeRange2 = New-Object Amazon.EC2.Model.InstanceEventWindowTimeRangeRequest
$timeRange2.StartWeekDay = "thursday"
$timeRange2.EndWeekDay = "friday"
$timeRange2.StartHour = 1
$timeRange2.EndHour = 6
Edit-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -TimeRange @($timeRange1, $timeRange2)
```

Per modificare l'espressione cron di una finestra di eventi

Utilizza il cmdlet Edit-EC2InstanceEventWindow.

```
Edit-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -CronExpression "* 21-23 * * 2,3"
```

Eliminazione di una finestra di eventi

Puoi eliminare una finestra di eventi alla volta.

Console

Per eliminare una finestra di eventi

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione selezionare Events (Eventi).
3. Seleziona Operazioni, Gestisci finestre di eventi.
4. Seleziona la finestra di eventi da eliminare, quindi seleziona Operazioni, Elimina finestra di eventi per l'istanza.
5. Quando richiesto, digitare **`delete`**, quindi scegliere Delete (Elimina).

AWS CLI

Per eliminare una finestra di eventi

Utilizza il comando delete-instance-event-window e specifica la finestra di eventi da eliminare.

```
aws ec2 delete-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890
```

Per forzare l'eliminazione di una finestra di eventi

Utilizza il parametro `--force-delete` se la finestra di eventi è attualmente associata a destinazioni.

```
aws ec2 delete-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --force-delete
```

PowerShell

Per eliminare una finestra di eventi

Utilizza il cmdlet Remove-EC2InstanceEventWindow.

```
Remove-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890
```

Per forzare l'eliminazione di una finestra di eventi

Utilizza il cmdlet Remove-EC2InstanceEventWindow.

```
Remove-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -ForceDelete $true
```

Monitora le tue istanze utilizzando CloudWatch

Puoi monitorare le tue istanze utilizzando Amazon CloudWatch, che raccoglie ed elabora i dati grezzi da Amazon EC2 in metriche leggibili e quasi in tempo reale. Queste statistiche vengono registrate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione Web.

Per impostazione predefinita, Amazon EC2 invia dati metrici a intervalli di 5 minuti. CloudWatch Per inviare dati metrici per la tua istanza CloudWatch in periodi di 1 minuto, puoi abilitare il monitoraggio dettagliato dell'istanza. Per ulteriori informazioni, consulta Gestione del monitoraggio dettagliato per le istanze EC2.

La console Amazon EC2 mostra una serie di grafici basati sui dati grezzi di Amazon. CloudWatch A seconda delle tue esigenze, potresti preferire ottenere i dati per le tue istanze da Amazon CloudWatch anziché dai grafici nella console.

Per informazioni sulla CloudWatch fatturazione e sui costi di Amazon, consulta CloudWatch fatturazione e costi nella Guida per l'utente di Amazon. CloudWatch

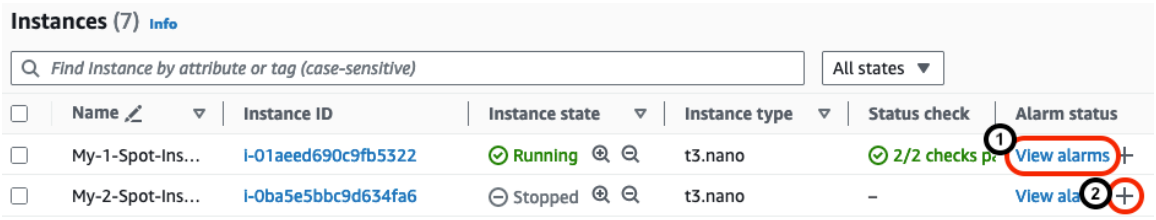
Indice

- Gestisci gli CloudWatch allarmi per le tue istanze EC2 nella console Amazon EC2

- Gestione del monitoraggio dettagliato per le istanze EC2
- CloudWatch metriche disponibili per le tue istanze
- Installa e configura l' CloudWatch agente utilizzando la console Amazon EC2 per aggiungere metriche aggiuntive
- Statistiche relative alle CloudWatch metriche relative alle tue istanze
- Visualizzare i grafici di monitoraggio delle istanze
- Crea un CloudWatch allarme per un'istanza
- Creazione di allarmi che arrestano, terminano, riavviano o recuperano un'istanza

Gestisci gli CloudWatch allarmi per le tue istanze EC2 nella console Amazon EC2

Dalla schermata Istanze della console Amazon EC2, puoi gestire gli CloudWatch allarmi Amazon per le tue istanze. Nella tabella Istanze, la colonna Stato dell'allarme fornisce due controlli della console: uno per visualizzare gli allarmi e l'altro per crearli o modificarli. Il seguente screenshot mostra questi controlli della console, con il numero 1 (Visualizza gli allarmi) e 2 (un segno + per creare o modificare un allarme).



Visualizzare gli allarmi dalla schermata Istanze

È possibile visualizzare gli allarmi di ogni istanza dalla schermata Istanze.

Per visualizzare l'allarme di un'istanza dalla schermata Istanze

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Nella tabella Istanze, vai all'istanza desiderata e seleziona Visualizza gli allarmi (numero 1 nello screenshot precedente).
4. Nella *i-1234567890abcdef0* finestra Dettagli dell'allarme, scegli il nome dell'avviso per visualizzarlo nella CloudWatch console.

Creare allarmi dalla schermata Istanze

È possibile creare un allarme per ogni istanza dalla schermata Istanze.

Per creare un allarme per un'istanza dalla schermata Istanze

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Nella tabella Istanze, vai all'istanza desiderata e seleziona il segno più (numero 2 nello screenshot precedente).
4. Nella schermata Gestisci CloudWatch allarmi, crea la tua sveglia. Per ulteriori informazioni, consulta Crea un CloudWatch allarme per un'istanza.

Modificare gli allarmi dalla schermata Istanze

È possibile modificare l'allarme per un'istanza dalla schermata Istanze.

Per modificare un allarme per un'istanza dalla schermata Istanze

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Nella tabella Istanze, vai all'istanza desiderata e seleziona il segno più (numero 2 nello screenshot precedente).
4. Nella schermata Gestisci CloudWatch allarmi, modifica la sveglia. Per ulteriori informazioni, consulta Modificare o eliminare un CloudWatch allarme nella Amazon CloudWatch User Guide.

Gestione del monitoraggio dettagliato per le istanze EC2

Amazon CloudWatch offre due categorie di monitoraggio: monitoraggio di base e monitoraggio dettagliato. Per impostazione predefinita, l'istanza è configurata con il monitoraggio base. Facoltativamente, è possibile abilitare il monitoraggio dettagliato per identificare e intervenire più rapidamente in caso di problemi operativi. È possibile attivare o disattivare il monitoraggio dettagliato al momento dell'avvio o quando un'istanza è in esecuzione o è stata arrestata.

L'abilitazione del monitoraggio dettagliato su un'istanza non influisce sul monitoraggio dei volumi EBS collegati. Per ulteriori informazioni, consulta Amazon CloudWatch Metrics for Amazon EBS.

La seguente tabella evidenzia le differenze tra il monitoraggio base e il monitoraggio dettagliato delle istanze.

Tipo di monitoraggio	Descrizione	Costi
Monitoraggio base	I parametri di verifica dello stato sono disponibili in periodi di 1 minuto. Tutti gli altri parametri sono disponibili in periodi di 5 minuti.	Nessun costo.
Monitoraggio dettagliato	Puoi ottenere le metriche a intervalli di 1 minuto, a condizione di abilitare il monitoraggio dettagliato per l'istanza. Dopo aver abilitato il monitoraggio dettagliato, puoi aggregare i dati tra gruppi di istanze simili.	Ti viene addebitato in base alla metrica a cui Amazon EC2 invia. CloudWatch Non verrà addebitat o alcun costo per l'archiviazione dei dati. Per ulteriori informazioni, consulta il livello a pagamento nella pagina dei CloudWatch prezzi di Amazon.

Indice

- Autorizzazioni richieste
- Abilitazione del monitoraggio dettagliato al lancio
- Gestione del monitoraggio dettagliato

Autorizzazioni richieste

Per abilitare il monitoraggio dettagliato per un'istanza, l'utente deve disporre dell'autorizzazione per utilizzare l'operazione API MonitorInstances. Per disabilitare il monitoraggio dettagliato per un'istanza, l'utente deve disporre dell'autorizzazione per utilizzare l'operazione API UnmonitorInstances.

Abilitazione del monitoraggio dettagliato al lancio

Utilizzare le seguenti procedure per abilitare il monitoraggio dettagliato al lancio. Per impostazione predefinita, l'istanza utilizza il monitoraggio base.

Console

Per abilitare il monitoraggio dettagliato durante l'avvio di un'istanza

Quando avvii un'istanza utilizzando la console Amazon EC2, in Dettagli avanzati, seleziona la casella di CloudWatch controllo Monitoraggio dettagliato.

AWS CLI

Per abilitare il monitoraggio dettagliato durante l'avvio di un'istanza

Utilizza il comando run-instances con l'opzione `--monitoring`.

```
--monitoring Enabled=true
```

PowerShell

Per abilitare il monitoraggio dettagliato durante l'avvio di un'istanza

Usa il New-EC2Instance cmdlet con il parametro. `-Monitoring`

```
-Monitoring $true
```

Gestione del monitoraggio dettagliato

Utilizzare le seguenti procedure per gestire il monitoraggio dettagliato per un'istanza in esecuzione o arrestata.

Console

Per gestire il monitoraggio dettagliato

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, seleziona Instances (Istanze).
3. Selezionare l'istanza.
4. Seleziona Azioni, Monitoraggio e risoluzione dei problemi, Gestisci il monitoraggio dettagliato.
5. Nella pagina Monitoraggio dettagliato, esegui una delle seguenti operazioni per Monitoraggio dettagliato:
   - Monitoraggio dettagliato: seleziona Abilita.
   - Monitoraggio base: deseleziona Abilita.

6. Scegli Conferma.

AWS CLI

Per abilitare il monitoraggio dettagliato

Utilizza il seguente comando monitor-instances.

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

Per disabilitare il monitoraggio dettagliato

Utilizza il comando unmonitor-instances.

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Per abilitare il monitoraggio dettagliato

Utilizza il cmdlet Start-EC2InstanceMonitoring.

```
Start-EC2InstanceMonitoring -InstanceId i-1234567890abcdef0
```

Per disabilitare il monitoraggio dettagliato

Utilizza il cmdlet Stop-EC2InstanceMonitoring.

```
Stop-EC2InstanceMonitoring -InstanceId i-1234567890abcdef0
```

CloudWatch metriche disponibili per le tue istanze

Amazon EC2 invia i parametri ad Amazon. CloudWatch Puoi utilizzare l'API Console di gestione AWS AWS CLI, la o un'API per elencare le metriche a cui Amazon EC2 invia. CloudWatch Per impostazione predefinita, ciascun punto dati copre i 5 minuti seguenti all'orario di avvio delle attività dell'istanza. Se hai abilitato il monitoraggio dettagliato, ciascun punto dati copre il primo minuto di attività successivo all'orario di avvio. Per le statistiche Minimum (Minimo), Maximum (Massimo) e Average (Media), la granularità minima per i parametri forniti da EC2 è di 1 minuto.

Per informazioni su come visualizzare le metriche disponibili utilizzando Console di gestione AWS o the AWS CLI, consulta Visualizza le metriche disponibili nella Amazon User Guide. CloudWatch

Per informazioni su come ottenere le statistiche relative a questi parametri, consulta Statistiche relative alle CloudWatch metriche relative alle tue istanze.

Indice

- Parametri dell'istanza
- Metriche dell'acceleratore
- Parametri dei crediti CPU
- Parametri degli host dedicati
- Metriche di Amazon EBS per le istanze Nitro-based
- Parametri di controllo dello stato
- Parametri di mirroring del traffico
- Parametri del gruppo con scalabilità automatica
- Dimensioni dei parametri Amazon EC2
- Parametri di utilizzo Amazon EC2

Parametri dell'istanza

Il namespace `AWS/EC2` include i seguenti parametri di istanza.

Parametro	Description	Unità	Statistiche significative
`CPUUtilization`	La percentuale di tempo della CPU fisica che Amazon EC2 utilizza per eseguire l'istanza EC2, che include il tempo impiegato per eseguire sia il codice utente che il codice Amazon EC2. A un livello molto alto, `CPUUtilization` è la somma di `CPUUtilization` guest e `CPUUtilization` hypervisor.	Percent	• Average • Minimum • Maximum

Parametro	Description	Unità	Statistiche significative
	Gli strumenti del tuo sistema operativo possono mostrare una percentuale diversa rispetto a quella CloudWatch dovuta a fattori quali la simulazione di dispositivi legacy, la configura zione di dispositivi non legacy, i carichi di lavoro ad alta intensità di interruzioni, la migrazione in tempo reale e l'aggiornamento in tempo reale.		
`DiskReadOps`	Operazioni di lettura completate da tutti i volumi di instance store disponibili per l'istanza in un determinato periodo di tempo. Per calcolare la media I/O delle operazioni al secondo (IOPS) per il periodo, dividi il totale delle operazioni nel periodo per il numero di secondi in quel periodo. Se non vi sono volumi instance store, il valore è 0 oppure il parametro non è riportato.	Count	• Sum • Average • Minimum • Maximum
`DiskWriteOps`	Operazioni di scrittura completate in tutti i volumi di instance store disponibili per l'istanza in un determinato periodo di tempo. Per calcolare la media I/O delle operazioni al secondo (IOPS) per il periodo, dividi il totale delle operazioni nel periodo per il numero di secondi in quel periodo. Se non vi sono volumi instance store, il valore è 0 oppure il parametro non è riportato.	Count	• Sum • Average • Minimum • Maximum

Parametro	Description	Unità	Statistiche significative
`DiskReadBytes`	Byte letti da tutti i volumi di instance store disponibili per l'istanza. Questo parametro viene utilizzato per determinare il volume dei dati che l'applicazione legge dal disco rigido dell'istanza. Può essere utilizzato per determinare la velocità dell'applicazione. Il numero segnalato è il numero di byte ricevuti durante il periodo. Se utilizzi il monitoraggio di base (5 minuti), puoi dividere questo numero per 300 per Bytes/second trovarlo. Se hai il monitoraggio dettagliato (1 minuto), dividi per 60. Puoi anche usare la funzione matematica CloudWatch metrica `DIFF_TIME` per trovare i byte al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch as`m1`, la `DiskReadBytes` formula matematica delle metriche restituisce la metrica in. `m1/(DIFF_TIME(m1))` bytes/second Per ulteriori informazioni `DIFF_TIME` e altre funzioni matematiche metriche, consulta Use metric math nella Amazon User Guide. CloudWatch Se non vi sono volumi instance store, il valore è 0 oppure il parametro non è riportato.	Bytes	• Sum • Average • Minimum • Maximum

Parametro	Description	Unità	Statistiche significative
`DiskWriteBytes`	Byte scritti in tutti i volumi di instance store disponibili per l'istanza. Questo parametro viene utilizzato per determinare il volume dei dati che l'applicazione scrive sul disco rigido dell'istanza. Può essere utilizzato per determinare la velocità dell'appl icazione. Il numero segnalato è il numero di byte ricevuti durante il periodo. Se utilizzi un monitoraggio di base (5 minuti), puoi dividere questo numero per 300 per trovarlo. Bytes/second Se hai il monitoraggio dettagliato (1 minuto), dividi per 60. Puoi anche usare la funzione matematic a CloudWatch metrica `DIFF_TIME` per trovare i byte al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch asm1, la `DiskWriteBytes` formula matematica delle metriche restituisce la metrica in. `m1/(DIFF_TIME(m1))` bytes/second Per ulteriori informazioni `DIFF_TIME` e altre funzioni matematiche metriche, consulta Use metric math nella Amazon User Guide. CloudWatch Se non vi sono volumi instance store, il valore è 0 oppure il parametro non è riportato.	Bytes	• Sum • Average • Minimum • Maximum

Parametro	Description	Unità	Statistiche significative
`MetadataNoToken`	Il numero di volte in cui è stato effettuato correttamente l'accesso al servizio di metadati di istanza (IMDS) utilizzando un metodo che non utilizza un token. Questo parametro viene utilizzato per determinare se sono presenti processi che accedono ai metadati delle istanze che usano il servizio di metadati di istanza Versione 1 (IMDSv1), che non utilizza un token. Se tutte le richieste utilizzano sessioni supportate da token, ovvero Instance Metadata Service Version 2 (IMDSv2), il valore è 0. Per ulteriori informazioni, consulta Passaggio all'utilizzo di Servizio di metadati dell'istanza Versione 2.	Count	• Sum • Percentiles
`MetadataNoTokenRejected`	Il numero di tentativi di chiamata a IMDSv1 dopo la disattivazione di IMDSv1. Se viene visualizzato questo parametro, significa che una chiamata a IMDSv1 è stata tentata e rifiutata. È necessario riabilitare IMDSv1 o assicurarsi che tutte le chiamate usino IMDSv2. Per ulteriori informazioni, consulta Passaggio all'utilizzo di Servizio di metadati dell'istanza Versione 2.	Count	• Sum • Percentiles

Parametro	Description	Unità	Statistiche significative
`NetworkIn`	Il numero di byte ricevuti dall'istanza su tutte le interfacce di rete. Questo parametro identifica il volume del traffico di rete in entrata in una singola istanza. Il numero segnalato è il numero di byte ricevuti durante il periodo. Se utilizzi un monitoraggio di base (5 minuti) e la statistica è Sum, puoi dividere questo numero per 300 per trovarlo. Bytes/second Se hai il monitoraggio dettagliato (1 minuto) e la statistica è Sum (Somma), dividi per 60.	Bytes	• Sum • Average • Minimum • Maximum
`NetworkOut`	Il numero di byte inviati dall'istanza su tutte le interfacce di rete. Questo parametro identifica il volume del traffico di rete in uscita da una singola istanza. Il numero segnalato è il numero di byte inviati durante il periodo. Se utilizzi il monitoraggio di base (5 minuti) e la statistica è Sum, puoi dividere questo numero per 300 per trovarlo. Bytes/second Se hai il monitoraggio dettagliato (1 minuto) e la statistica è Sum (Somma), dividi per 60.	Bytes	• Sum • Average • Minimum • Maximum

Parametro	Description	Unità	Statistiche significative
`NetworkPackets In`	Il numero di pacchetti ricevuti dall'istanza su tutte le interfacce di rete. Questo parametro identifica il volume del traffico in entrata in termini di numero di pacchetti su una singola istanza. Questo parametro è disponibile solo per il monitoraggio di base (periodi di 5 minuti). Per calcolare il numero di pacchetti al secondo (PPS) ricevuti dall'istanza per 5 minuti, dividi il valore della statistica Sum per 300.	Count	• Sum • Average • Minimum • Maximum
`NetworkPackets Out`	Il numero di pacchetti inviati dall'istanza su tutte le interfacce di rete. Questo parametro identifica il volume del traffico in uscita in termini di numero di pacchetti su una singola istanza. Questo parametro è disponibile solo per il monitoraggio di base (periodi di 5 minuti). Per calcolare il numero di pacchetti al secondo (PPS) inviati dall'istanza nell'arco dei 5 minuti, dividi il valore della statistica Sum (Somma) per 300.	Count	• Sum • Average • Minimum • Maximum

Metriche dell'acceleratore

Il namespace `AWS/EC2` include la seguente metrica di accelerazione per le istanze a calcolo accelerato. Supportato solo su un sottoinsieme di tipi di istanze a calcolo accelerato.

Metrica	Description	Unità	Statistiche significative
`GPUPowerUtilization`	Utilizzo di energia attiva come percentuale della potenza attiva massima.	Percentuale	• Average • Minimum • Maximum

Parametri dei crediti CPU

Il namespace `AWS/EC2` include i seguenti parametri di credito CPU per le istanze dalle prestazioni ottimizzabili.

Parametro	Description	Unità	Statistiche significative
`CPUCreditUsage`	Il numero di crediti CPU spesi dall'istanza per l'utilizzo della CPU. Un credito CPU equivale a un vCPU che viene eseguito al 100% dell'utilizzo per un minuto o una combinazione equivalente di vCPU, utilizzo e tempo (per esempio, un vCPU che viene eseguito al 50% dell'utilizzo per due minuti o due vCPU che vengono eseguiti al 25% dell'utilizzo per due minuti). I parametri di credito CPU sono disponibili solo con una frequenza di 5 minuti. Se specifichi un periodo superiore a 5 minuti, usa la statistica `Sum` al posto di quella `Average`.	Crediti (vCPU-minutes)	• Sum • Average • Minimum • Maximum
`CPUCreditBalance`	Il numero di crediti CPU ottenuti, che un'istanza ha accumulato da quando è stata lanciata o avviata. Per le T2 Standard `CPUCreditBalance` include anche il numero di crediti di lancio che sono stati accumulati.	Crediti (vCPU-minutes)	• Sum • Average • Minimum • Maximum

Parametro	Description	Unità	Statistiche significative
	I crediti vengono accumulati nel saldo del credito dopo che sono stati ottenuti e rimossi dal saldo del credito una volta spesi. Il saldo del credito ha un limite massimo, determinato dalla dimensione dell'istanza. Una volta che il limite viene raggiunto, tutti i nuovi crediti guadagnati vengono scartati. Per le T2 Standard, i crediti di lancio non contano per il limite. I crediti in `CPUCreditBalance` sono disponibili affinché l'istanza li spenda per andare oltre l'utilizzo di base della CPU. Quando l'istanza è in fase di esecuzione, i crediti in `CPUCreditBalance` non scadono. Quando un'istanza T3 o T3a si arresta, il valore `CPUCreditBalance` persiste per sette giorni. Successivamente, tutti i crediti accumulati vengono persi. Quando un'istanza T2 si arresta, il valore `CPUCreditBalance` non persiste e tutti i crediti accumulati vengono persi. I parametri di credito CPU sono disponibili solo con una frequenza di 5 minuti.		

Parametro	Description	Unità	Statistiche significative
`CPUSurplusCreditBalance`	Il numero di crediti extra spesi da un'istanza a `unlimited` quando il rispettivo valore `CPUCreditBalance` è pari a zero. Il valore `CPUSurplusCreditBalance` viene saldato con i crediti CPU ottenuti. Se il numero dei crediti extra va oltre il numero massimo di crediti che un'istanza può ottenere in un periodo di 24 ore, i crediti extra spesi, eccedenti il limite, incorreranno in costi aggiuntivi. I parametri di credito CPU sono disponibili solo con una frequenza di 5 minuti.	Crediti (vCPU-minutes)	• Sum • Average • Minimum • Maximum
`CPUSurplusCreditsCharged`	Il numero di crediti extra spesi da un'istanza, che non sono saldati con i crediti CPU ottenuti e che pertanto incorrono in costi aggiuntivi. I crediti extra spesi subiscono costi aggiuntivi quando si verifica uno dei seguenti casi: • I crediti extra spesi vanno oltre il numero massimo di crediti che un'istanza può ottenere in un periodo di 24 ore. I crediti extra spesi, che eccedono il limite, subiscono costi aggiuntivi alla fine dell'ora; • l'istanza viene arrestata o terminata; • l'istanza passa da `unlimited` a `standard`. I parametri di credito CPU sono disponibili solo con una frequenza di 5 minuti.	Crediti (vCPU-minutes)	• Sum • Average • Minimum • Maximum

Parametri degli host dedicati

Il namespace `AWS/EC2` include i seguenti parametri per gli host dedicati T3.

Metrica	Description	Unità	Statistiche significative
`DedicatedHostCPUUtilization`	La percentuale di capacità di calcolo allocata attualmente in uso dalle istanze in esecuzione sull'host dedicato.	Percent	• Sum • Average • Minimum • Maximum

Metriche di Amazon EBS per le istanze Nitro-based

Il `AWS/EC2` namespace include parametri Amazon EBS aggiuntivi per i volumi collegati a istanze che non sono Nitro-based istanze bare metal.

Metrica	Description	Unità	Statistiche significative
`InstanceEBSIOPSExceededCheck`	Indica se un'applicazione ha tentato di generare IOPS che supera i limiti massimi di IOPS di EBS per l'istanza nell'ultimo minuto. Questa metrica può essere `0` (IOPS non superata) o 1 (IOPS superata).	Nessuno	• Somma • Media • Minimo • Massimo
`InstanceEBSThroughputExceededCheck`	Indica se un'applicazione ha tentato di generare un throughput superiore ai limiti massimi di throughput EBS per l'istanza nell'ultimo minuto. Questa metrica può essere `0` (throughput non superata) o 1 (throughput superato).	Nessuno	• Somma • Media • Minimo • Massimo
`EBSReadOps`	Operazioni di lettura completate da tutti i volumi Amazon EBS collegati all'istanza in un determinato periodo di tempo.	Conteggio	• Somma • Media • Minimo

Metrica	Description	Unità	Statistiche significative
	Per calcolare la media I/O delle operazioni di lettura al secondo (Read IOPS) per il periodo, dividi il totale delle operazioni nel periodo per il numero di secondi in quel periodo. Se utilizzi il monitoraggio base (5 minuti), puoi dividere questo numero per 300 per calcolare le operazioni IOPS di lettura. Se hai il monitoraggio dettagliato (1 minuto), dividi per 60. Puoi anche utilizzare la funzione matematica CloudWatch metrica `DIFF_TIME` per trovare le operazioni al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch as`m1`, la formula `m1/(DIFF_TIME(m1))` matematica metrica restituisce la metrica `EBSReadOps` in. operations/second Per ulteriori informazioni `DIFF_TIME` e altre funzioni matematiche metriche, consulta Use metric math nella Amazon User Guide. CloudWatch		• Massimo

Metrica	Description	Unità	Statistiche significative
`EBSWriteOps`	Le operazioni di scrittura completate su tutti i volumi EBS collegati all'istanza in un determinato periodo di tempo. Per calcolare la media I/O delle operazioni di scrittura al secondo (Write IOPS) per il periodo, dividi il totale delle operazioni nel periodo per il numero di secondi in quel periodo. Se utilizzi il monitoraggio base (5 minuti), puoi dividere questo numero per 300 per calcolare le operazioni IOPS di scrittura. Se hai il monitoraggio dettagliato (1 minuto), dividi per 60. Puoi anche utilizzare la funzione matematica CloudWatch metrica `DIFF_TIME` per trovare le operazioni al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch as`m1`, la formula `m1/(DIFF_TIME(m1))` matematica metrica restituisce la metrica `EBSWriteOps` in. operations/second Per ulteriori informazioni `DIFF_TIME` e altre funzioni matematiche metriche, consulta Use metric math nella Amazon User Guide. CloudWatch	Conteggio	• Somma • Media • Minimo • Massimo

Metrica	Description	Unità	Statistiche significative
`EBSReadBytes`	I byte letti da tutti i volumi EBS collegati all'istanza in un determinato periodo di tempo. Il numero segnalato è il numero di byte letti durante il periodo. Se utilizzi un monitoraggio di base (5 minuti), puoi dividere questo numero per 300 per ottenere Read. Bytes/second Se hai il monitoraggio dettagliato (1 minuto), dividi per 60. Puoi anche usare la funzione matematica CloudWatch metrica `DIFF_TIME` per trovare i byte al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch as`m1`, la `EBSReadBytes` formula matematica delle metriche restituisce la metrica in. `m1/(DIFF_TIME(m1))` bytes/second Per ulteriori informazioni `DIFF_TIME` e altre funzioni matematiche metriche, consulta Use metric math nella Amazon User Guide. CloudWatch	Byte	• Somma • Media • Minimo • Massimo

Metrica	Description	Unità	Statistiche significative
`EBSWriteBytes`	I byte scritti su tutti i volumi EBS collegati all'istanza in un determinato periodo di tempo. Il numero segnalato è il numero di byte scritti durante il periodo. Se utilizzi un monitoraggio di base (5 minuti), puoi dividere questo numero per 300 per trovare Write. Bytes/second Se hai il monitoraggio dettagliato (1 minuto), dividi per 60. Puoi anche usare la funzione matematica CloudWatch metrica `DIFF_TIME` per trovare i byte al secondo. Ad esempio, se hai rappresentato graficamente CloudWatch as`m1`, la `EBSWriteBytes` formula matematica delle metriche restituisce la metrica in. `m1/(DIFF_TIME(m1))` bytes/second Per ulteriori informazioni `DIFF_TIME` e altre funzioni matematiche metriche, consulta Use metric math nella Amazon User Guide. CloudWatch	Byte	• Somma • Media • Minimo • Massimo
`EBSIOBalance%`	Fornisce informazioni sulla percentuale di I/O crediti rimanenti nel burst bucket. Questo parametro è disponibile solo per il monitoraggio base. Questo parametro è disponibile solo per alcune istanze di dimensioni `*.4xlarge` e inferiori che supportano le prestazioni massime per soli 30 minuti almeno una volta ogni 24 ore. La statistica `Sum` non è applicabile a questo parametro.	Percentuale	• Minimo • Massimo

Metrica	Description	Unità	Statistiche significative
`EBSByteBalance%`	Fornisce informazioni sulla percentuale di crediti del throughput rimanenti nel burst bucket. Questo parametro è disponibile solo per il monitoraggio base. Questo parametro è disponibile solo per alcune istanze di dimensioni `*.4xlarge` e inferiori che supportano le prestazioni massime per soli 30 minuti almeno una volta ogni 24 ore. La statistica `Sum` non è applicabile a questo parametro.	Percentuale	• Minimo • Massimo

Per informazioni sui parametri forniti per i volumi EBS, consultare Parametri per i volumi Amazon EBS nella Guida per l'utente di Amazon EBS. Per informazioni sui parametri forniti per i parchi EC2 e parchi istanze spot, consultare Monitora la tua flotta EC2 o la tua flotta Spot utilizzando CloudWatch.

Parametri di controllo dello stato

Per impostazione predefinita, i parametri di controllo dello stato sono disponibili a una frequenza di 1 minuto senza costi aggiuntivi. Per un'istanza appena avviata, i dati del parametro di controllo dello stato sono disponibili solo dopo che l'istanza ha completato lo stato di inizializzazione (entro pochi minuti da quando l'istanza assume lo stato `running`). Per ulteriori informazioni sui controlli di stato EC2, vedere Verifiche dello stato delle istanze Amazon EC2.

Il namespace `AWS/EC2` include i parametri di controllo dello stato descritti di seguito.

Metrica	Description	Unità	Statistiche significative
`StatusCheckFailed`	Indica se l'istanza ha superato tutte le verifiche dello stato nell'ultimo minuto. Questo parametro può essere `0` (superato) o `1` (non riuscito).	Count	• Average • Minimum • Maximum

Metrica	Description	Unità	Statistiche significative
	Per impostazione predefinita, questo parametro è disponibile a una frequenza di 1 minuto senza costi aggiuntivi.		
`StatusCheckFailed_Instance`	Indica se l'istanza ha superato il controllo dello stato dell'istanza nell'ultimo minuto. Questo parametro può essere `0` (superato) o `1` (non riuscito). Per impostazione predefinita, questo parametro è disponibile a una frequenza di 1 minuto senza costi aggiuntivi.	Count	• Average • Minimum • Maximum
`StatusCheckFailed_System`	Indica se l'istanza ha superato il controllo dello stato del sistema nell'ultimo minuto. Questo parametro può essere `0` (superato) o `1` (non riuscito). Per impostazione predefinita, questo parametro è disponibile a una frequenza di 1 minuto senza costi aggiuntivi.	Count	• Average • Minimum • Maximum
`StatusCheckFailed_AttachedEBS`	Indica se l'istanza ha superato il controllo dello stato del volume EBS collegato nell'ultimo minuto. Questo parametro può essere `0` (superato) o `1` (non riuscito). Per impostazione predefinita, questo parametro è disponibile a una frequenza di 1 minuto senza costi aggiuntivi.	Count	• Average • Minimum • Maximum

Il namespace `AWS/EBS` include il parametro di verifica dello stato descritto di seguito.

Metrica	Description	Unità	Statistiche significative
`VolumeStalledIOCheck`	Nota: solo per istanze Nitro. Non pubblicato per i volumi collegati ad Amazon ECS e alle attività. AWS Fargate Riporta se un volume ha superato o meno un controllo I/O bloccato nell'ultimo minuto. Questo parametro può essere `0` (superato) o `1` (non riuscito).	Nessuno	• Average • Minimum • Maximum

Parametri di mirroring del traffico

Il namespace `AWS/EC2` include i parametri per il traffico con mirroring. Per ulteriori informazioni, consulta Monitorare il traffico con mirroring utilizzando Amazon CloudWatch nella Amazon VPC Traffic Mirroring Guide.

Parametri del gruppo con scalabilità automatica

Il namespace `AWS/AutoScaling` include i parametri per i gruppi Auto Scaling. Per ulteriori informazioni, consulta le CloudWatch metriche di monitoraggio per i gruppi e le istanze di Auto Scaling nella Amazon EC2 Auto Scaling User Guide.

Dimensioni dei parametri Amazon EC2

È possibile utilizzare le seguenti dimensioni per perfezionare i parametri elencati nelle tabelle precedenti.

Dimensione	Descrizione
`AutoScalingGroupName`	Questa dimensione filtra i dati richiesti per tutte le istanze in un gruppo di capacità specificato. Un gruppo Auto Scaling è una raccolta di istanze che definisci se utilizzi Auto Scaling. La dimensione è disponibile solo per i parametri di Amazon EC2 quando le istanze si trovano in un gruppo Auto Scaling.

Dimensione	Descrizione
	Disponibile per le istanze con monitoraggio dettagliato o di base abilitato.
`ImageId`	Questa dimensione filtra i dati richiesti per tutte le istanze che eseguono questa Amazon Machine Image (AMI) di Amazon EC2. Disponibile per le istanze con monitoraggio dettagliato abilitato.
`InstanceId`	Questa dimensione filtra i dati richiesti solo per l'istanza identific ata. Ciò aiuta a definire un'istanza esatta dalla quale monitorare i dati.
`InstanceType`	Questa dimensione filtra i dati richiesti per tutte le istanze in esecuzione con questo tipo di istanza specificato. Ciò aiuta a categorizzare i dati in base al tipo di istanza in esecuzion e. Ad esempio, puoi confrontare i dati da un'istanza m1.small e un'istanza m1.large per determinare quale ha il valore commerciale migliore per la tua applicazione. Disponibile per le istanze con monitoraggio dettagliato abilitato.

Parametri di utilizzo Amazon EC2

Puoi utilizzare le metriche di CloudWatch 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 EC2 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 EC2 pubblica i seguenti parametri nel namespace `AWS/Usage`.

Parametro	Descrizione
`ResourceCount`	Il numero delle risorse specificate in esecuzione nell'account. Le risorse sono definite dalle dimensioni associate al parametro. La statistica più utile per questo parametro è `MAXIMUM`, che rappresenta il numero massimo di risorse utilizzate durante il periodo di 1 minuto.

Le seguenti dimensioni vengono utilizzate per perfezionare i parametri di utilizzo pubblicati da Amazon EC2.

Dimensione	Description
`Service`	Il nome del AWS servizio che contiene la risorsa. Per i parametri di utilizzo di Amazon EC2, il valore per questa dimensione è `EC2`.
`Type`	Il tipo di entità che viene segnalato. Attualmente, l'unico valore valido per i parametri di utilizzo Amazon EC2 è `Resource`.
`Resource`	Il tipo di risorsa in esecuzione. Attualmente, l'unico valore valido per i parametri di utilizzo di Amazon EC2 è `vCPU`, che restituisce informazioni sulle istanze in esecuzione.
`Class`	La classe della risorsa monitorata. Per i parametri di utilizzo di Amazon EC2 con `vCPU` come valore della dimensione `Resource`, i valori validi sono `Standard/OnDemand` , `F/OnDemand` , `G/OnDemand` , `Inf/OnDemand` , `P/OnDemand` e `X/OnDemand` . I valori per questa dimensione definiscono la prima lettera dei tipi di istanza segnalati dal parametro. Ad esempio, `Standard/OnDemand` restituisce informazioni su tutte le istanze in esecuzione con tipi che iniziano con A, C, D, H, I, M, R, T e Z e `G/OnDemand` restituisce informazioni su tutte le istanze in esecuzione con tipi che iniziano con G.

Installa e configura l' CloudWatch agente utilizzando la console Amazon EC2 per aggiungere metriche aggiuntive

Description
L'installazione e la configurazione dell' CloudWatch agente tramite la console Amazon EC2 sono in versione beta per Amazon EC2 e sono soggette a modifiche.

Per impostazione predefinita, Amazon CloudWatch fornisce metriche di base, come `CPUUtilization` e `NetworkIn`, per il monitoraggio delle istanze Amazon EC2. Per raccogliere metriche aggiuntive, puoi installare l' CloudWatch agente sulle tue istanze EC2 e quindi configurarlo per emettere le metriche selezionate. Invece di installare e configurare manualmente l' CloudWatch agente su ogni istanza EC2, puoi utilizzare la console Amazon EC2 per eseguire questa operazione al posto tuo.

Puoi utilizzare la console Amazon EC2 per installare l' CloudWatch agente sulle tue istanze e configurarlo in modo che emetta le metriche selezionate.

In alternativa, per completare questo processo manualmente, consulta Installazione CloudWatch dell'agente nella Amazon User Guide. CloudWatch Per ulteriori informazioni sull' CloudWatch agente, consulta Raccogli metriche, log e tracce utilizzando l' CloudWatch agente.

Indice

- Prerequisiti
- Come funziona
- Costi
- Installa e configura l'agente CloudWatch

Prerequisiti

Per utilizzare Amazon EC2 per installare e configurare l' CloudWatch agente, devi soddisfare i prerequisiti per l'utente e l'istanza descritti in questa sezione.

> **Tip**
>
> Questa funzionalità non è disponibile in tutte le versioni. Regioni AWS Se la voce di menu descritta nella procedura di installazione in questa pagina non esiste nella console Amazon EC2 e puoi essere flessibile su dove eseguire le istanze, prova un'altra regione. Altrimenti, puoi utilizzare le istruzioni manuali contenute nella Amazon CloudWatch User Guide per installare e configurare l'agente.

Prerequisiti dell'utente

Per utilizzare questa funzionalità, l'utente o il ruolo IAM della console devono disporre delle autorizzazioni necessarie per l'utilizzo di Amazon EC2 e delle seguenti autorizzazioni IAM:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/EC2-Custom-Metrics-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:ListCommandInvocations",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetInstanceProfile",
                "iam:SimulatePrincipalPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Prerequisiti dell'istanza

- Stato dell'istanza: `running`
- Sistema operativo supportato: Linux
- AWS Systems Manager Agente (agente SSM): installato. Due note sull'agente SSM:
  - L'agente SSM è preinstallato su alcune Amazon Machine Images (AMI) fornite da AWS terze parti affidabili. Per informazioni sulle AMI supportate e istruzioni per l'installazione dell'agente SSM, consultare Amazon Machine Images (AMI) con agente SSM preinstallato nella Guida per l'utente di AWS Systems Manager .
  - In caso di problemi con l'agente SSM, consultare Risoluzione dei problemi dell'agente SSM nella Guida per l'utente di AWS Systems Manager .
- Autorizzazioni IAM per l'istanza: le seguenti politiche AWS gestite devono essere aggiunte a un ruolo IAM collegato all'istanza:
  - AmazonSSMManagedInstanceCore— Consente a un'istanza di utilizzare Systems Manager per installare e configurare l' CloudWatch agente.
  - CloudWatchAgentServerPolicy— Consente a un'istanza di utilizzare l' CloudWatchagente per scrivere dati CloudWatch.

  Per informazioni su come aggiungere autorizzazioni IAM alle istanze, consulta Use instance profiles nella Guida per l'utente IAM.

Come funziona

Prima di poter utilizzare la console Amazon EC2 per installare e configurare l' CloudWatch agente, devi assicurarti che il tuo utente o ruolo IAM e le istanze su cui desideri aggiungere le metriche soddisfino determinati prerequisiti. Quindi, puoi utilizzare la console Amazon EC2 per installare e configurare l' CloudWatch agente sulle istanze selezionate.

Per prima cosa, incontra il prerequisiti

- Sono necessarie le autorizzazioni IAM richieste: prima di iniziare, assicurarsi che l'utente o il ruolo della console dispongano delle autorizzazioni IAM necessarie per utilizzare questa funzionalità.
- Istanze: per utilizzare la funzionalità, le istanze EC2 devono essere istanze Linux, avere l'agente SSM installato, disporre delle autorizzazioni IAM richieste ed essere in esecuzione.

Allora puoi usa la funzione

1. Seleziona le tue istanze: nella console Amazon EC2, selezioni le istanze su cui installare e configurare l'agente. CloudWatch Quindi avvii il processo scegliendo Configure agent. CloudWatch
2. Convalida dell'agente SSM: Amazon EC2 verifica che l'agente SSM sia installato e avviato su ogni istanza. Tutte le istanze che non superano questo controllo vengono escluse dal processo. L'agente SSM viene utilizzato per eseguire azioni sull'istanza durante questo processo.
3. Convalida delle autorizzazioni IAM: Amazon EC2 verifica che ogni istanza disponga delle autorizzazioni IAM necessarie per questo processo. Tutte le istanze che non superano questo controllo vengono escluse dal processo. Le autorizzazioni IAM consentono all' CloudWatch agente di raccogliere le metriche dall'istanza e di integrarle AWS Systems Manager per utilizzare l'agente SSM.
4. CloudWatch Agente di convalida: Amazon EC2 verifica che l' CloudWatch agente sia installato e in esecuzione su ogni istanza. Se alcune istanze non superano questo controllo, Amazon EC2 offre l'installazione e l'avvio dell' CloudWatch agente per te. L' CloudWatch agente raccoglierà le metriche selezionate su ciascuna istanza al termine del processo.
5. Seleziona la configurazione delle metriche: selezioni le metriche che l' CloudWatch agente deve emettere dalle tue istanze. Una volta selezionati, Amazon EC2 archivia un file di configurazione in Parameter Store, dove rimane fino al completamento del processo. Amazon EC2 eliminerà il file di configurazione da Parameter Store a meno che il processo non venga interrotto. Tenere presente che, se non viene selezionato un parametro aggiunto in precedenza all'istanza, tale parametro verrà rimosso dall'istanza al termine del processo.
6. Aggiorna la configurazione CloudWatch dell'agente: Amazon EC2 invia la configurazione delle metriche all'agente. CloudWatch Questo è l'ultimo passaggio del processo. Se il processo viene completato correttamente, le istanze possono emettere dati per i parametri selezionati e Amazon EC2 elimina il file di configurazione da Parameter Store.

Costi

I parametri aggiuntivi inseriti durante questo processo vengono fatturati come parametri personalizzati. Per ulteriori informazioni sui prezzi delle CloudWatch metriche, consulta Amazon Pricing. CloudWatch

Installa e configura l'agente CloudWatch

Puoi utilizzare la console Amazon EC2 per installare e configurare l' CloudWatch agente per aggiungere metriche aggiuntive.

> **Note**
>
> Ogni volta che esegui questa procedura, sovrascrivi la configurazione dell'agente esistente CloudWatch . Se non si seleziona un parametro scelto in precedenza, verrà rimosso dall'istanza.

Per installare e configurare l' CloudWatch agente utilizzando la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona le istanze su cui installare e configurare l' CloudWatch agente.
4. Scegli Azioni, Monitora e risolvi i problemi, Configura agente. CloudWatch
5. Per ogni fase della procedura, leggi il testo della console, quindi seleziona Avanti.
6. Per completare la procedura, seleziona Completa al passaggio finale.

Per aggiornare la configurazione dell'agente creata dalla console Amazon EC2

Puoi personalizzare manualmente la configurazione creata dalla console EC2. Per ulteriori informazioni, consulta Creare o modificare manualmente il file di configurazione CloudWatch dell'agente nella Amazon CloudWatch User Guide.

Statistiche relative alle CloudWatch metriche relative alle tue istanze

Puoi ottenere statistiche per le CloudWatch metriche relative alle tue istanze. Le statistiche sono aggregazioni di dati metrici in periodi di tempo specificati. CloudWatch fornisce statistiche basate

sui dati metrici forniti dai dati personalizzati dell'utente o forniti da altri servizi in ambito. AWS CloudWatch Le aggregazioni vengono effettuate usando il namespace, il nome parametro, le dimensioni e l'unità di misura del punto dati, entro un periodo di tempo specificato. Nella seguente tabella vengono descritte le statistiche disponibili.

Statistica	Descrizione
`Minimum`	Il valore più basso osservato durante il periodo specificato. Puoi utilizzare questo valore per determinare volumi di attività bassi per l'applicazione.
`Maximum`	Il valore più alto osservato durante il periodo specificato. Puoi utilizzare questo valore per determinare volumi di attività alti per l'applicazione.
`Sum`	Tutti i valori inviati per i parametri abbinati uniti insieme. Questa statistica può essere utile per determinare il volume totale di un parametro.
`Average`	Il valore `Sum`/`SampleCount` durante il periodo specificato. Confrontando questa statistica con `Minimum` e `Maximum`, puoi determinare l'ambito completo di un parametro e come l'uso della media sia vicino a `Minimum` e `Maximum`. Questo confronto consente di sapere quando aumentare o diminuire le risorsa in base alle esigenze.
`SampleCount`	Il conteggio (numero) dei punti dati utilizzato per il calcolo statistico.
`pNN.NN`	Il valore di uno specifico percentile. Puoi specificare qualsiasi percentile, utilizzando fino a due decimali (ad esempio, p95,45).

Indice

- Ottenere le statistiche su un'istanza specifica
- Aggregazione di statistiche tra istanze
- Aggregazione di statistiche per gruppo Auto Scaling
- Aggregazione di statistiche per AMI

Ottenere le statistiche su un'istanza specifica

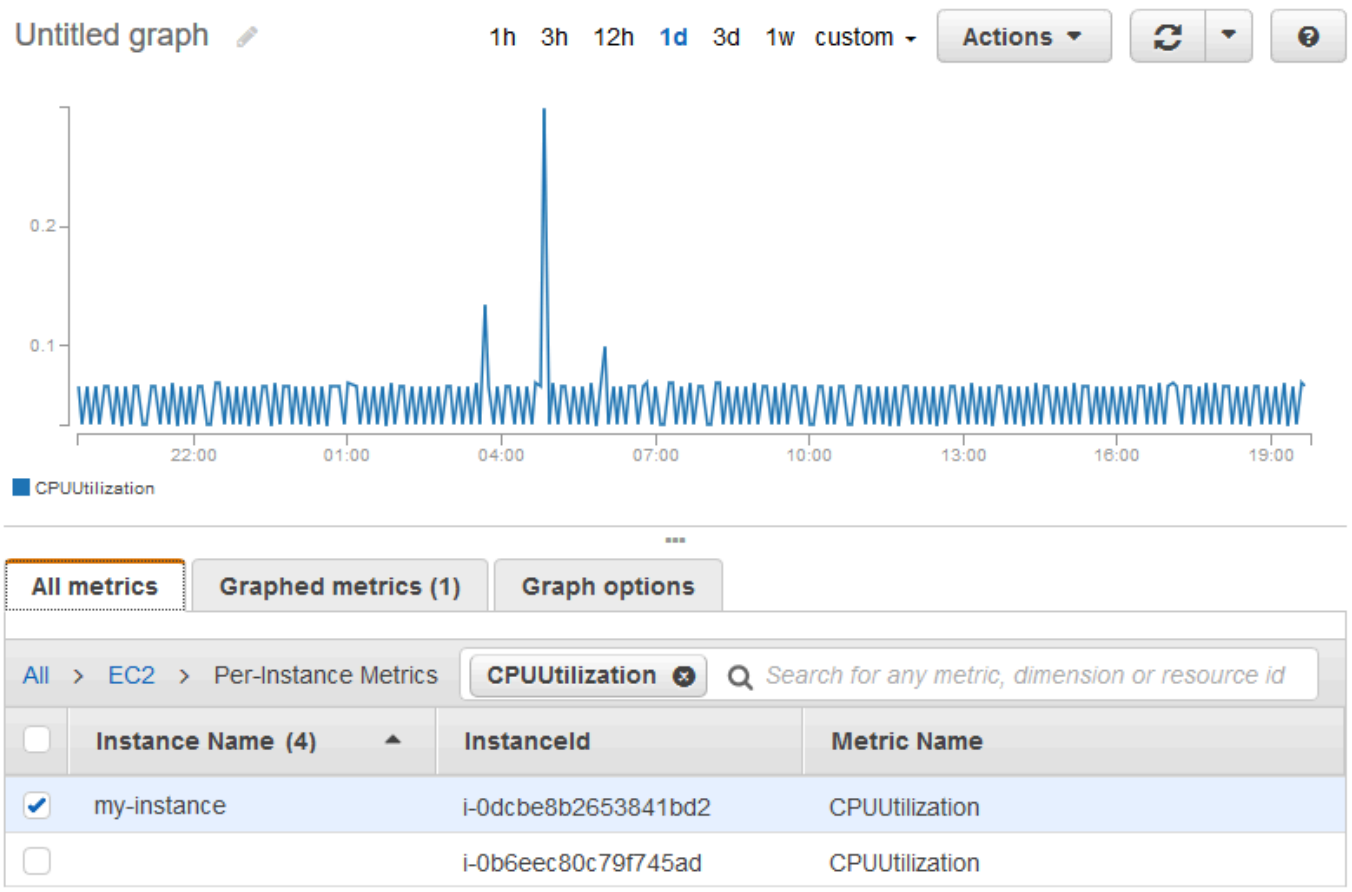
Puoi usare Console di gestione AWS o the AWS CLI per ottenere statistiche per un'istanza specifica. Gli esempi seguenti mostrano come utilizzare Console di gestione AWS o per AWS CLI determinare l'utilizzo massimo della CPU di una specifica istanza EC2.

Requisiti

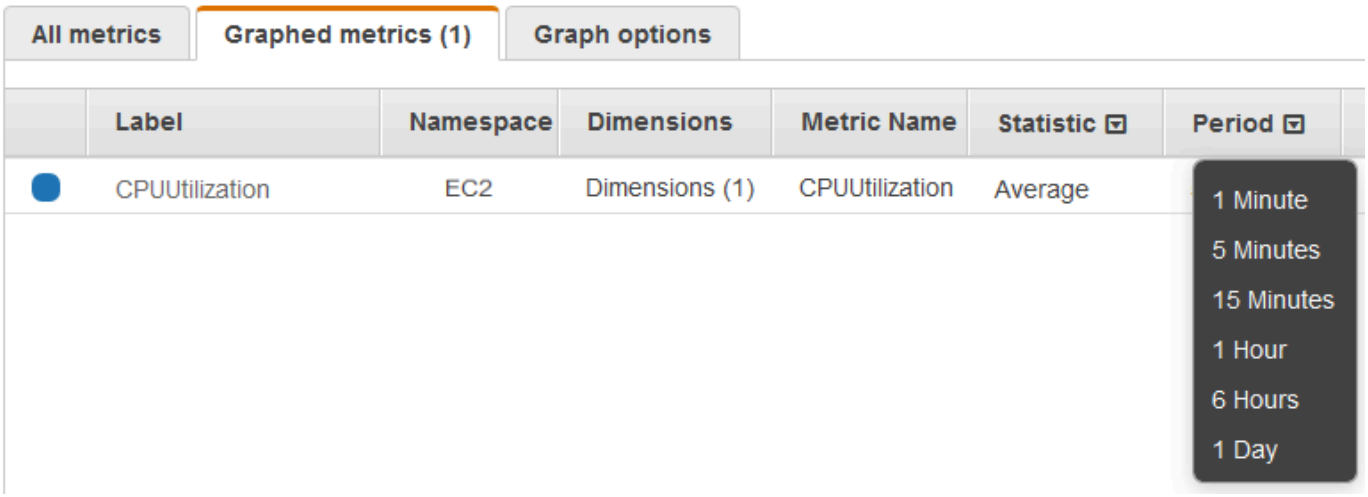
- Devi disporre dell'ID dell'istanza. Puoi ottenere l'ID dell'istanza tramite la Console di gestione AWS o il comando describe-instances.
- Per impostazione predefinita, il monitoraggio base è abilitato, ma puoi tuttavia abilitare il monitoraggio dettagliato. Per ulteriori informazioni, consulta Gestione del monitoraggio dettagliato per le istanze EC2.

Per visualizzare l'utilizzo della CPU di un'istanza specifica (console)

1. Apri la CloudWatch console all'indirizzo. https://console.aws.amazon.com/cloudwatch/
2. Nel riquadro di navigazione, seleziona Parametri.
3. Selezionare il parametro namespace EC2.
4. Scegli la dimensione Per-Instance Metriche.
5. Nel campo di ricerca digitare **`CPUUtilization`** e premere Invio. Selezionare la riga dell'istanza specifica, che mostra un grafico del parametro CPUUtilization dell'istanza. Per assegnare un nome al grafico, scegliere l'icona a forma di matita. Per modificare l'intervallo di tempo, selezionare uno dei valori predefiniti o scegliere custom (personalizzato).



6. Per modificare le statistiche o il periodo del parametro, scegliere la scheda Graphed metrics (Parametri nel grafico). Scegliere l'intestazione di colonna o un valore singolo, quindi scegliere un valore diverso.



Per ottenere l'utilizzo della CPU per un'istanza specifica (AWS CLI)

Utilizza il comando get-metric-statistics seguente per ottenere il parametro CPUUtilization per l'istanza specificata, utilizzando il periodo e l'intervallo di tempo specificati:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2022-10-18T23:18:00 --end-time 2022-10-19T23:18:00
```

Di seguito è riportato un output di esempio. Ogni valore rappresenta la percentuale di utilizzo massimo della CPU di una singola istanza EC2.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-19T00:18:00Z",
            "Maximum": 0.33000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T03:18:00Z",
            "Maximum": 99.670000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T07:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T12:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```

Aggregazione di statistiche tra istanze

Le statistiche aggregate sono disponibili per le istanze per le quali è stato abilitato il monitoraggio dettagliato. Le istanze che utilizzano il monitoraggio base non sono incluse nelle aggregazioni. Prima

di poter ottenere le statistiche aggregate per le istanze, devi abilitare il monitoraggio dettagliato (a un costo aggiuntivo), che fornisce i dati in periodi di 1 minuto.

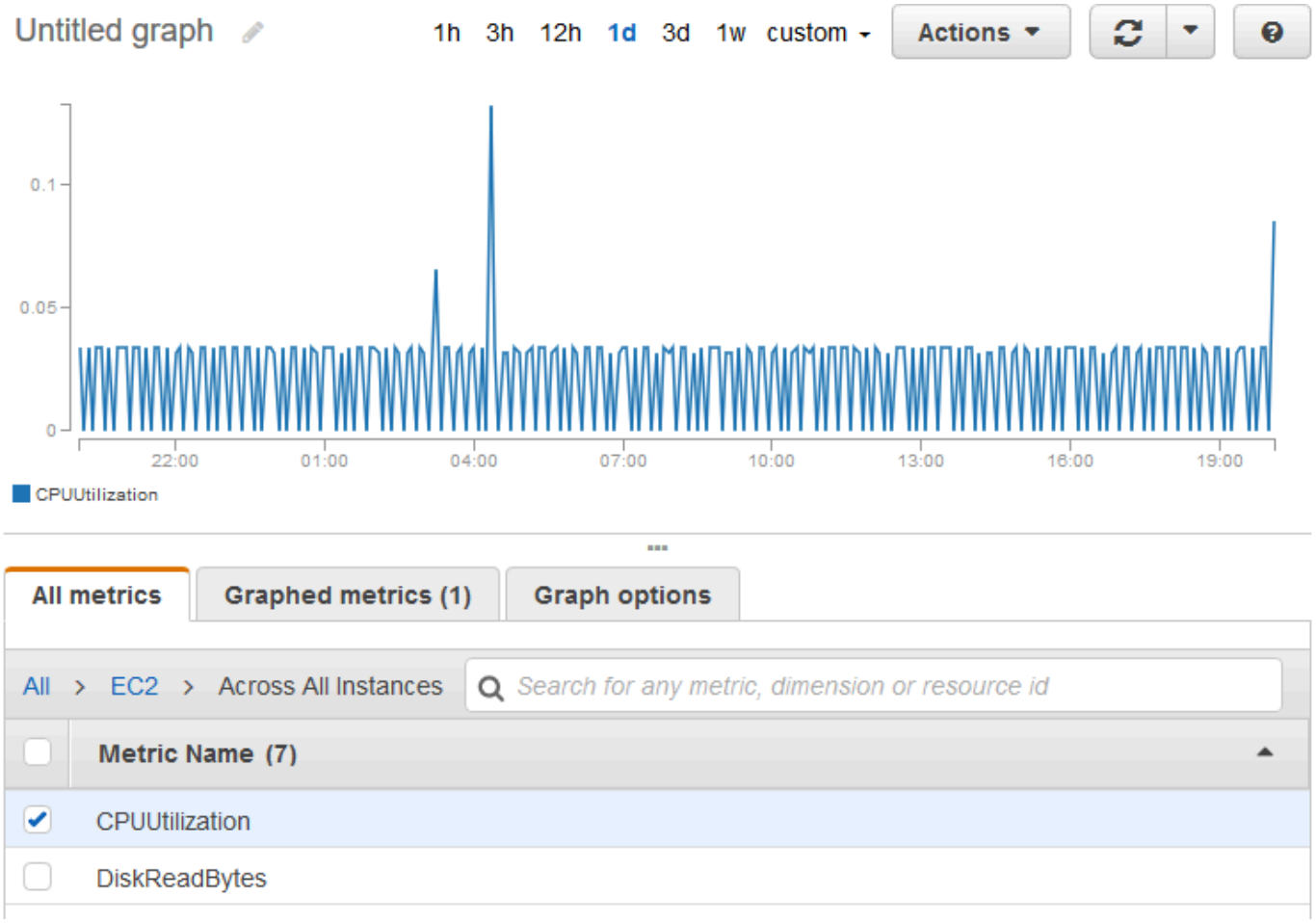
Tieni presente che Amazon CloudWatch non può aggregare i dati tra le regioni. AWS I parametri sono completamente indipendenti tra le regioni.

Questo esempio illustra come utilizzare il monitoraggio dettagliato per ottenere l'utilizzo medio della CPU delle istanze EC2. Poiché non è specificata alcuna dimensione, CloudWatch restituisce le statistiche per tutte le dimensioni nel `AWS/EC2` namespace.

> **Important**
>
> Questa tecnica per recuperare tutte le dimensioni in un AWS namespace non funziona per i namespace personalizzati pubblicati su Amazon. CloudWatch Con gli spazi dei nomi personalizzati, è necessario specificare il set completo delle dimensioni associate a un determinato punto dati per recuperare le statistiche comprendenti il punto dati.

Per visualizzare l'utilizzo medio della CPU nelle istanze (console)

1. Apri CloudWatch https://console.aws.amazon.com/cloudwatch/ la console all'indirizzo.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Selezionare il namespace EC2, quindi selezionare Across All Instances (Per tutte le istanze).
4. Selezionare la riga contenente CPUUtilization, che mostra un grafico del parametro per tutte le istanze EC2. Per assegnare un nome al grafico, scegliere l'icona a forma di matita. Per modificare l'intervallo di tempo, selezionare uno dei valori predefiniti o scegliere custom (personalizzato).



5. Per modificare le statistiche o il periodo del parametro, scegliere la scheda Graphed metrics (Parametri nel grafico). Scegliere l'intestazione di colonna o un valore singolo, quindi scegliere un valore diverso.

Per ottenere l'utilizzo medio della CPU tra le tue istanze (AWS CLI)

Utilizza il comando get-metric-statistics come riportato di seguito per ottenere la media del parametro CPUUtilization tra le istanze.

```
aws cloudwatch get-metric-statistics \
    --namespace AWS/EC2 \
    --metric-name CPUUtilization \
    --period 3600  --statistics "Average" "SampleCount" \
    --start-time 2022-10-11T23:18:00 \
    --end-time 2022-10-12T23:18:00
```

Di seguito è riportato un output di esempio:

```
{
    "Datapoints": [
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-12T07:18:00Z",
            "Average": 0.038235294117647062,
            "Unit": "Percent"
        },
        {
            "SampleCount": 240.0,
            "Timestamp": "2022-10-12T09:18:00Z",
            "Average": 0.16670833333333332,
            "Unit": "Percent"
        },
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-11T23:18:00Z",
            "Average": 0.041596638655462197,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```


Aggregazione di statistiche per gruppo Auto Scaling

Puoi aggregare le statistiche per le istanze EC2 in un gruppo di Auto Scaling. Tieni presente che Amazon CloudWatch non può aggregare i dati tra le regioni. AWS I parametri sono completamente indipendenti tra le regioni.

Questo esempio illustra come recuperare il numero totale di byte scritti sul disco per un gruppo di Auto Scaling. Il totale viene calcolato per periodi di 1 minuto per un intervallo di 24 ore all'interno di tutte le istanze EC2 nel gruppo Auto Scaling specificato.

Da visualizzare DiskWriteBytes per le istanze in un gruppo Auto Scaling (console)

1. Aprire la CloudWatch console all'indirizzo. https://console.aws.amazon.com/cloudwatch/
2. Nel riquadro di navigazione, seleziona Parametri.
3. Selezionare il namespace EC2, quindi selezionare By Auto Scaling Group (Per gruppo Auto Scaling).

4. Scegliete la riga per la DiskWriteBytes metrica e il gruppo Auto Scaling specifico, che visualizza un grafico della metrica per le istanze del gruppo Auto Scaling. Per assegnare un nome al grafico, scegliere l'icona a forma di matita. Per modificare l'intervallo di tempo, selezionare uno dei valori predefiniti o scegliere custom (personalizzato).
5. Per modificare le statistiche o il periodo del parametro, scegliere la scheda Graphed metrics (Parametri nel grafico). Scegliere l'intestazione di colonna o un valore singolo, quindi scegliere un valore diverso.

DiskWriteBytes Per visualizzare le istanze in un gruppo Auto Scaling (AWS CLI)

Utilizza il comando get-metric-statistics come riportato di seguito.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes
 --period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2022-10-16T23:18:00 --end-time 2022-10-18T23:18:00
```

Di seguito è riportato un output di esempio:

```
{
    "Datapoints": [
        {
            "SampleCount": 18.0,
            "Timestamp": "2022-10-19T21:36:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "SampleCount": 5.0,
            "Timestamp": "2022-10-19T21:42:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        }
    ],
    "Label": "DiskWriteBytes"
}
```

Aggregazione di statistiche per AMI

È possibile aggregare le statistiche in base all'AMI per le istanze per le quali è stato abilitato il monitoraggio dettagliato. Le istanze che utilizzano il monitoraggio base non sono incluse nelle aggregazioni. Prima di poter ottenere le statistiche aggregate per le istanze, devi abilitare il monitoraggio dettagliato (a un costo aggiuntivo), che fornisce i dati in periodi di 1 minuto.

Tieni presente che Amazon CloudWatch non può aggregare i dati tra le regioni. AWS I parametri sono completamente indipendenti tra le regioni.

Questo esempio illustra come determinare l'utilizzo medio della CPU per tutte le istanze che utilizzano un'Amazon Machine Image (AMI) specifica. La media supera intervalli di tempo di 60 secondi per un periodo di un giorno.

Per visualizzare l'utilizzo medio della CPU per AMI (console)

1. Apri la CloudWatch console all'indirizzo. https://console.aws.amazon.com/cloudwatch/
2. Nel riquadro di navigazione, seleziona Parametri.
3. Selezionare il namespace EC2, quindi selezionare By Image (AMI) Id (Per ID immagine (AMI)).
4. Selezionare la riga del parametro CPUUtilization e l'AMI specifica, che mostra un grafico del parametro per l'AMI specificata. Per assegnare un nome al grafico, scegliere l'icona a forma di matita. Per modificare l'intervallo di tempo, selezionare uno dei valori predefiniti o scegliere custom (personalizzato).
5. Per modificare le statistiche o il periodo del parametro, scegliere la scheda Graphed metrics (Parametri nel grafico). Scegliere l'intestazione di colonna o un valore singolo, quindi scegliere un valore diverso.

Per ottenere l'utilizzo medio della CPU per un ID di immagine (AWS CLI)

Utilizza il comando get-metric-statistics come riportato di seguito.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-
time 2022-10-10T00:00:00 --end-time 2022-10-11T00:00:00
```

Di seguito è riportato un output di esempio. Ogni valore rappresenta una percentuale di utilizzo medio della CPU per le istanze EC2 che eseguono l'AMI specificata.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-10T07:00:00Z",
            "Average": 0.041000000000000009,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T14:00:00Z",
            "Average": 0.079579831932773085,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T06:00:00Z",
            "Average": 0.036000000000000011,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```


Visualizzare i grafici di monitoraggio delle istanze

Dopo aver avviato un'istanza, puoi aprire la console Amazon EC2 e visualizzare i relativi grafici di monitoraggio per l'istanza nella scheda Monitoring (Monitoraggio). Ciascun grafico si basa su uno dei parametri di Amazon EC2 disponibili.

Sono disponibili i seguenti grafici:

- Utilizzo medio della CPU (percentuale)
- Letture medie del disco (byte)
- Scritture medie sul disco (byte)
- Rete massima in entrata (byte)
- Rete massima in uscita (byte)
- Operazioni di lettura del disco di riepilogo (numero)
- Operazioni di scrittura sul disco di riepilogo (numero)
- Stato riepilogo (qualsiasi)
- Istanza dello stato di riepilogo (numero)

- Sistema dello stato di riepilogo (numero)

Per ulteriori informazioni sui parametri e i relativi dati visualizzati nei grafici, consulta CloudWatch metriche disponibili per le tue istanze.

Rappresenta le metriche utilizzando la console CloudWatch

Puoi anche utilizzare la CloudWatch console per rappresentare graficamente i dati metrici generati da Amazon EC2 e altri servizi. AWS Per ulteriori informazioni, consulta la sezione Grafica delle metriche nella Amazon User Guide. CloudWatch

Crea un CloudWatch allarme per un'istanza

Puoi creare un CloudWatch allarme che monitora le CloudWatch metriche per una delle tue istanze. CloudWatchti invierà automaticamente una notifica quando la metrica raggiunge una soglia specificata. Puoi creare un CloudWatch allarme utilizzando la console Amazon EC2 o utilizzando le opzioni più avanzate fornite dalla CloudWatch console.

Per creare un allarme utilizzando la console CloudWatch

Per esempi, consulta Creazione di CloudWatch allarmi Amazon nella Amazon CloudWatch User Guide.

Per creare un allarme tramite la console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e scegli Azioni, Monitora e risolvi i problemi, Gestisci gli allarmi. CloudWatch
4. Nella pagina dei dettagli della gestione CloudWatch degli allarmi, in Aggiungi o modifica allarme, seleziona Crea un allarme.
5. Per Notifica di allarme, scegli se configurare le notifiche Amazon Simple Notification Service (Amazon SNS). Immettere un argomento Amazon SNS esistente o immettere un nome per creare un nuovo argomento.
6. Per Operazione per gli allarmi, scegli se specificare un'operazione da effettuare quando viene attivato l'allarme. Scegli un'operazione dall'elenco.

7. Per Alarm thresholds (Soglie di allarme=, selezionare il parametro e i criteri per l'allarme. Ad esempio, per creare un allarme che viene attivato quando l'utilizzo della CPU raggiunge l'80% per un periodo di 5 minuti, procedi come segue:

   a. Mantieni l'impostazione predefinita per Raggruppa esempi per (Media) e Tipo di dati da campionare (Utilizzo CPU).

   b. Scegli **>=** per Allarme quando, quindi immetti **`0.80`** per Percentuale.

   c. Inserisci **`1`** per Periodo consecutivo e seleziona 5 minuti per Periodo.

8. (Facoltativo) Per Sample metric data (Dati dei parametri di esempio), scegliere Add to dashboard (Aggiungi al pannello di controllo).

9. Scegli Create (Crea).

Puoi modificare le impostazioni CloudWatch degli allarmi dalla console Amazon EC2 o dalla CloudWatch console. Se desideri eliminare la sveglia, puoi farlo dalla CloudWatch console. Per ulteriori informazioni, consulta Modificare o eliminare un CloudWatch allarme nella Amazon CloudWatch User Guide.

Creazione di allarmi che arrestano, terminano, riavviano o recuperano un'istanza

Utilizzando Amazon CloudWatch alarm actions, puoi creare allarmi che interrompono, terminano, riavviano o ripristinano automaticamente le tue istanze. Puoi utilizzare le operazioni di arresto o termine per aiutarti a risparmiare denaro quando non necessiti più dell'esecuzione di un'istanza. Puoi utilizzare le operazioni di riavvio e recupero per riavviare automaticamente tali istanze o recuperarle in un nuovo hardware, se si verifica un danneggiamento del sistema.

> **Note**
>
> Per informazioni sulla fatturazione e sui prezzi di Amazon CloudWatch Alarms, consulta CloudWatch fatturazione e costi nella Guida per l'utente di Amazon. CloudWatch

Il ruolo `AWSServiceRoleForCloudWatchEvents` collegato al servizio consente di eseguire azioni di allarme AWS per tuo conto. La prima volta che crei un allarme nell'API IAM Console di gestione AWS AWS CLI, nella o nell'API IAM, CloudWatch crea automaticamente il ruolo collegato al servizio.

Esistono diversi scenari in cui potresti voler arrestare o terminare automaticamente l'istanza. Ad esempio, potresti disporre di istanze dedicate a processi di elaborazione della retribuzione in batch o ad attività di calcolo scientifico che vengono eseguite per un periodo di tempo, dopodiché completano il proprio lavoro. Anziché lasciare tali istanze inattive (accumulando addebiti), puoi arrestarle o terminarle, ciò ti consente di risparmiare denaro. La differenza principale tra l'uso delle operazioni di allarme di arresto o di termine consiste nel poter avviare comodamente un'istanza arrestata se è necessario eseguirla in un secondo momento, mantenendo gli stessi ID istanza e volume radice. Tuttavia, non puoi avviare un'istanza terminata. Al contrario, è necessario avviare una nuova istanza. Quando un'istanza viene arrestata o terminata, i dati nei volumi dell'archivio dell'istanza vengono persi.

Puoi aggiungere le azioni di arresto, terminazione, riavvio o ripristino a qualsiasi allarme impostato su una metrica Amazon EC2 per istanza, comprese le metriche di monitoraggio di base e dettagliate fornite da Amazon CloudWatch (nello spazio dei `AWS/EC2` nomi), nonché qualsiasi metrica personalizzata che includa la `InstanceId` dimensione, purché il suo valore si riferisca a un'istanza Amazon EC2 valida in esecuzione.

> **Important**
>
> Gli allarmi di verifica dello stato possono assumere temporaneamente lo stato `INSUFFICIENT_DATA` se vi sono punti dati dei parametri mancanti. Nonostante sia una circostanza rara, può verificarsi in caso di un'interruzione del sistema di report dei parametri, anche quando un'istanza è integra. Consigliamo di considerare lo stato `INSUFFICIENT_DATA` come avviso di dati mancanti e non come un utilizzo fuori limite segnalato dall'allarme, soprattutto durante la configurazione di un allarme che arresta, termina, riavvia o recupera un'istanza.

Supporto della console

Puoi creare allarmi utilizzando la console Amazon EC2 o la console. CloudWatch Le procedure in questa documentazione utilizzano la console Amazon EC2. Per le procedure che utilizzano la CloudWatch console, consulta Creazione di allarmi che interrompono, terminano, riavviano o ripristinano un'istanza nella Amazon User Guide. CloudWatch

Permissions

È necessario che tu disponga del `iam:CreateServiceLinkedRole` per creare o modificare un allarme che esegue le operazioni di allarme EC2. 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.

Indice

- Aggiungi azioni di arresto agli allarmi di Amazon CloudWatch
- Aggiungi azioni di interruzione agli allarmi Amazon CloudWatch
- Aggiungi azioni di riavvio agli allarmi Amazon CloudWatch
- Aggiungi azioni di ripristino agli CloudWatch allarmi Amazon
- Scenari CloudWatch di azione di allarme Amazon

Aggiungi azioni di arresto agli allarmi di Amazon CloudWatch

Puoi creare un allarme per arrestare un'istanza Amazon EC2 al raggiungimento di una determinata soglia. Ad esempio, potresti eseguire istanze di sviluppo o di test e occasionalmente dimenticare di disattivarle. Puoi creare un allarme che viene attivato quando la percentuale di utilizzo medio della CPU è inferiore al 10% per 24 ore, segnalando che la CPU è inattiva e non più in uso. Puoi regolare la soglia, la durata e il periodo di tempo in base alle tue esigenze. Puoi inoltre aggiungere una notifica Amazon Simple Notification Service (Amazon SNS) in modo da ricevere un'e-mail all'attivazione dell'allarme.

Le istanze che utilizzano un volume Amazon EBS come volume root possono essere arrestate o terminate, mentre le istanze che utilizzano l'archivio dell'istanza come volume root possono solo essere terminate. Quando l'istanza viene terminata o arrestata, i dati nei volumi dell'archivio dell'istanza vengono persi.

Per creare un allarme per arrestare un'istanza inattiva (console Amazon EC2)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e scegli Azioni, Monitora e risolvi i problemi, Gestisci gli allarmi. CloudWatch

   In alternativa, è possibile scegliere il segno più (

) nella colonna Alarm status (Stato allarme).

4. Nella pagina Gestisci CloudWatch allarmi, procedi come segue:

   a. Scegliere Create an alarm (Crea un allarme).

   b. Per ricevere un'e-mail quando viene attivato l'allarme, per Alarm notification (Notifica allarme), scegli un argomento Amazon SNS esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) messaging (Utilizzo di Amazon SNS per la messaggistica da applicazione a persona (A2P)) nella Guida per lo sviluppatore di Amazon Simple Notification Service.

   c. Attivare Alarm action (Azione Allarme)e scegliere Stop (Interrompi).

   d. Per Group samples by (Raggruppa campioni per) e Type of data to sample (Tipo di dati da campionare), scegliere una statistica e un parametro. In questo esempio, scegliere Average (Media) e CPU Utilization (Utilizzo CPU).

   e. Per Alarm When (Avvia allarme quando) e Percent (Percentuale), specificare la soglia del parametro. In questo esempio, specifica <= e 10%.

   f. Per Consecutive period (Periodo consecutivo) e Period (Periodo), specificare il periodo di valutazione per l'allarme. In questo esempio, specificare 1 periodo consecutivo di 5 minuti.

   g. Amazon crea CloudWatch automaticamente un nome di allarme per te. Per modificare il nome, immettere un nuovo nome in Alarm name (Nome allarme). I nomi degli allarmi devono contenere solo caratteri ASCII.

      > **Note**
      >
      > Puoi modificare la configurazione dell'allarme in base ai tuoi requisiti prima di creare l'allarme oppure puoi modificarlo in seguito. Questo include il parametro, la soglia, la durata, l'operazione e le impostazioni delle notifiche. Tuttavia, dopo aver creato l'allarme non è possibile modificarne il nome.

   h. Scegli Create (Crea).

Aggiungi azioni di interruzione agli allarmi Amazon CloudWatch

Puoi creare un allarme per terminare automaticamente un'istanza EC2 al raggiungimento di una determinata soglia, purché non sia abilitata la protezione da cessazione dell'istanza. Ad esempio, potresti voler terminare un'istanza una volta che ha completato il suo lavoro e non averne più bisogno. Se intendessi utilizzare l'istanza in un secondo momento, sarebbe necessario arrestare

l'istanza anziché terminarla. Quando un'istanza viene terminata, i dati nei volumi dell'archivio dell'istanza vengono persi. Per ulteriori informazioni sull'abilitazione e la disabilitazione della protezione da terminazione per un'istanza, consulta Modifica della protezione da terminazione dell'istanza.

Per creare un allarme per arrestare un'istanza inattiva (console Amazon EC2)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e scegli Azioni, Monitora e risolvi i problemi, Gestisci gli allarmi. CloudWatch

   In alternativa, è possibile scegliere il segno più (

) nella colonna Alarm status (Stato allarme).
4. Nella pagina Gestisci CloudWatch allarmi, procedi come segue:

   a. Scegliere Create an alarm (Crea un allarme).

   b. Per ricevere un'e-mail quando viene attivato l'allarme, per Alarm notification (Notifica allarme), scegli un argomento Amazon SNS esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) messaging (Utilizzo di Amazon SNS per la messaggistica da applicazione a persona (A2P)) nella Guida per lo sviluppatore di Amazon Simple Notification Service.

   c. Attivare Alarm action (Azione allarme)e scegliere Terminate (Termina).

   d. Per Group samples by (Raggruppa campioni per) e Type of data to sample (Tipo di dati da campionare), scegliere una statistica e un parametro. In questo esempio, scegliere Average (Media) e CPU Utilization (Utilizzo CPU).

   e. Per Alarm When (Avvia allarme quando) e Percent (Percentuale), specificare la soglia del parametro. In questo esempio, specificare => e 10 percento.

   f. Per Consecutive period (Periodo consecutivo) e Period (Periodo), specificare il periodo di valutazione per l'allarme. In questo esempio, specificare 24 periodi consecutivi di 1 ora.

   g. Amazon crea CloudWatch automaticamente un nome di allarme per te. Per modificare il nome, immettere un nuovo nome in Alarm name (Nome allarme). I nomi degli allarmi devono contenere solo caratteri ASCII.

> **Note**
>
> Puoi modificare la configurazione dell'allarme in base ai tuoi requisiti prima di creare l'allarme oppure puoi modificarlo in seguito. Questo include il parametro, la soglia, la durata, l'operazione e le impostazioni delle notifiche. Tuttavia, dopo aver creato l'allarme non è possibile modificarne il nome.

h. Scegli Create (Crea).

Aggiungi azioni di riavvio agli allarmi Amazon CloudWatch

Puoi creare un CloudWatch allarme Amazon che monitora un'istanza Amazon EC2 e riavvia automaticamente l'istanza. L'operazione di allarme di riavvio è consigliata per gli errori di controllo dello stato dell'istanza (contrariamente all'operazione di allarme di recupero, adatta agli errori di controllo dello stato del sistema). Il riavvio di un'istanza equivale al riavvio di un sistema operativo. Nella maggior parte dei casi, sono necessari pochi minuti per riavviare l'istanza. Quando riavvii un'istanza, questa rimane sullo stesso host fisico, in modo che l'istanza conservi il proprio nome DNS pubblico, indirizzo IP privato e tutti i dati presenti nei volumi instance store.

A differenza dell'arresto e riavvio, il reboot di un'istanza non comporta l'inizio di un nuovo periodo di fatturazione oraria dell'istanza (con un addebito minimo di un minuto). Quando l'istanza viene riavviata, i dati nei volumi dell'archivio dell'istanza vengono conservati. I volumi dell'archivio dell'istanza devono essere rimontati nel file system dopo il riavvio. Per ulteriori informazioni, consulta Riavvio di un'istanza Amazon EC2.

> **Important**
>
> Per evitare una race condition tra le operazioni di riavvio e di recupero, evita di impostare gli stessi periodi di valutazione per entrambi gli allarmi di riavvio e di recupero. È consigliabile impostare gli allarmi di riavvio su tre periodi di valutazione di un minuto ciascuno. Per ulteriori informazioni, consulta Evaluating an alarm nella Amazon CloudWatch User Guide.

Per creare un allarme per riavviare un'istanza (console Amazon EC2)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).

3. Seleziona l'istanza e scegli Azioni, Monitora e risolvi i problemi, Gestisci gli allarmi. CloudWatch

   In alternativa, è possibile scegliere il segno più (

) nella colonna Alarm status (Stato allarme).

4. Nella pagina Gestisci CloudWatch allarmi, procedi come segue:

   a. Scegliere Create an alarm (Crea un allarme).

   b. Per ricevere un'e-mail quando viene attivato l'allarme, per Alarm notification (Notifica allarme), scegli un argomento Amazon SNS esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) messaging (Utilizzo di Amazon SNS per la messaggistica da applicazione a persona (A2P)) nella Guida per lo sviluppatore di Amazon Simple Notification Service.

   c. Attivare Alarm action (Azione allarme)e scegliere Reboot (Riavvia).

   d. Per Group samples by (Raggruppa campioni per) e Type of data to sample (Tipo di dati da campionare), scegliere una statistica e un parametro. In questo esempio, scegliere Average (Media) e Status check failed: instance (Controllo stato fallito: istanza).

   e. Per Consecutive period (Periodo consecutivo) e Period (Periodo), specificare il periodo di valutazione per l'allarme. In questo esempio, inserire 3 periodi consecutivi di 1 minuto. Se 1 minuto è disabilitato, è necessario abilitare il monitoraggio dettagliato oppure scegliere 5 minuti.

   f. Amazon crea CloudWatch automaticamente un nome di allarme per te. Per modificare il nome, immettere un nuovo nome in Alarm name (Nome allarme). I nomi degli allarmi devono contenere solo caratteri ASCII.

   g. Scegli Create (Crea).

Aggiungi azioni di ripristino agli CloudWatch allarmi Amazon

Puoi creare un CloudWatch allarme Amazon che monitora un'istanza Amazon EC2. Se l'istanza viene danneggiata a causa di un guasto hardware sottostante o di un problema che richiede l' AWS intervento di riparazione, puoi ripristinarla automaticamente. Le istanze terminate non possono essere recuperate. Un'istanza recuperata è identica all'istanza originale, incluso l'ID istanza, gli indirizzi IP privati, gli indirizzi IP elastici e tutti i metadati dell'istanza.

CloudWatch impedisce di aggiungere un'azione di ripristino a un allarme presente su un'istanza che non supporta le azioni di ripristino.

Quando viene attivato l'allarme `StatusCheckFailed_System` e viene avviata l'operazione di ripristino, riceverai una notifica dall'argomento Amazon SNS selezionato al momento della creazione dell'allarme e dell'associazione dell'operazione di ripristino. Durante il recupero dell'istanza, l'istanza viene migrata durante un riavvio di istanza e tutti i dati in memoria andranno persi. Una volta completato il processo, l'informazione viene pubblicata nell'argomento SNS configurato per l'allarme. Tutti coloro che hanno eseguito la sottoscrizione a questo argomento SNS ricevono una notifica e-mail che include lo stato del tentativo di recupero ed eventuali ulteriori istruzioni. Si nota riavvio di istanza nell'istanza recuperata.

> **Note**
>
> L'operazione di recupero può essere utilizzata solo con `StatusCheckFailed_System`, non con `StatusCheckFailed_Instance`.

I problemi seguenti possono causare il mancato superamento delle verifiche dello stato del sistema:

- Perdita di connettività di rete
- Perdita di alimentazione elettrica del sistema
- Problemi di software sull'host fisico
- Problemi hardware sull'host fisico che incidono sulla raggiungibilità della rete

L'operazione di recupero è supportata solo sulle istanze che soddisfano alcune caratteristiche. Per ulteriori informazioni, consulta Ripristino automatico dell'istanza.

Se la tua istanza dispone di un indirizzo IP pubblico, manterrà lo stesso indirizzo IP pubblico dopo il recupero.

> **Important**
>
> Per evitare una race condition tra le operazioni di riavvio e di recupero, evita di impostare gli stessi periodi di valutazione per entrambi gli allarmi di riavvio e di recupero. È consigliabile impostare gli allarmi di recupero su due periodi di valutazione di un minuto ciascuno. Per ulteriori informazioni, consulta Evaluating an alarm nella Amazon CloudWatch User Guide.

Per creare un allarme per recuperare un'istanza (console Amazon EC2)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza e scegli Azioni, Monitora e risolvi i problemi, Gestisci gli allarmi. CloudWatch

   In alternativa, è possibile scegliere il segno più (

) nella colonna Alarm status (Stato allarme).
4. Nella pagina Gestisci CloudWatch allarmi, procedi come segue:

   a. Scegliere Create an alarm (Crea un allarme).

   b. Per ricevere un'e-mail quando viene attivato l'allarme, per Alarm notification (Notifica allarme), scegli un argomento Amazon SNS esistente. Per fare ciò, è necessario creare un argomento Amazon SNS utilizzando la console di Amazon SNS. Per ulteriori informazioni, consulta Using Amazon SNS for application-to-person (A2P) messaging (Utilizzo di Amazon SNS per la messaggistica da applicazione a persona (A2P)) nella Guida per lo sviluppatore di Amazon Simple Notification Service.

      > **Note**
      >
      > Gli utenti devono sottoscrivere l'argomento SNS specificato per ricevere messaggi e-mail di notifica quando vengono attivati gli allarmi. Riceve Utente root dell'account AWS sempre notifiche e-mail quando vengono eseguite azioni automatiche di ripristino dell'istanza, anche se non è specificato un argomento SNS o l'utente root non è iscritto all'argomento SNS specificato.

   c. Attivare Alarm action (Azione allarme)e scegliere Recover (Recupera).

   d. Per Group samples by (Raggruppa campioni per) e Type of data to sample (Tipo di dati da campionare), scegliere una statistica e un parametro. In questo esempio, scegliere Average (Media) e Status check failed: system (Controllo stato fallito: system).

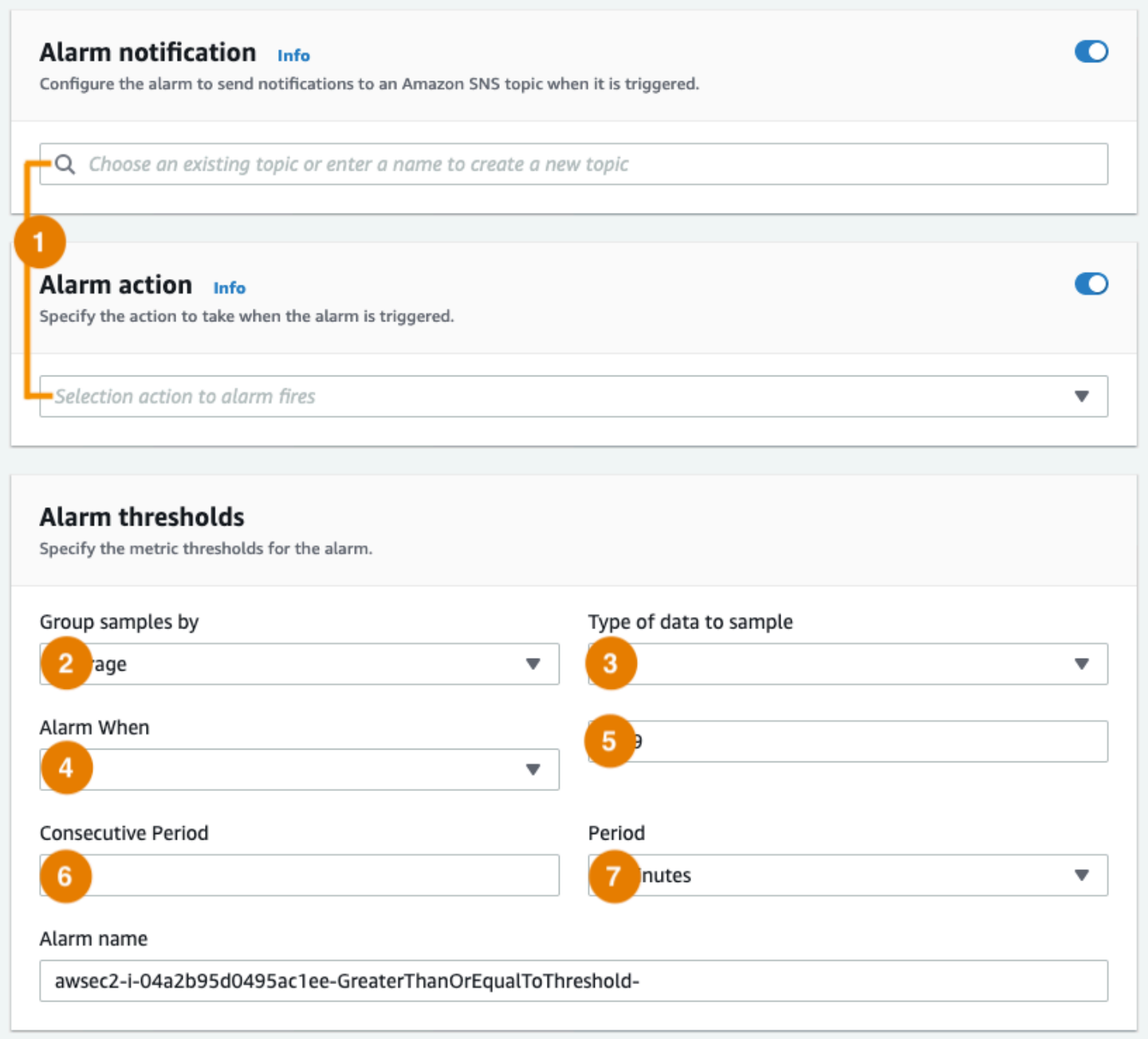
   e. Per Consecutive period (Periodo consecutivo) e Period (Periodo), specificare il periodo di valutazione per l'allarme. In questo esempio, inserire 2 periodi consecutivi di 1 minuto. Se 1 minuto è disabilitato, è necessario abilitare il monitoraggio dettagliato oppure scegliere 5 minuti.

f. Amazon crea CloudWatch automaticamente un nome di allarme per te. Per modificare il nome, immettere un nuovo nome in Alarm name (Nome allarme). I nomi degli allarmi devono contenere solo caratteri ASCII.

g. Scegli Create (Crea).

Scenari CloudWatch di azione di allarme Amazon

È possibile utilizzare la console Amazon EC2 per creare operazioni dell'allarme che arrestano, avviano o terminano un'istanza Amazon EC2, se vengono soddisfatte determinate condizioni. Nello screen capture seguente della pagina della console dove configuri le operazioni dell'allarme, abbiamo numerato le impostazioni. Abbiamo anche numerato le impostazioni nello scenario che segue, per aiutarti a creare le operazioni appropriate.



Scenario 1: arrestare lo sviluppo inattivo e testare le istanze

Creare un allarme che fermi un'istanza utilizzata nello sviluppo software o testare quando è stata inattiva per almeno un'ora.

Impostazione	Valore
1	Interrompi

Impostazione	Valore
2	Massimo
3	Utilizzo CPU
4	<=
5	10%
6	1
7	1 ora

Scenario 2: interrompere le istanze inattive

Creare un allarme che fermi un'istanza e invii un'e-mail quando l'istanza è stata inattiva per 24 ore.

Impostazione	Valore
1	Arresto ed e-mail
2	Media
3	Utilizzo CPU
4	<=
5	5%
6	24
7	1 ora

Scenario 3: inviare un'e-mail riguardo i server Web con traffico elevato insolito

Creare un allarme che invii un'e-mail quando un'istanza eccede i 10 GB di traffico di rete in uscita al giorno.

Impostazione	Valore
1	E-mail
2	Somma
3	Rete in uscita
4	>
5	10 GB
6	24
7	1 ora

Scenario 4: interrompere i server Web con traffico elevato insolito

Creare un allarme che fermi un'istanza e invii un messaggio di testo (SMS) se il traffico di rete in uscita al giorno eccede 1 GB all'ora.

Impostazione	Valore
1	Arresto e invio SMS
2	Somma
3	Rete in uscita
4	>
5	1 GB
6	1
7	1 ora

Scenario 5: interrompere un'istanza danneggiata

Creare un allarme che fermi un'istanza che per tre volte consecutive fallisce la verifica di stato (effettuata con intervalli di 5 minuti).

Impostazione	Valore
1	Interrompi
2	Media
3	Verifica stato non riuscita: sistema
4	-
5	-
6	1
7	15 minuti

Scenario 6: terminare le istanze quando i processi delle elaborazioni in batch sono completati

Creare un allarme che termini un'istanza che esegue processi batch quando non invia più dati di risultati.

Impostazione	Valore
1	Interruzione
2	Massimo
3	Rete in uscita
4	<=
5	100.000 byte
6	1

Impostazione	Valore
7	5 minuti

Automatizza Amazon utilizzando EC2 EventBridge

Puoi utilizzare Amazon EventBridge per automatizzare Servizi AWS e rispondere automaticamente agli eventi di sistema, come problemi di disponibilità delle applicazioni o modifiche delle risorse. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale. Puoi creare regole che indichino a quali eventi sei interessato e quali operazioni automatizzate eseguire quando un evento corrisponde a una regola. Le azioni che possono essere attivate automaticamente includono le seguenti:

- Invoca una funzione AWS Lambda
- Richiama il comando Amazon EC2 Run
- Inoltro dell'evento a flusso di dati Amazon Kinesis
- Attiva una macchina a AWS Step Functions stati
- Notifica di un argomento Amazon SNS
- Notifica di una coda Amazon SQS

Di seguito sono riportati alcuni esempi di utilizzo EventBridge con Amazon EC2:

- Attivazione di una funzione Lambda ogni volta che un'istanza entra in stato di esecuzione.
- Notifica di un argomento Amazon SNS quando un volume Amazon EBS viene creato o modificato.
- Invia un comando a una o più EC2 istanze Amazon utilizzando Amazon EC2 Run Command ogni volta che si verifica un determinato evento in un altro AWS servizio.

Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

Tipi di EC2 eventi Amazon

Amazon EC2 supporta i seguenti tipi di eventi:

- EC2 Cambio di stato AMI
- EC2 Avvio rapido, notifica di modifica dello stato

- EC2 Errore della flotta
- EC2 Informazioni sulla flotta
- EC2 Modifica della flotta di istanze
- EC2 Modifica della richiesta di istanza Fleet Spot
- EC2 Modifica dello stato della flotta
- EC2 Raccomandazione per il riequilibrio delle istanze
- EC2 Notifica di modifica dello stato dell'istanza
- EC2 Spot Fleet Error
- EC2 Informazioni sulla flotta Spot
- EC2 Modifica della flotta di istanze Spot
- EC2 Modifica della richiesta di istanza Spot Fleet Spot
- EC2 Modifica dello stato della flotta Spot
- EC2 Avviso di interruzione dell'istanza Spot
- EC2 Esecuzione delle richieste di istanze Spot
- EC2 Notifica di sottoutilizzo dell'ODCR

Per informazioni sui tipi di eventi supportati da Amazon EBS, consulta Amazon EventBridge for Amazon EBS.

Registra le chiamate API Amazon EC2 utilizzando AWS CloudTrail

L'API Amazon EC2 è integrata con AWS CloudTrail un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o un. Servizio AWS CloudTrail acquisisce tutte le chiamate API Amazon EC2 come eventi. Le chiamate acquisite includono chiamate effettuate dalla console. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata all'API Amazon EC2, l'indirizzo IP da cui è stata effettuata la richiesta e quando è stata effettuata.

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.

Eventi di gestione delle API di Amazon EC2 in CloudTrail

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse presenti nel tuo Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

Tutte le operazioni dell'API Amazon EC2 sono registrate come eventi di gestione. Per un elenco delle azioni API a cui si effettua l'accesso CloudTrail, consulta Amazon EC2 API Reference. Le chiamate alle operazioni RunInstances, DescribeInstances e StopInstances, per esempio, sono registrate come eventi di gestione.

Esempi di eventi dell'API Amazon EC2

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.

Il seguente record di file di log mostra che un utente ha terminato un'istanza.


```
{
   "Records":[
      {
         "eventVersion":"1.03",
         "userIdentity":{
            "type":"Root",
            "principalId":"123456789012",
            "arn":"arn:aws:iam::123456789012:root",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"user"
         },
         "eventTime":"2016-05-20T08:27:45Z",
         "eventSource":"ec2.amazonaws.com",
         "eventName":"TerminateInstances",
         "awsRegion":"us-west-2",
```

```
        "sourceIPAddress":"198.51.100.1",
        "userAgent":"aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
        "requestParameters":{
           "instancesSet":{
              "items":[{
                 "instanceId":"i-1a2b3c4d"
              }]
           }
        },
        "responseElements":{
           "instancesSet":{
              "items":[{
                 "instanceId":"i-1a2b3c4d",
                 "currentState":{
                    "code":32,
                    "name":"shutting-down"
                 },
                 "previousState":{
                    "code":16,
                    "name":"running"
                 }
              }]
           }
        },
        "requestID":"be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
        "eventID":"6e12345-2a4e-417c-aa78-7594fEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
     }
   ]
}
```


Per informazioni sui contenuti dei CloudTrail record, consulta i contenuti dei CloudTrail record nella Guida AWS CloudTrail per l'utente.

Connessioni di audit effettuate tramite EC2 Instance Connect

Puoi utilizzarlo AWS CloudTrail per controllare gli utenti che si connettono alle tue istanze utilizzando EC2 Instance Connect.

Per controllare l'attività SSH tramite EC2 Instance Connect utilizzando AWS CloudTrail console

1. Apri la CloudTrail console all'indirizzo. https://console.aws.amazon.com/cloudtrail/

2. Verificare di trovarsi nella regione appropriata.
3. Nel riquadro di navigazione scegliere Event history (Cronologia eventi).
4. Per Filtro, scegliere Event source (Origine evento), ec2-instance-connect.amazonaws.com.
5. (Facoltativo) Per Time range (Intervallo temporale), selezionare un intervallo di tempo.
6. Scegliere l'icona Refresh events (Aggiorna eventi).
7. La pagina visualizza gli eventi che corrispondono alle chiamate API SendSSHPublicKey. Espandi un evento utilizzando la freccia per visualizzare dettagli aggiuntivi, come il nome utente e la chiave di AWS accesso utilizzati per effettuare la connessione SSH e l'indirizzo IP di origine.
8. Per visualizzare informazioni complete sull'evento in formato JSON, scegliere View event (Visualizza evento). Il campo requestParameters contiene l'ID istanza di destinazione, il nome utente del sistema operativo e la chiave pubblica utilizzata per stabilire la connessione SSH.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-09-21T21:37:58Z"}
        }
    },
    "eventTime": "2018-09-21T21:38:00Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "SendSSHPublicKey ",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceId": "i-0123456789EXAMPLE",
        "osUser": "ec2-user",
        "SSHKey": {
            "publicKey": "ssh-rsa ABCDEFGHIJKLMNO01234567890EXAMPLE"
        }
     },
```

```
    "responseElements": null,
    "requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",
    "eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",
    "eventType": "AwsApiCall",
    "recipientAccountId": "0987654321"
}
```

Se hai configurato il tuo AWS account per raccogliere CloudTrail eventi in un bucket S3, puoi scaricare e controllare le informazioni a livello di programmazione. Per ulteriori informazioni, consulta Ottenere e visualizzare i file di CloudTrail registro nella Guida per l'utente. AWS CloudTrail

Monitora le applicazioni.NET e SQL Server utilizzando Application Insights CloudWatch

CloudWatch Application Insights ti aiuta a monitorare le tue applicazioni.NET e SQL Server che utilizzano istanze Amazon EC2 insieme ad altre risorse AWS applicative. Identifica e configura i log delle metriche chiave e gli allarmi tra risorse dell'applicazione e stack tecnologico (ad esempio, il database di Microsoft SQL server, i server web (IIS) e di applicazione, il sistema operativo, i bilanciatori del carico e le code). Controlla in modo continuo i parametri e i log per rilevare e correlare anomalie ed errori. Quando sono rilevati errori e anomalie, Application Insights genera eventi che puoi utilizzare per impostare notifiche o eseguire operazioni. Per assistere nella risoluzione dei problemi, crea pannelli di controllo automatizzati per i problemi rilevati, che includono anomalie parametri ed errori di log correlati, insieme ad altri approfondimenti per il indirizzare verso la causa principale potenziale. I pannelli di controllo automatizzati consentono di eseguire operazioni di correzione rapide per mantenere le applicazioni integre e prevenire l'impatto sugli utenti finali dell'applicazione.

Informazioni fornite sui problemi rilevati

- Un breve riepilogo del problema
- L'ora e la data di inizio del problema
- La gravità del problema: High/Medium/Low
- Lo stato del problema rilevato: In- progress/Resolved
- Approfondimenti: approfondimenti generati automaticamente sul problema rilevato e la possibile causa principale

- Feedback sugli approfondimenti: feedback fornito sull'utilità degli approfondimenti generati da CloudWatch Application Insights for .NET e SQL Server
- Osservazioni correlate: una vista dettagliata delle anomalie parametro e frammenti di errore di log pertinenti correlati al problema su vari componenti dell'applicazione

Feedback

Puoi fornire feedback sugli approfondimenti generati automaticamente sui problemi rilevati designandoli come utili o non utili. Il feedback sugli approfondimenti, insieme alla diagnostica dell'applicazione (anomalie parametri ed eccezioni di log), viene utilizzato per migliorare il rilevamento futuro di problemi simili.

Per ulteriori informazioni, consulta la documentazione di CloudWatch Application Insights nella Amazon CloudWatch User Guide.

Monitorare l'utilizzo del piano gratuito per Amazon EC2

Quando crei il tuo Account AWS, puoi iniziare a usare Amazon EC2 gratuitamente utilizzando il piano AWS gratuito. I vantaggi del piano gratuito variano a seconda che tu abbia creato l'account prima del 15 luglio 2025 oppure il 15 luglio 2025 o successivamente. Per ulteriori informazioni, consulta Explore AWS services with AWS Free Tier nella Guida per l'AWS Billing utente.

Vantaggi del piano gratuito prima e dopo il 15 luglio 2025

La tabella seguente confronta i vantaggi del piano gratuito in base alla data di creazione Account AWS :

Vantaggio del piano gratuito	Account creato prima del 15 luglio 2025	Account creato il 15 luglio 2025 o successivamente
Tipi di istanze contrassegnati come idonei al piano gratuito	`t2.micro`, `t3.micro`	`t3.micro`, `t3.small`, `t4g.micro` , `t4g.small` , `c7i-flex.large` , `m7i-flex.large`
Tipi di volume Amazon EBS contrassegnati come idonei al piano gratuito	`standard`, `st1`, `sc1`, `gp2`, e `gp3`	`standard`, `st1`, `sc1`, `gp2`, e `gp3`

Vantaggio del piano gratuito	Account creato prima del 15 luglio 2025	Account creato il 15 luglio 2025 o successivamente
AMI contrassegnate come idonea al piano gratuito.	Controlla AMI contrassegnate come idonea al piano gratuito.	Controlla AMI contrassegnate come idonea al piano gratuito.
Limite di utilizzo	Limitato ai limiti di utilizzo, dopo la fine dei quali ti sono fatturate le tariffe con pagamento in base al consumo.	Ricevi 100 USD di credito di iscrizione e guadagna fino a 100 USD in crediti aggiuntivi.
Durata del piano gratuito	Il piano gratuito dura 12 mesi dalla data di creazione dell'account. Durante questo periodo, se superi i limiti di utilizzo del piano gratuito, ti saranno fatturate le tariffe con pagamento in base al consumo.	Il piano gratuito dura 6 mesi a partire dalla data di creazione dell'account o dal momento in cui i crediti sono esauriti, a seconda dell'evento che si verifica per primo. Non puoi superare i limiti del piano gratuito.

Per elencare i tipi di istanze idonei al piano gratuito

Utilizza il comando describe-instance-types con il filtro `free-tier-eligible`.

```
aws ec2 describe-instance-types \
    --filters Name=free-tier-eligible,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Per elencare le AMI idonee al piano gratuito

Utilizza il comando describe-images con il filtro `free-tier-eligible`.

```
aws ec2 describe-images \
    --filters Name=free-tier-eligible,Values=true \
    --query "Images[*].[ImageId]" \
    --output text | sort
```

Tracciamento dell'utilizzo del piano gratuito per gli account creati prima del 15 luglio 2025

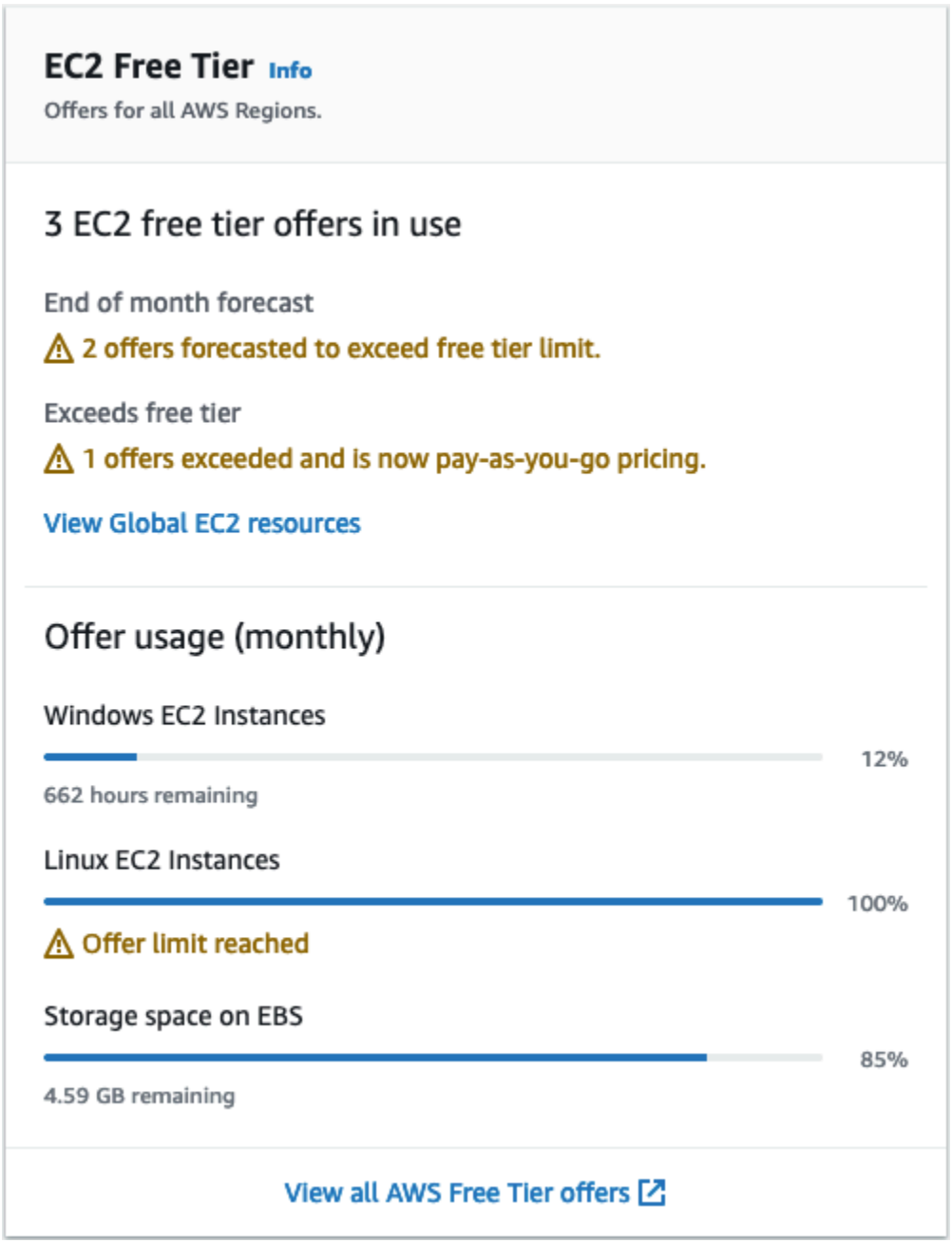
> **Note**
>
> Questa sezione si applica solo agli utenti del livello gratuito che hanno creato Account AWS prima del 15 luglio 2025. Se hai creato il tuo account il 15 luglio 2025 o dopo tale data, consulta Monitoraggio dell'utilizzo del piano AWS gratuito nella Guida per l' AWS Billing utente.

Se hai creato il tuo account prima del 15 luglio 2025, puoi utilizzare Amazon EC2 senza incorrere in addebiti se sei AWS cliente da meno di 12 mesi e rimani entro i limiti di utilizzo. Piano gratuito di AWS È importante tenere traccia dell'utilizzo del piano gratuito per evitare sorprese di fatturazione. Se superi i limiti del piano gratuito, dovrai sostenere addebiti standard con pagamento in base al consumo. Per ulteriori informazioni, consulta Piano gratuito di AWS.

> **Note**
>
> Se sei AWS cliente da più di 12 mesi, non sei più idoneo all'utilizzo del piano gratuito e non vedrai la casella EC2 Free Tier descritta nella procedura seguente.

Monitoraggio dell'utilizzo del piano gratuito

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere EC2 Dashboard (Pannello di controllo EC2).
3. Individua la casella del piano gratuito EC2 (in alto a destra).



4. Nella casella del piano gratuito EC2, controlla l'utilizzo del piano gratuito, come segue:

   - Nella sezione Offerte del piano gratuito EC2 in uso, prendi nota dei seguenti avvisi:
     - Previsione di fine mese: ti avvisa che, se continui con il modello di utilizzo attuale, questo mese verranno addebitati degli importi.
     - Supera il piano gratuito: ti avvisa che hai superato i limiti del livello gratuito e che stai già incorrendo in addebiti.

- Nella sezione Utilizzo dell'offerta (mensile), prendi nota dell'utilizzo delle istanze Linux, delle istanze Windows e dello spazio di archiviazione EBS. La percentuale indica quanti limiti del piano gratuito hai utilizzato questo mese. Se hai raggiunto il 100%, ti verranno addebitati dei costi per un ulteriore utilizzo.

> **Note**
>
> Queste informazioni vengono visualizzate solo dopo aver creato un'istanza. Tuttavia, le informazioni sull'utilizzo non vengono aggiornate in tempo reale; ma sono aggiornate tre volte al giorno.

5. Per evitare di incorrere in ulteriori spese, elimina tutte le risorse che stanno attualmente incorrendo in addebiti o che potrebbero essere addebitate se superi il limite di utilizzo del piano gratuito.

   - Per istruzioni sull'eliminazione dell'istanza, consultare Terminare le istanze Amazon EC2.
   - Per verificare se disponi di risorse in altre regioni che potrebbero essere soggette a costi, nella casella Piano gratuito EC2, scegli Visualizza risorse EC2 globali per aprire Vista globale EC2. Per ulteriori informazioni, consulta Visualizza le risorse tra le regioni utilizzando AWS Global View.

6. Per visualizzare l'utilizzo delle risorse per tutti Piano gratuito di AWS, nella parte inferiore del Servizi AWS riquadro EC2 Free Tier, scegli Visualizza tutte le Piano gratuito di AWS offerte. Per ulteriori informazioni, consulta Provare i servizi utilizzando il Piano gratuito di AWS nella Guida per l'utente di Fatturazione AWS .

Comprendi i codici di Amazon EC2 nei report di fatturazione e utilizzo

Quando usi Amazon EC2, includiamo i codici correlati nei report di AWS fatturazione e utilizzo. La revisione di questi codici ti aiuta a comprendere i costi e i modelli di utilizzo di Amazon EC2. Il monitoraggio e la gestione delle spese sono essenziali per ottimizzare i costi.

Le tabelle seguenti descrivono i codici per Amazon EC2 visualizzati nei report di fatturazione e utilizzo. Per un elenco dei codici regionali usati nei report di fatturazione e di utilizzo, consulta AWS Region billing codes.

Codici di fatturazione per:

- Istanze
- Istanze Bare Metal
- Host dedicati
- Istanze dedicate
- Ottimizzazione EBS
- Prenotazioni della capacità

Risorse correlate

- the section called "Opzioni di fatturazione e acquisto"
- the section called "Comprendere la fatturazione AMI"
- EC2 Prezzi Amazon

Istanze

Codice	Description	unità
region-BoxUsage :*instance-type*	Il tempo di esecuzione per le istanze on demand.	Ore
region-HostBoxUsage :*instance-type*	Il tempo di esecuzione per le istanze su host dedicati.	Ore
region-SpotUsage :*instance-type*	Il tempo di esecuzione per le istanze spot.	Ore

Istanze Bare Metal

Codice	Description	unità
region-BoxUsage : *instance-family* .metal	Il tempo di esecuzione per le istanze on demand bare metal.	Ore
region-HostBoxUsage : .metallo *instance-family*	Il tempo di esecuzione per le istanze bare metal su host dedicati.	Ore
region-SpotUsage : .metallo *instance-family*	La durata di esecuzione per le istanze spot bare metal.	Ore

Host dedicati

Codice	Description	unità
region-HostUsage :*host-type*	L'ora in cui avviene il provisioning degli host dedicati.	Ore
region-ReservedHostUsage :*host-type*	L'ora in cui vengono applicate le prenotazioni di host dedicati.	Ore

Istanze dedicate

Codice	Description	unità
region-DedicatedUsage :*instance-type*	Il tempo di esecuzione per le istanze dedicate.	Ore + tariffa per regione

Ottimizzazione EBS

Codice	Description	unità
region-EBSOptimized :*instance-type*	L'ora in cui l'ottimizzazione EBS viene abilitata.	Ore

Prenotazioni della capacità

Codice	Description	unità
region-Reservation :*instance-type*	Il tempo riservato dell'istanza per la prenotazione della capacità.	Ore
region-UnusedBox :*instance-type*	Il tempo dell'istanza inutilizzato riservato per la prenotazione della capacità.	Ore
region-DedicatedRes :*instance-type*	Il tempo riservato dell'istanza per la prenotazione della capacità dedicata.	Ore
region-UnusedDed :*instance-type*	Il tempo dell'istanza riservato inutilizzato per la prenotazione della capacità dedicata.	Ore

Creazione di un inventario delle istanze EC2

Amazon EC2 fornisce capacità di calcolo dimensionabili e on demand. Un'istanza EC2 è un server virtuale che viene eseguito nella AWS rete.

La tabella seguente descrive le caratteristiche principali di un'istanza EC2. Un amministratore di sistema può utilizzare le indicazioni fornite in questa guida per ottenere informazioni su queste

caratteristiche e utilizzarle per configurare server funzionalmente equivalenti eseguiti on-premises o nella rete di un altro provider di servizi cloud.

Caratteristica	Description
Posizione geografica	Amazon EC2 è ospitato in tutte le AWS regioni del mondo. Scegli le posizioni per le tue istanze vicine ai clienti. Puoi avviare istanze in più posizioni.
Specifiche hardware	Amazon EC2 fornisce un'ampia selezione di tipi di istanza, ottimizzati per diversi casi d'uso. I tipi di istanza selezionati determinano le relative risorse di calcolo, memoria, rete e archiviaz ione.
Immagini	Un'Amazon Machine Image (AMI) include il software da installare sull'istanza al momento dell'avvio. Ciò include il sistema operativo, i pacchetti software e le configurazioni personali zzate.
Indirizzi IP e nomi host DNS	Le istanze ricevono indirizzi IP privati e un nome host DNS privato. Se configuri un indirizzo IP pubblico per un'istanza, quest'ult ima riceve anche un nome host DNS pubblico.
Regole del gruppo di sicurezza	Le regole del gruppo di sicurezza associate alle istanze determinano il traffico in entrata e in uscita consentito.
Dati utente	I dati degli utenti vengono resi disponibili alle istanze al momento dell'avvio. È costituito da script di shell (Linux) o PowerShell script (Windows).

Posizione geografica

Amazon EC2 è disponibile in tutte AWS le regioni del mondo. Ciascuna regione è un'area geografica distinta. Puoi ridurre la latenza di rete selezionando per i tuoi server le Regioni vicine alla maggior parte degli utenti.

Puoi utilizzare Amazon EC2 Global View per elencare le tue istanze Amazon EC2 in tutte le Regioni. Con l'API Console di gestione AWS e, devi elencare le istanze per ciascuna regione singolarmente.

Perché è importante

Dopo aver determinato la posizione delle istanze, puoi decidere se implementare server funzionalmente equivalenti nelle stesse posizioni o in luoghi diversi, a seconda delle tue esigenze.

Per ottenere un riepilogo delle istanze EC2 in tutte le Regioni

1. Apri la console Amazon EC2 Global View all'indirizzo. https://console.aws.amazon.com/ec2globalview/home
2. Nella scheda Esplora regioni, in Riepilogo, controlla il numero di risorse in Istanze, che include il numero di istanze e il numero di Regioni. Scegli il testo sottolineato per vedere come viene distribuito il numero di istanze tra le regioni.
3. Nella scheda Ricerca globale, seleziona il filtro client Tipo di risorsa = Istanza. Puoi filtrare ulteriormente i risultati specificando una Regione o un tag.

Per ottenere il numero di istanze EC2 in una regione utilizzando AWS CLI

Utilizza il comando describe-instances seguente per descrivere le istanze della Regione specificata. Devi eseguire questo comando in ogni Regione in cui sono disponibili istanze.

```
aws ec2 describe-instances \
    --region us-east-2 \
    --query "length(Reservations[*].Instances[])"
```

Di seguito è riportato un output di esempio.

```
27
```

Per ottenere un elenco degli ID delle istanze anziché il numero di istanze, utilizza invece il seguente parametro `--query`.

```
--query "Reservations[*].Instances[].InstanceId"
```

Specifiche dell'hardware

Il tipo di istanza specificato per un'istanza EC2 determina le risorse di calcolo, memoria, archiviazione e rete disponibili. Ogni famiglia di istanza mette a disposizione diverse risorse di calcolo, memoria, rete e archiviazione. Per maggiori informazioni, consulta la Guida ai tipi di istanza Amazon EC2.

Perché sono importanti

Dopo aver determinato le specifiche hardware per le istanze, puoi decidere le specifiche minime richieste per server funzionalmente equivalenti.

Per ottenere un riepilogo dei tipi di istanze utilizzati dalle istanze

Utilizza il seguente comando describe-instances. Il comando sed rimuove le righe con parentesi e le righe vuote. Devi eseguire questo comando in ogni Regione in cui sono disponibili istanze.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].InstanceType" | sed 's/[][]//g;/^$/d' | sort |
 uniq -c | sort -nr
```

Di seguito è riportato un output di esempio.

```
  20    "c6i.4xlarge",
   5    "t2.micro",
   2    "g6e.2xlarge",
```

Per ottenere informazioni su tipi di istanza specifiche.

Per descrivere i tipi di istanza, utilizza il seguente comando describe-instance-types. Il parametro `--query` include solo i campi specificati nell'output. Queste sono le caratteristiche di base. Puoi includere tutti i campi aggiuntivi di cui hai bisogno oppure consulta Amazon EC2 instance type specifications nella Guida ai tipi di istanze di Amazon EC2.

```
aws ec2 describe-instance-types \
    --instance-types c6i.4xlarge t2.micro g6e.2xlarge \
    --query "InstanceTypes[*].
[InstanceType,VCpuInfo.DefaultVCpus,MemoryInfo.SizeInMiB,NetworkInfo.NetworkPerformance]"
 \
```

```
    --output table
```

Di seguito è riportato un output di esempio. Le colonne sono tipo di istanza, vCPU, memoria (GiB) e larghezza di banda della rete (Gbps).

```
-----------------------------------------------------
|               DescribeInstanceTypes               |
+--------------+-----+--------+----------------------+
|  t2.micro    |  1  |  1024  |  Low to Moderate     |
|  c6i.4xlarge |  16 |  32768 |  Up to 12.5 Gigabit  |
|  g6e.2xlarge |  8  |  65536 |  Up to 20 Gigabit    |
+--------------+-----+--------+----------------------+
```

Immagini

Un'Amazon Machine Image (AMI) fornisce il software installato sull'istanza al momento dell'avvio, come il sistema operativo, i servizi, gli strumenti di sviluppo e le applicazioni. Puoi esportare un'AMI in altri formati per utilizzarla con altri server.

Perché sono importanti

Dopo aver determinato le AMI per le tue istanze, puoi pianificare le immagini necessarie per server funzionalmente equivalenti. Potrebbe essere possibile esportare le AMI in un formato utilizzabile altrove. In alternativa, potresti dover connetterti a un'istanza avviata da ogni AMI, confermare cosa è installato e come è configurato e assicurarti di avere una copia di tutto ciò di cui hai bisogno.

Per ottenere le AMI per le tue istanze

Utilizza il seguente comando describe-instances. Il comando sed rimuove le righe con parentesi e le righe vuote. Devi eseguire questo comando in ogni Regione in cui sono disponibili istanze.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].ImageId" | sed 's/[][]//g;/^$/d' | sort | uniq
 -c | sort -nr
```

Di seguito è riportato un output di esempio.

```
20     "ami-0a70b9d193ae8a79",
 5     "ami-07d9cf938edb0739b",
```

```
 2     "ami-09245d5773578a1d6",
```

Per ottenere le informazioni su un'AMI specifica

Utilizza il seguente comando describe-images. Il parametro `--query` include solo i campi specificati nell'output. Puoi includere tutti i campi aggiuntivi di cui hai bisogno.

```
aws ec2 describe-images \
    --image-id ami-0a70b9d193ae8a79 ami-07d9cf938edb0739b ami-09245d5773578a1d6 \
    --query "Images[*].
{ID:ImageId,CreateDate:CreationDate,Name:Name,Description:Description}"
```

Di seguito è riportato un output di esempio.

```
[
    {
        "ID": "ami-0a70b9d193ae8a799",
        "CreateDate": "2025-03-01T02:22:41.000Z",
        "Name": "web-server-3.1",
        "Description": "Image for web servers"
    },
    {
        "ID": "ami-07d9cf938edb0739b",
        "CreateDate": "2025-02-01T23:59:03.000Z",
        "Name": "awesome-application-11.5",
        "Description": "Image for Awesome Application"
    },
    {
        "ID": "ami-09245d5773578a1d6",
        "CreateDate": "2025-01-31T02:22:41.000Z",
        "Name": "monitoring-4.2",
        "Description": "Monitoring software"
    }
]
```

Per creare un file VM da un'AMI

Utilizza il comando export-image. I formati di immagine supportati sono VHD (compatibile con Citrix Xen e Microsoft Hyper-V), VMDK (compatibile con VMware ESX e VMware vSphere) e formato raw (compatibile con hypervisor KVM e Xen). Per informazioni sui requisiti Import/Export e Import/Export le limitazioni della macchina virtuale, consulta Requisiti delle macchine virtuali.

Indirizzi IP e nomi host DNS

I tuoi utenti si connettono alle tue istanze EC2 tramite internet utilizzando i loro nomi host DNS pubblici. Il nome host DNS pubblico di un'istanza EC2 viene risolto nel suo indirizzo IP pubblico. Le istanze EC2 possono comunicare tra loro tramite l'indirizzo IP privato.

Perché sono importanti

Gli indirizzi IP consentono ai dispositivi di comunicare tra loro su una rete locale o su internet. Annotando gli indirizzi IP e i nomi DNS delle istanze, puoi contribuire a garantire che server funzionalmente equivalenti possano comunicare con gli stessi client o dispositivi delle tue istanze. Ad esempio, puoi aggiornare la configurazione del bilanciatore del carico o i record DNS che hai creato per il tuo provider DNS.

Per ottenere gli indirizzi IP e i nomi host DNS per le tue istanze

Utilizza il seguente comando describe-instances. Devi eseguire questo comando in ogni Regione in cui sono disponibili istanze. Il parametro `--query` include solo i campi specificati nell'output. Puoi includere tutti i campi aggiuntivi di cui hai bisogno.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].[InstanceId,PrivateIpAddress,PublicDnsName]" \
    --output table
```

Di seguito è riportato un output di esempio. Le colonne sono ID istanza, Indirizzo IPv4 privato e Nome DNS IPv4 pubblico.

```
----------------------------------------------------------------------------------
|                                DescribeInstances
 |
+---------------------+------------+-------------------------------------------------
+
| i-0bac57d7472c89bac | 10.0.2.139 | ec2-192-0-2-142.us-east-2.compute.amazonaws.com
 |
| i-0fa8b7678975a3fff | 10.0.14.85 | ec2-198-51-100-56.us-east-2.compute.amazonaws.com
 |
  ...
  ...
| i-08fd74f3f1595fdbd | 10.0.1.241 | ec2-203.0.113.13.us-east-2.compute.amazonaws.com
 |
```

```
+--------------------+-----------+-------------------------------------------------
+
```

Regole del gruppo di sicurezza

Un gruppo di sicurezza funziona da firewall virtuale. Dopo aver associato un gruppo di sicurezza a un'istanza EC2, le sue regole consentono il traffico in entrata e in uscita per l'istanza EC2 su porte e protocolli specifici.

Perché sono importanti

Dopo aver determinato il traffico in entrata che può raggiungere il server e il traffico in uscita a cui è consentito uscire dal server, puoi pianificare le regole del firewall necessarie per server funzionalmente equivalenti.

Per ottenere i gruppi di sicurezza per l'istanza

Utilizza il seguente comando describe-instances. Il comando sed rimuove le righe con parentesi e le righe vuote. Devi eseguire questo comando in ogni Regione in cui sono disponibili istanze.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].SecurityGroups[].GroupId" | sed 's/[][]//g;/^
$/d' | sort | uniq -c | sort -nr
```

Di seguito è riportato un output di esempio.

```
27     "sg-01dd3383691d02f42",
10     "sg-08c77cc910c0b3b2c",
 2     "sg-00f4e409629f1a42d",
```

Per aggiungere regole in entrata al gruppo di sicurezza

Utilizza il seguente comando describe-security-group-rules per visualizzare le regole per il gruppo di sicurezza specificato in cui `IsEgress` è `false`.

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-01dd3383691d02f42 \
    --query 'SecurityGroupRules[?IsEgress==`false`]'
```

Di seguito è riportato un output di esempio. La prima regola è quella in entrata predefinita, che consente il traffico in entrata da tutte le risorse assegnate a questo gruppo di sicurezza. L'altra regola

consente il traffico SSH dagli indirizzi IP nell'elenco di prefissi specificato. Per descrivere gli intervalli CIDR in un elenco di prefissi, utilizza il comando describe-prefix-lists.

```
[
    {
        "SecurityGroupRuleId": "sgr-06c8b42574a91db1b",
        "GroupId": "sg-01dd3383691d02f42",
        "GroupOwnerId": "123456789012",
        "IsEgress": false,
        "IpProtocol": "-1",
        "FromPort": -1,
        "ToPort": -1,
        "ReferencedGroupInfo": {
            "GroupId": "sg-01dd3383691d02f42",
            "UserId": "123456789012"
        },
        "Tags": [],
        "SecurityGroupRuleArn": "arn:aws:ec2:us-west-2:123456789012:security-group-
rule/sgr-06c8b42574a91db1b"
    },
    {
        "SecurityGroupRuleId": "sgr-0886a5d46afcd1758",
        "GroupId": "sg-01dd3383691d02f42",
        "GroupOwnerId": "123456789012",
        "IsEgress": false,
        "IpProtocol": "tcp",
        "FromPort": 22,
        "ToPort": 22,
        "PrefixListId": "pl-f8a6439125e7bf465",
        "Tags": [],
        "SecurityGroupRuleArn": "arn:aws:ec2:us-east-2:123456789012:security-group-
rule/sgr-0886a5d46afcd1758"
    }
]
```

Per ottenere le regole in uscita per un gruppo di sicurezza

Utilizza il seguente comando describe-security-group-rules per visualizzare le regole per il gruppo di sicurezza specificato in cui `IsEgress` è `true`.

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-01dd3383691d02f42 \
```

```
    --query 'SecurityGroupRules[?IsEgress==`true`]'
```

Di seguito è riportato un output di esempio. Contiene solo la regola in uscita predefinita, che consente tutto il traffico IPv4 in uscita.

```
[
    {
        "SecurityGroupRuleId": "sgr-048f09a719247dce7",
        "GroupId": "sg-01dd3383691d02f42",
        "GroupOwnerId": "123456789012",
        "IsEgress": true,
        "IpProtocol": "-1",
        "FromPort": -1,
        "ToPort": -1,
        "CidrIpv4": "0.0.0.0/0",
        "Tags": [],
        "SecurityGroupRuleArn": "arn:aws:ec2:us-east-2:123456789012:security-group-
rule/sgr-048f09a719247dce7"
    }
]
```

Dati utente

Quando avvii un'istanza EC2, puoi passare uno script di shell all'istanza utilizzando i dati utente. Tieni presente che i dati utente sono codificati in Base64, quindi devi decodificarli per leggere lo script.

Perché è importante

Se esegui comandi all'avvio come parte della configurazione delle istanze, potresti dover eseguire le stesse attività quando configuri server funzionalmente equivalenti.

Per visualizzare i dati utente decodificati per un'istanza

Utilizza il seguente comando describe-instance-attribute. Il comando base64 decodifica i dati utente.

```
aws ec2 describe-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --attribute userData \
    --output text \
    --query "UserData.Value" | base64 --decode
```

Di seguito è riportato un output di esempio.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Risorse correlate

Le seguenti sono caratteristiche aggiuntive delle istanze EC2:

- Coppie di chiavi
- Storage
- Tag

Puoi verificare se stai utilizzando le seguenti impostazioni per avviare istanze EC2 o distribuire il traffico tra le tue istanze EC2:

- Gruppi Auto Scaling
- Parco istanze EC2
- Elastic Load Balancing

Risoluzione dei problemi relativi alle istanze Amazon EC2

Le procedure e i suggerimenti riportati di seguito possono aiutare a risolvere problemi associati alle istanze Amazon EC2.

Problemi

- Risoluzione dei problemi di avvio dell'istanza Amazon EC2
- Risoluzione dei problemi di arresto dell'istanza Amazon EC2
- Risoluzione dei problemi relativi alla terminazione dell'istanza Amazon EC2
- Risoluzione di problemi relativi a un'istanza Amazon EC2 irraggiungibile
- Risoluzione dei problemi di connessione all'istanza Linux di Amazon EC2
- Risoluzione dei problemi relativi alle istanze Amazon EC2 Linux con esito negativo delle verifiche dello stato
- Risoluzione dei problemi relativi all'avvio di un'istanza Amazon EC2 Linux dal volume sbagliato
- Risoluzione dei problemi di connessione all'istanza Windows di Amazon EC2
- Risolvi i problemi relativi all'avvio delle istanze Windows di Amazon EC2
- Risolvi i problemi relativi alle istanze Windows di Amazon EC2
- Debug del kernel per le istanze di Windows sulla rete
- Reimpostazione della password dell'amministratore Windows per un'istanza Amazon EC2 Windows
- Risoluzione dei problemi di Sysprep relativi alle istanze Amazon EC2 Windows
- Risoluzione dei problemi relativi all'istanza Amazon EC2 Linux danneggiata utilizzando EC2Rescue
- Risoluzione dei problemi relativi all'istanza Amazon EC2 Windows danneggiata utilizzando EC2Rescue
- Console seriale EC2 per istanze
- Inviare un'interruzione della diagnostica per eseguire il debug di un'istanza Amazon EC2 non raggiungibile

Risoluzione dei problemi di avvio dell'istanza Amazon EC2

I suggerimenti riportati di seguito possono aiutarti a risolvere i problemi durante l'avvio di un'istanza di Amazon EC2.

Problemi di avvio

- Nome del dispositivo non valido
- Superamento del limite di istanze
- Capacità insufficiente dell'istanza
- La configurazione richiesta attualmente non è supportata. Controlla la documentazione per verificare le configurazioni supportate.
- Terminazione immediata dell'istanza
- Autorizzazioni insufficienti
- Utilizzo elevato della CPU poco dopo l'avvio di Windows (solo istanze Windows)
- L'avvio di un' IMDSv1-enabled istanza non riesce

Nome del dispositivo non valido

Description

Viene restituito l'errore `Invalid device name` *`device_name`* quando si tenta di avviare una nuova istanza.

Causa

La visualizzazione di questo errore durante l'avvio di un'istanza indica che il nome del dispositivo specificato per uno o più volumi nella richiesta ha un nome del dispositivo non valido. Tra le cause possibili sono incluse:

- Il nome del dispositivo potrebbe essere utilizzato dall'AMI selezionata.
- Il nome del dispositivo potrebbe essere riservato ai volumi root.
- Il nome del dispositivo potrebbe essere utilizzato per un altro volume nella richiesta.
- Il nome del dispositivo potrebbe non essere valido per il sistema operativo.

Soluzione

Per risolvere il problema:

- Verifica che il nome del dispositivo non sia utilizzato nell'AMI selezionata. Esegui il comando seguente per visualizzare i nomi dei dispositivi utilizzati dall'AMI.

```
aws ec2 describe-images --image-id ami-0abcdef1234567890 --query
 'Images[*].BlockDeviceMappings[].DeviceName'
```

- Evita di utilizzare un nome di dispositivo riservato ai volumi root. Per ulteriori informazioni, consulta Nomi dei dispositivi disponibili.
- Verifica che ogni volume specificato nella richiesta disponga di un nome di dispositivo univoco.
- Verifica che i nomi dei dispositivi specificati siano nel formato corretto. Per ulteriori informazioni, consulta Nomi dei dispositivi disponibili.

Superamento del limite di istanze

Description

Viene restituito l'errore `InstanceLimitExceeded` quando si tenta di avviare una nuova istanza o di riavviare un'istanza interrotta.

Causa

Se viene restituito un errore `InstanceLimitExceeded` mentre si tenta di avviare una nuova istanza o di riavviare un'istanza interrotta, significa che è stato raggiunto il numero massimo di istanze che si possono avviare in una regione. Quando crei il tuo AWS account, impostiamo dei limiti predefiniti sul numero di istanze che puoi eseguire per regione.

Soluzione

È possibile richiedere un aumento del limite di istanze in base alle singole regioni. Per ulteriori informazioni, consulta Service Quotas di Amazon EC2.

Capacità insufficiente dell'istanza

Description

Viene restituito l'errore `InsufficientInstanceCapacity` quando si tenta di avviare una nuova istanza o di riavviare un'istanza interrotta.

Causa

Se ricevi questo errore quando provi ad avviare un'istanza o a riavviare un'istanza interrotta, AWS significa che al momento non ha abbastanza On-Demand capacità disponibile per soddisfare la tua richiesta.

Soluzione

Per risolvere il problema, prova a eseguire queste operazioni:

- Attendere alcuni minuti, quindi inviare di nuovo la richiesta; la capacità può cambiare di frequente.
- Inviare una nuova richiesta con un numero ridotto di istanze. Ad esempio, se si effettua un'unica richiesta di avvio di 15 istanze, tentare creando 3 richieste per 5 istanze oppure 15 richieste per 1 istanza.
- Se si sta avviando un'istanza, inviare una nuova richiesta senza specificare alcuna zona di disponibilità.
- Se si sta avviando un'istanza, inviare una nuova richiesta utilizzando un tipo di istanza diverso (che è possibile ridimensionare in un secondo momento). Per ulteriori informazioni, consulta Modifiche del tipo di istanza Amazon EC2.
- Se si stanno avviando delle istanze in un gruppo di collocazione cluster, si potrebbe ricevere un errore di capacità insufficiente.

La configurazione richiesta attualmente non è supportata. Controlla la documentazione per verificare le configurazioni supportate.

Description

Viene visualizzato l'errore `Unsupported` quando si tenta di avviare una nuova istanza perché la configurazione dell'istanza non è supportata.

Causa

Il messaggio di errore fornisce ulteriori dettagli. Ad esempio, un tipo di istanza o un'opzione di acquisto di istanza potrebbe non essere supportata nell'area o nella zona di disponibilità specificata.

Soluzione

Prova con una configurazione di istanza diversa. Per cercare un tipo di istanza che soddisfi i requisiti, consulta Individuazione di un tipo di istanza Amazon EC2.

Terminazione immediata dell'istanza

Description

La tua istanza passa dallo stato `pending` allo stato `terminated`.

Causa

Di seguito sono riportati alcuni motivi per cui un'istanza potrebbe terminare immediatamente:

- Hai superato i limiti di volume EBS. Per ulteriori informazioni, consulta Limiti di volume di Amazon EBS per le istanze Amazon EC2.
- Una snapshot EBS è danneggiata.
- Il volume EBS root è crittografato e non disponi delle autorizzazioni per accedere alla Chiave KMS per la decrittografia.
- Uno snapshot specificato nel mapping del dispositivo a blocchi per l'AMI è crittografato e non si dispone delle autorizzazioni per accedere alla Chiave KMS per la decrittografia o non si dispone dell'accesso alla Chiave KMS per crittografare i volumi ripristinati.
- Nell'Amazon S3-backed AMI che hai utilizzato per avviare l'istanza manca una parte obbligatoria (un file image.part). file xx).

Per ulteriori informazioni, ottenere il motivo della cessazione utilizzando uno dei seguenti metodi.

Per recuperare il motivo della terminazione tramite console Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza.
3. Nella prima scheda, individuare il motivo accanto a State transition reason (Motivo transizione stato).

Per ottenere il motivo del recesso utilizzando il AWS CLI

1. Utilizzare il comando describe-instances e specificare l'ID istanza.

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

2. Analizzare la risposta JSON restituita dal comando e annotare i valori nell'elemento della risposta `StateReason`.

   Il seguente blocco di codice mostra un esempio di un elemento di risposta `StateReason`.

```
"StateReason": {
  "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",
  "Code": "Server.InternalError"
},
```

Per ottenere il motivo della cessazione, utilizzare AWS CloudTrail

Per ulteriori informazioni, vedere Visualizzazione degli eventi con la cronologia degli CloudTrail eventi nella Guida per l'AWS CloudTrail utente.

Soluzione

Eseguire una delle seguenti operazioni, a seconda del motivo della terminazione:

- **`Client.VolumeLimitExceeded: Volume limit exceeded`** — Eliminare i volumi inutilizzati. È possibile inviare una richiesta per aumentare il limite di volume.
- **`Client.InternalError: Client error on launch`**— Assicurati di disporre delle autorizzazioni necessarie per accedere ai volumi AWS KMS keys utilizzati per decrittografare e crittografare. Per ulteriori informazioni, consulta Utilizzo delle policy delle chiavi in AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .

Autorizzazioni insufficienti

Description

Viene restituito l'errore `"errorMessage": "You are not authorized to perform this operation."` quando provi ad avviare una nuova istanza e l'avvio fallisce.

Causa

Se ricevi questo errore quando provi ad avviare un'istanza, non disponi delle autorizzazioni IAM necessarie per farlo.

Alcune delle possibili autorizzazioni mancanti sono le seguenti:

- `ec2:RunInstances`
- `iam:PassRole`

Potrebbero inoltre essere richieste altre autorizzazioni. Per l'elenco delle autorizzazioni necessarie per avviare un'istanza, consulta le policy IAM di esempio nelle pagine Esempio: utilizzo della procedura guidata per l'avvio dell'istanza EC2 e Istanze di avvio () RunInstances.

Soluzione

Per risolvere il problema:

- Se stai effettuando richieste come utente IAM, verifica di disporre delle autorizzazioni seguenti:
  - `ec2:RunInstances` con una risorsa jolly ("*")
  - `iam:PassRole` con la risorsa corrispondente all'ARN del ruolo (ad esempio, `arn:aws:iam::999999999999:role/ExampleRoleName`)
- Se non disponi delle autorizzazioni precedenti, modifica la policy IAM associata al ruolo o all'utente IAM per aggiungere le autorizzazioni richieste mancanti.

Se il problema persiste e continui a ricevere un errore di avvio non riuscito, puoi decodificare il messaggio di errore di autorizzazione incluso nell'errore. Il messaggio decodificato include le autorizzazioni che mancano nella policy IAM. Per ulteriori informazioni, vedi Come posso decodificare un messaggio di errore di autorizzazione dopo aver ricevuto un errore "UnauthorizedOperation" durante l'avvio di un'istanza EC2?

Utilizzo elevato della CPU poco dopo l'avvio di Windows (solo istanze Windows)

> **Note**
>
> Questo suggerimento per la risoluzione dei problemi è valido solo per le istanze Windows.

Se Windows Update viene impostato su Check for updates but let me choose whether to download and install them (Ricerca aggiornamenti ma permettimi di scegliere se scaricarli e installarli) (impostazione predefinita dell'istanza), questo controllo può richiedere l'utilizzo di una percentuale compresa tra il 50 e il 99% della CPU nell'istanza. Se questo utilizzo della CPU implica problemi per le applicazioni, puoi modificare manualmente le impostazioni di Windows Update in Control Panel (Pannello di controllo) o utilizzare lo script seguente nel campo dei dati dell'utente di Amazon EC2:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v
 AUOptions /t REG_DWORD /d 3 /f net stop wuauserv net start wuauserv
```

Quando esegui questo script, specifica un valore per /d. Il valore predefinito è 3. I valori possibili sono:

1. Non ricercare mai aggiornamenti
2. Ricerca aggiornamenti ma permettimi di scegliere se scaricarli e installarli
3. Scarica aggiornamenti ma permettimi di scegliere se installarli
4. Installa gli aggiornamenti automaticamente

Dopo avere modificato i dati utente, puoi eseguire l'istanza. Per ulteriori informazioni, consulta Esecuzione di comandi sull'istanza Windows all'avvio.

L'avvio di un' IMDSv1-enabled istanza non riesce

Description

Viene visualizzata un'`Unsupported0peration`eccezione con il seguente messaggio:

```
You can't launch instances with IMDSv1 because httpTokensEnforced
is enabled for this account. Either launch the instance with
httpTokens=required or contact your account owner to disable
httpTokensEnforced using the ModifyInstanceMetadataDefaults API or the
account settings in the EC2 console.
```

Causa

Questo errore viene generato quando si tenta di avviare una nuova istanza abilitata a IMDSv1 (`httpTokens = optional`) in un account in cui le impostazioni dell'account EC2 o una politica

dichiarativa AWS dell'Organizzazione impongono l'uso di IMDSv2 (). `httpTokensEnforced = enabled`

Soluzione

Se sei pronto a usare solo IMDSv2, avvia l'istanza con IMDSv1 disabilitato (). `httpTokens = required` Per verificare se sei pronto, consulta. Passaggio all'utilizzo di Servizio di metadati dell'istanza Versione 2

Se hai ancora bisogno del supporto IMDSv1 su istanze nuove o esistenti, dovrai disabilitare l'applicazione di IMDSv2 per l'account nella regione. Per disabilitare l'imposizione di IMDSv2, imposta su. `HttpTokensEnforced disabled` Per ulteriori informazioni, consulta Amazon ModifyInstanceMetadataDefaults EC2 API Reference. Se preferisci configurare questa impostazione utilizzando la console, consultaApplica IMDSv2 a livello di account.

Risoluzione dei problemi di arresto dell'istanza Amazon EC2

Se la tua EBS-backed istanza Amazon appare bloccata nello `stopping` stato, il problema potrebbe riguardare il computer host sottostante.

Per risolvere il problema, eseguire queste fasi:

1. Forzare l'arresto dell'istanza

   Usa la console Amazon EC2 o la AWS CLI per forzare l'arresto dell'istanza. Per la procedura, consultare Arresto forzato di un'istanza.

   L'istanza tenterà innanzitutto un arresto regolare, che include lo svuotamento delle cache e dei metadati del file system (sebbene possa evitare opzionalmente l'arresto regolare). Se l'arresto regolare non viene completato entro il periodo di timeout, l'istanza si chiude forzatamente senza svuotare le cache e i metadati del file system.
2. Dopo l'arresto forzato

   Eseguire le procedure di verifica e riparazione del file system.

   > **Important**
   >
   > L'esecuzione di queste procedure è fondamentale perché un arresto forzato impedisce lo svuotamento delle cache e dei metadati del file system.

3. Se l'arresto forzato fallisce

   Se dopo 10 minuti l'istanza non si è arrestata, effettuare le seguenti operazioni:

   a. Pubblicare una richiesta di assistenza su AWS re:Post. Per velocizzare la risoluzione, includere l'ID dell'istanza e descrivere le fasi già eseguite.

   b. In alternativa, se si dispone di un piano di supporto, creare un caso di supporto tecnico presso il Centro di supporto.

   c. In attesa dell'assistenza, se necessario, è possibile creare un'istanza sostitutiva. Per la procedura, consultare (Facoltativo) Creare un'istanza sostitutiva.

Non viene addebitato alcun costo per l'utilizzo dell'istanza se questa non si trova nello stato `stopping` o in qualsiasi altro stato, tranne `running`. I costi per l'utilizzo dell'istanza vengono addebitati solo quando un'istanza è nello stato `running`.

Indice

- Arresto forzato di un'istanza
- (Facoltativo) Creare un'istanza sostitutiva

Arresto forzato di un'istanza

Puoi forzare l'arresto di un'istanza. Se dopo 10 minuti l'istanza non si è arrestata, pubblica una richiesta di assistenza su AWS re:Post. Per velocizzare la risoluzione, includere l'ID dell'istanza e descrivere le fasi già eseguite. In alternativa, se si dispone di un piano di supporto, creare un caso di supporto tecnico presso il Centro di supporto.

> **Note**
>
> Utilizzando la console, puoi forzare un'istanza ad arrestarsi, mentre l'istanza è solo nello stato `stopping`. Utilizzando AWS CLI, puoi forzare un'istanza ad arrestarsi, mentre l'istanza è nello stato `pending`, `running` o `stopping`.

Console

Per arrestare forzatamente un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza bloccata.
3. Scegli Stato istanza, Forza arresto istanza.

   Nota che Force stop instance (Forza arresto istanza) è disponibile solo nella console se l'istanza è nello stato `stopping`. Se la tua istanza si trova in un altro stato (eccetto `shutting-down` `eterminated`), puoi utilizzare l'opzione AWS CLI per forzare l'arresto dell'istanza.
4. (Facoltativo) Per ignorare lo spegnimento controllato del sistema operativo durante l'arresto forzato, seleziona la casella di controllo Ignora l'arresto del sistema operativo.
5. Scegli Arresto forzato.

AWS CLI

Per arrestare forzatamente un'istanza

Utilizza il comando stop-instances con l'opzione `--force`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --force
```

Per ignorare il regolare spegnimento del sistema operativo durante l'arresto forzato, includi l'opzione `--skip-os-shutdown`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --force \
    --skip-os-shutdown
```

PowerShell

Per arrestare forzatamente un'istanza

Usa il Stop-EC2Instance cmdlet e imposta su`-Enforce`. `true`

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true
```

Per ignorare il regolare spegnimento del sistema operativo durante l'arresto forzato, includi `-SkipOsShutdown $true`.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true `
    -SkipOsShutdown $true
```

(Facoltativo) Creare un'istanza sostitutiva

In attesa dell'assistenza da AWS re:Post o dal Centro di supporto, è possibile creare un'istanza sostitutiva. Crea un AMI dall'istanza bloccata e avvia una nuova istanza utilizzando la nuova AMI.

> **Important**
>
> È possibile creare un'istanza sostitutiva se l'istanza bloccata produce solo controlli dello stato del sistema, poiché i controlli dello stato dell'istanza comporteranno la copia dell'AMI su una replica esatta del sistema operativo danneggiato. Dopo aver confermato il messaggio di stato, crea l'AMI e avvia una nuova istanza utilizzando la nuova AMI.

Console

Per creare un'istanza sostitutiva

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza bloccata.
3. Scegliere Actions (Operazioni), Image and templates (Immagine e modelli), Create image (Crea immagine).
4. Nella pagina Create image (Crea un'immagine), eseguire le operazioni seguenti:
   a. Immettere un nome e una descrizione per l'AMI.
   b. Deselezionare l'opzione Riavvia istanza.

c. Scegliere Create Image (Crea immagine).

Per ulteriori informazioni, consulta the section called "Creare un'AMI da un'istanza".

5. Avviare una nuova istanza dall'AMI e verificare che funzioni.
6. Selezionare l'istanza bloccata e scegliere Operazioni, Stato istanza, Termina (elimina) istanza. Se l'istanza si blocca anche durante il processo di terminazione, Amazon EC2 la forza automaticamente perché termini entro poche ore.

Se non è possibile creare un'AMI dall'istanza come descritto nella procedura precedente, è possibile configurare un'istanza sostitutiva come segue:

(In alternativa) Per creare un'istanza sostitutiva utilizzando la console

1. Selezionare l'istanza e scegliere Description (Descrizione), Block devices (Dispositivi a blocchi). Selezionare ciascun volume e prendere nota del relativo ID del volume. Accertarsi di annotarsi il volume root.
2. Nel riquadro di navigazione, selezionare Volumes (Volumi). Selezionare ogni volume dell'istanza e scegliere Actions (Operazioni), Create Snapshot (Crea snapshot).
3. Nel riquadro di navigazione, selezionare Snapshots (Snapshot). Selezionare la snapshot appena creata, quindi scegliere Actions (Operazioni), Create Volume (Crea volume).
4. Avviare un'istanza con lo stesso sistema operativo di quella bloccata. Prendere nota dell'ID del volume e del nome del dispositivo del relativo volume root.
5. Nel riquadro di navigazione scegliere Instances (Istanze), selezionare l'istanza appena avviata, scegliere Instance state (Stato istanza), Stop instance (Arresta istanza).
6. Nel riquadro di navigazione scegliere Volumes (Volumi), selezionare il volume root dall'istanza arrestata, quindi scegliere Actions (Operazioni), Detach Volume (Distacca volume).
7. Selezionare il volume root creato a partire dall'istanza bloccata, scegliere Actions (Operazioni), Attach Volume (Collega volume), quindi collegarlo alla nuova istanza come suo volume root (utilizzando il nome del dispositivo di cui si è preso nota). Collegare eventuali altri volumi non root all'istanza.
8. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza sostitutiva. Scegli Instance state (Stato istanza), Start instance (Avvia istanza). Verificare che l'istanza funzioni.

9. Selezionare l'istanza bloccata e scegliere Stato istanza, Termina (elimina) istanza. Se l'istanza si blocca anche durante il processo di terminazione, Amazon EC2 la forza automaticamente perché termini entro poche ore.

AWS CLI

Per creare un'istanza sostitutiva

1. Creare un'AMI dall'istanza bloccata utilizzando il comando create-image con l'opzione `--no-reboot`.

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "my-replacement-ami" \
    --description "AMI for replacement instance" \
    --no-reboot
```

2. Avvia una nuova istanza dall'AMI appena creata, utilizzando il comando run-instances.
3. Verificare che la nuova istanza funzioni.
4. (Facoltativo) Termina l'istanza bloccata utilizzando il comando terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

PowerShell

Per creare un'istanza sostitutiva

1. Crea un'AMI dall'istanza bloccata utilizzando il New-EC2Image cmdlet e impostala su. `-NoReboot true`

```
New-EC2Image `
    -InstanceId i-1234567890abcdef0 `
    -Name "my-replacement-ami" `
    -Description "AMI for replacement instance" `
    -NoReboot $true
```

2. Avvia una nuova istanza dall'AMI appena creata, utilizzando il New-EC2Instance cmdlet.
3. Verificare che la nuova istanza funzioni.

4. (Facoltativo) Termina l'istanza bloccata utilizzando il cmdlet. Remove-EC2Instance

```
Remove-EC2Instance -InstanceId i-1234567890abcdef0
```

Risoluzione dei problemi relativi alla terminazione dell'istanza Amazon EC2

L'arresto o l'eliminazione dell'istanza è nota come terminazione dell'istanza. Le informazioni seguenti possono essere utili per risolvere i problemi di terminazione dell'istanza.

Non viene addebitato alcun costo per l'utilizzo di un'istanza se questa non si trova nello stato `running`. In altre parole, quando un'istanza viene terminata, non appena il suo stato passa a non viene più addebitato alcun cost `shutting-down`.

Terminazione immediata dell'istanza

All'avvio, diversi problemi possono causare la chiusura immediata dell'istanza. Per ulteriori informazioni, consulta Terminazione immediata dell'istanza.

Ritardo della terminazione dell'istanza

Se l'istanza rimane nello stato `shutting-down` per più di alcuni minuti, è possibile che sia perché:

- L'istanza esegue script di spegnimento.
- C'è un problema con il computer host sottostante.

Dopo molte ore nello stato `shutting-down`, Amazon EC2 considera quell'istanza bloccata e ne forza la terminazione.

Per risolvere autonomamente un'istanza bloccata:

1. Termina forzatamente l'istanza

   Usa la console Amazon EC2 o la AWS CLI per forzare la terminazione dell'istanza. Per la procedura, consultare Termina forzatamente un'istanza.

   L'istanza tenterà innanzitutto un arresto regolare, che include lo svuotamento delle cache e dei metadati del file system (sebbene possa evitare opzionalmente l'arresto regolare). Se l'arresto

regolare non viene completato entro il periodo di timeout, l'istanza si chiude forzatamente senza svuotare le cache e i metadati del file system.

2. Se la terminazione forzata non ha esito positivo

   Se dopo alcune ore l'istanza non è interrotta e sembra bloccata nella condizione di terminazione, effettua quanto segue:

   a. Pubblicare una richiesta di assistenza su AWS re:Post. Per velocizzare la risoluzione, includere l'ID dell'istanza e descrivere le fasi già eseguite.
   b. In alternativa, se si dispone di un piano di supporto, creare un caso di supporto tecnico presso il Centro di supporto.

Termina forzatamente un'istanza

Se sembra che l'istanza sia bloccata nella condizione di terminazione, puoi forzarla. Se dopo alcune ore l'istanza non è terminata, pubblica una richiesta di assistenza su AWS re:Post. Per velocizzare la risoluzione, includere l'ID dell'istanza e descrivere le fasi già eseguite. In alternativa, se si dispone di un piano di supporto, creare un caso di supporto tecnico presso il Centro di supporto.

Console

Per terminare forzatamente un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza bloccata.
3. Scegli Stato dell'istanza, Termina forzatamente l'istanza.

   Nota che Termina forzatamente l'istanza è disponibile solo nella console se l'istanza è nello stato `stopping`. Se la tua istanza si trova in un altro stato (eccetto `shutting-down` `eterminated`) puoi utilizzare la AWS CLI terminazione forzata dell'istanza.
4. (Facoltativo) Per evitare il regolare spegnimento del sistema operativo durante il termine forzato, seleziona la casella di controllo Salta l'arresto del sistema operativo.
5. Scegli Terminazione forzata.

AWS CLI

Per terminare forzatamente un'istanza

Utilizza il comando terminate-instances con l'opzione `--force`.

```
aws ec2 terminate-instances \
    --instance-ids i-1234567890abcdef0 \
    --force
```

Per ignorare il regolare spegnimento del sistema operativo durante la terminazione forzata, includi l'opzione `--skip-os-shutdown`.

```
aws ec2 terminate-instances \
    --instance-ids i-1234567890abcdef0 \
    --force \
    --skip-os-shutdown
```

PowerShell

Per terminare forzatamente un'istanza

Usa il Remove-EC2Instance cmdlet e imposta su. `-Enforce true`

```
Remove-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true
```

Per ignorare il regolare spegnimento del sistema operativo durante la terminazione forzata, includi `-SkipOsShutdown $true`.

```
Remove-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true `
    -SkipOsShutdown $true
```

L'istanza terminata rimane visualizzata

Dopo essere stata terminata, un'istanza rimane visibile per un breve periodo prima di essere eliminata. Lo stato indicato è `terminated`. Se dopo molte questa voce non viene eliminata, contattare il supporto.

Errore: l'istanza non può essere terminata. Modifica il relativo attributo di istanza «disable» ApiTermination

Quando provi a terminare un'istanza, appare il messaggio di errore `The instance i-1234567890abcdef0 may not be terminated. Modify its 'disableApiTermination' instance attribute` nel quale è indicato che l'istanza è stata abilitata per la protezione da terminazione. La protezione da terminazione impedisce la terminazione involontaria dell'istanza.

Per terminare l'istanza, devi innanzitutto disabilitare tale protezione.

Per ulteriori informazioni, consulta Modifica della protezione da terminazione dell'istanza.

Istanze avviate o terminate automaticamente

In genere i seguenti comportamenti indicano che sono stati utilizzati Amazon EC2 Auto Scaling, un parco istanze EC2 o un parco istanze Spot per dimensionare automaticamente le risorse di calcolo in base ai criteri che hai definito:

- Termina un'istanza e una nuova istanza viene avviata automaticamente.
- Avvia un'istanza e una delle istanze viene terminata automaticamente.
- Arresta un'istanza e terminala e una nuova istanza viene avviata automaticamente.

Per interrompere il ridimensionamento automatico, individua il gruppo Auto Scaling o il parco istanze che avvia le istanze e impostane la capacità su 0 o eliminalo.

Risoluzione di problemi relativi a un'istanza Amazon EC2 irraggiungibile

Le informazioni seguenti possono essere utili per risolvere i problemi relativi alle istanze Amazon EC2. È possibile acquisire screenshot o accedere all'output della console per diagnosticare i problemi e determinare se occorre riavviare l'istanza. Per le istanze Windows non raggiungibili, risolvere i problemi esaminando gli screenshot restituiti dal servizio.

Indice

- Riavvio dell'istanza

- Output della console delle istanze
- Acquisizione di uno screenshot di un'istanza irraggiungibile
- Screenshot comuni per la risoluzione dei problemi relativi alle istanze di Windows non raggiungibili
- Ripristino delle istanze in caso di errori del computer host
- L'istanza è apparsa offline ed è stata inaspettatamente riavviata

Riavvio dell'istanza

La possibilità di riavviare le istanze altrimenti non raggiungibili è importante sia per la risoluzione dei problemi che per la gestione generale delle istanze.

Così come puoi ripristinare un computer tramite l'apposito pulsante, puoi ripristinare le istanze EC2 utilizzando la console di Amazon EC2, la CLI o l'API. Per ulteriori informazioni, consulta Riavvio di un'istanza Amazon EC2.

Output della console delle istanze

L'output della console rappresenta un prezioso strumento per diagnosticare i problemi. In particolare, è utile per risolvere i problemi del kernel e della configurazione dei servizi che potrebbero causare la terminazione o la mancata raggiungibilità di un'istanza prima che il relativo daemon SSH possa essere avviato.

- Istanze Linux: l'output della console delle istanze visualizza esattamente lo stesso output che verrebbe normalmente visualizzato su un monitor fisico collegato a un computer. L'output della console restituisce le informazioni di buffering pubblicate poco dopo lo stato transitorio di un'istanza (avvio, arresto, riavvio e terminazione). L'output pubblicato non viene aggiornato continuamente, ma solo quando viene ritenuto importante.
- Istanze Windows: l'output della console include gli ultimi tre errori del log degli eventi relativi al sistema.

Solo il proprietario dell'istanza può accedere all'output della console.

È possibile recuperare l'ultimo output seriale della console durante il ciclo di vita dell'istanza. Questa opzione è supportata solo nelle Nitro-based istanze.

Console

Per ottenere l'output della console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Instances (Istanze).
3. Selezionare l'istanza.
4. Scegliere Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), quindi Get system log (Ottieni il log di sistema).

AWS CLI

Per ottenere l'output della console

Utilizza il comando get-console-output.

```
aws ec2 get-console-output --instance-id i-1234567890abcdef0
```

PowerShell

Per ottenere l'output della console

Utilizza il cmdlet Get-EC2ConsoleOutput.

```
Get-EC2ConsoleOutput -InstanceId i-1234567890abcdef0
```

Acquisizione di uno screenshot di un'istanza irraggiungibile

Se è impossibile connettersi all'istanza, è possibile acquisire uno screenshot dell'istanza e visualizzarla come immagine. L'immagine può fornire visibilità dello stato dell'istanza e risolvere più rapidamente eventuali problemi.

Puoi generare screenshot mentre l'istanza è in esecuzione o dopo il suo arresto. L'immagine è generata in formato JPG e non supera i 100 KB. Per lo screenshot non sono previsti costi di trasferimento dei dati.

Limitazioni

Questa funzionalità non è supportata dalle seguenti istanze:

- Istanze bare metal (istanze del tipo `*.metal`)
- L'istanza utilizza un driver NVIDIA GRID
- Istanze alimentate da Arm-based processori Graviton
- Istanze Windows attive AWS Outposts
- Istanze di Windows nelle zone locali AWS

Supporto di una regione

Questa funzionalità non è disponibile nelle seguenti regioni:

- Asia Pacifico (Thailandia)
- Messico (centrale)
- GovCloud Regioni

Console

Per ottenere uno screenshot di un'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegli Instances (Istanze).
3. Selezionare l'istanza da acquisire.
4. Scegliere Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), quindi Get instance screenshot (Ottieni screenshot istanza).
5. Scegli Scarica o apri il menu contestuale (clic con il pulsante destro del mouse) per scaricare e salvare l'immagine.

AWS CLI

Per acquisire uno screenshot di un'istanza

Utilizza il comando get-console-screenshot. L'output è con codifica base64.

```
aws ec2 get-console-screenshot --instance-id i-1234567890abcdef0
```

PowerShell

Per acquisire uno screenshot di un'istanza

Utilizza il cmdlet Get-EC2ConsoleScreenshot. L'output è con codifica base64.

```
Get-EC2ConsoleScreenshot -InstanceId i-1234567890abcdef0
```

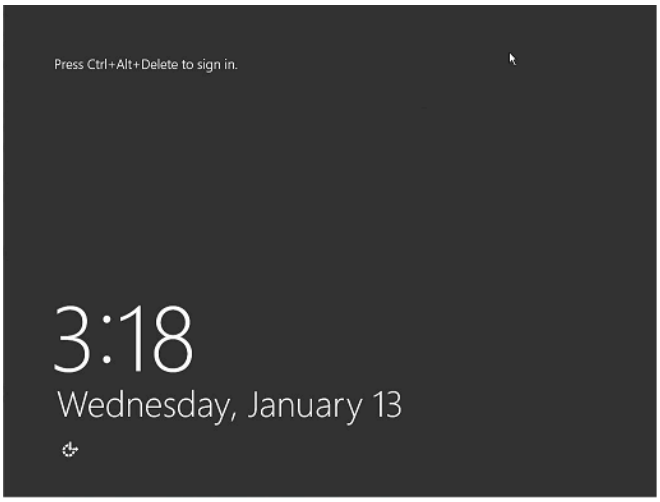
Screenshot comuni per la risoluzione dei problemi relativi alle istanze di Windows non raggiungibili

Puoi utilizzare le informazioni seguenti per facilitare la risoluzione dei problemi associati a un'istanza Windows irraggiungibile in base all'acquisizione di screenshot restituiti dal servizio.

- Schermata di accesso (Ctrl+Alt+Canc)
- Schermata della console di ripristino
- Schermata Windows Boot Manager
- Schermata Sysprep
- Schermata di preparazione
- Schermata Windows Update
- Chkdsk

Schermata di accesso (Ctrl+Alt+Canc)

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.





Se un'istanza diventa irraggiungibile durante l'accesso, potrebbe esserci un problema relativo alla configurazione di rete o ai Servizi Desktop remoto di Windows. Un'istanza può inoltre non rispondere se un processo utilizza una quantità significativa di CPU.

Configurazione della rete

Utilizza le seguenti informazioni per verificare che le tue AWS configurazioni di rete, di Microsoft Windows e locali (o locali) non blocchino l'accesso all'istanza.

AWS configurazione della rete

Configurazione	Verifica
Configurazione del gruppo di sicurezza	Verifica che la porta 3389 sia aperta per il gruppo di sicurezza. Verifica che ti stai collegando all'indirizzo IP pubblico corretto. Se l'istanza non è associata a un IP elastico, l'IP pubblico cambia dopo l'istanza. stops/starts Per ulteriori informazioni, consulta Il desktop remoto non può connettersi al computer remoto.
Configurazione VPC (liste di controllo degli accessi di rete)	Verifica che la lista di controllo accessi (ACL) del tuo Amazon VPC non stia bloccando l'accesso. Per informazioni, consulta Liste di controllo degli accessi di rete nella Guida per l'utente di Amazon VPC.
Configurazione VPN	Se ti stai connettendo al VPC tramite una rete privata virtuale (VPN), verifica la connettività del tunnel della VPN. Per ulteriori informazioni, consulta Troubleshooting AWS Client VPN: problemi di connettività del tunnel verso un VPC.

Configurazione di rete Windows

Configurazione	Verifica
Windows Firewall	Verifica che Windows Firewall non stia bloccando le connessioni alla istanza. Disabilit a Windows Firewall come descritto al punto 7 della sezione di risoluzione dei problemi del desktop remoto, Il desktop remoto non può connettersi al computer remoto.
TCP/IP Configurazione avanzata (uso dell'IP statico)	L'istanza potrebbe non rispondere perché hai configurato un indirizzo IP statico. Per un VPC, creare un'interfaccia di rete e collegarla all'istanza.

Configurazione di rete locale o on-premises

Verifica che una configurazione di rete locale non stia bloccando l'accesso. Prova a connetterti a un'altra istanza nello stesso VPC dell'istanza irraggiungibile. Se non riesci ad accedere a un'altra istanza, contatta il tuo amministratore di rete locale per stabilire se una policy locale limita l'accesso.

Problema correlato ai Servizi Desktop remoto

Se l'istanza diventa irraggiungibile durante l'accesso, potrebbe esserci un problema relativo ai Servizi Desktop remoto (RDS) nell'istanza.

> **Tip**
>
> Puoi utilizzare il runbook `AWSSupport-TroubleshootRDP` per verificare e modificare varie impostazioni che potrebbero influire sulle connessioni RDP (Remote Desktop Protocol). Per ulteriori informazioni, consulta `AWSSupport-TroubleshootRDP` in Documentazione di riferimento del runbook AWS Systems Manager .

Configurazione dei Servizi Desktop remoto

Configurazione	Verifica
RDS in esecuzione	Verificare che RDS sia in esecuzione sull'istanza. Connettiti all'istanza tramite l'applicazione Servizi di Microsoft Managemen t Console (MMC) (`services.msc`). Nell'elenco dei servizi verificare che Remote Desktop Services (Servizi Desktop remoto) sia Running (In esecuzione). In caso contrario, avviarli e impostare il tipo di avvio su Automatic (Automatico). Se non è possibile connettersi all'istanza utilizzando l'applicazione Servizi, distaccare il volume root dall'istanza, acquisire uno snapshot del volume o creare un'AMI da esso, collegare il volume originale a un'altra istanza nella stessa zona di disponibilità come volume secondario e modificare la chiave di registro Start. Una volta terminato, ricollega il volume radice all'istanza originale.
RDS abilitato	Anche se il servizio è avviato, potrebbe essere disabilitato. Distacca il volume root dall'istanza, acquisisci una snapshot del volume o crea un'AMI da esso, collega il volume originale a un'altra istanza nella stessa zona di disponibilità come volume secondario e abilita il servizio modificando la chiave di registro Terminal Server come descritto in Abilitazione di Desktop remoto in un'istanza EC2 con il Registro di sistema remoto: Una volta terminato, ricollega il volume radice all'istanza originale.

Elevato utilizzo della CPU

Verifica la metrica di utilizzo della CPU (massimo) sulla tua istanza utilizzando Amazon. CloudWatch Se il valore CPUUtilization (Maximum) è un numero elevato, attendere che si abbassi e riprovare. Un utilizzo elevato della CPU può essere causato da:

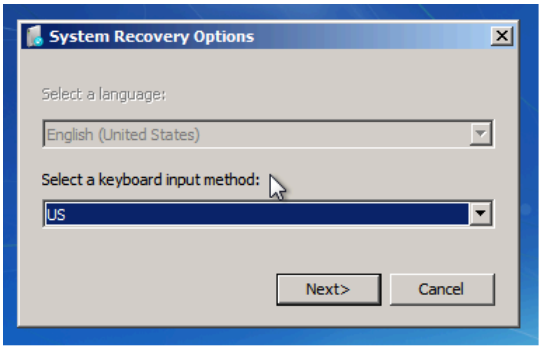
- Windows Update
- Scansione del software di sicurezza
- Script di avvio personalizzato

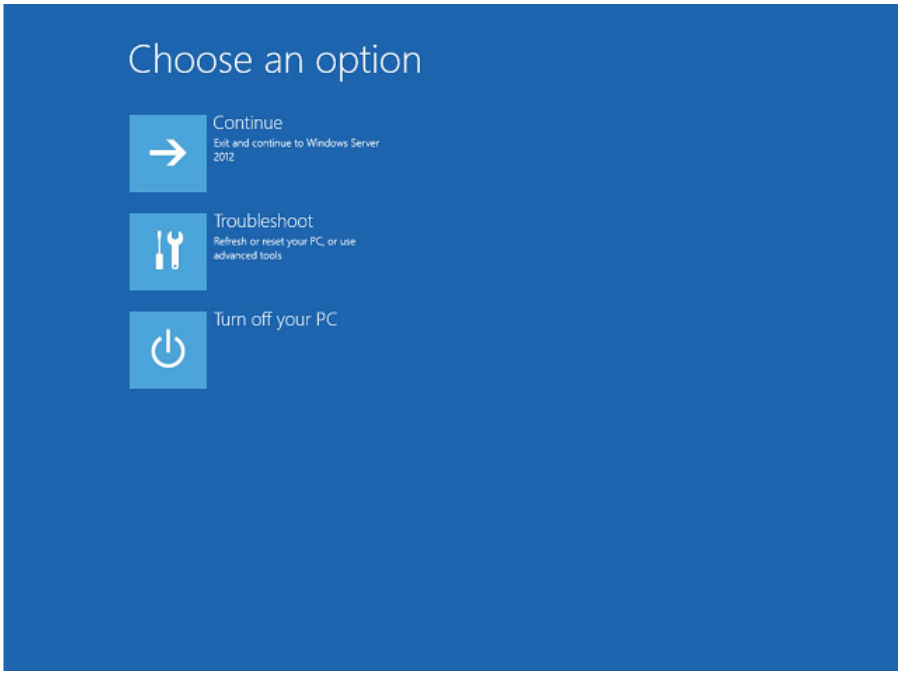
- Pianificatore di attività

Per ulteriori informazioni, consulta Get Statistics for a Specific Resource nella Amazon User Guide. CloudWatch Per ulteriori suggerimenti per la risoluzione di problemi, consulta Utilizzo elevato della CPU poco dopo l'avvio di Windows (solo istanze Windows).

Schermata della console di ripristino

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.





Se `bootstatuspolicy` non è impostato su `ignoreallfailures`, il sistema operativo potrebbe avviarsi nella console di ripristino e restare bloccato in questo stato. Utilizza la procedura seguente per cambiare la configurazione `bootstatuspolicy` in `ignoreallfailures`.

Per impostazione predefinita, la configurazione delle policy per le AMI Windows pubbliche fornite da AWS è impostata su. `ignoreallfailures`

1. Arrestare l'istanza irraggiungibile.
2. Creare una snapshot del volume root. Il volume root è collegato all'istanza come `/dev/sda1`.

   Distacca il volume root dall'istanza irraggiungibile, acquisisci una snapshot del volume o crea un'AMI da esso, quindi collegalo a un'altra istanza nella stessa zona di disponibilità come volume secondario.

> **Warning**
>
> Se la tua istanza temporanea e l'istanza originale sono state avviate utilizzando la stessa AMI, dovrai completare altre operazioni o non sarai in grado di avviare l'istanza originale dopo aver ripristinato il volume root a causa di un conflitto di firme del disco. Se devi creare un'istanza temporanea utilizzando la stessa AMI, completa le operazioni in Collisione della firma del disco per evitare un conflitto di firma del disco.
> In alternativa, seleziona un'AMI diversa per l'istanza temporanea. Ad esempio, se l'istanza originale utilizza un'AMI per Windows Server 2016, avvia l'istanza temporanea utilizzando un'AMI per Windows Server 2019.

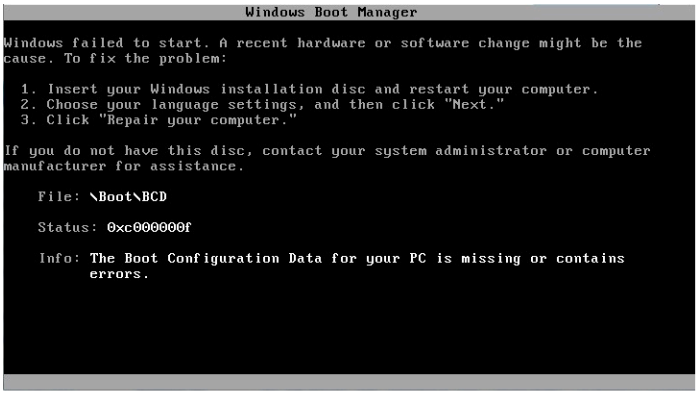
3. Accedi all'istanza ed emetti il comando seguente da un prompt di comandi per modificare la configurazione di `bootstatuspolicy` in `ignoreallfailures`.

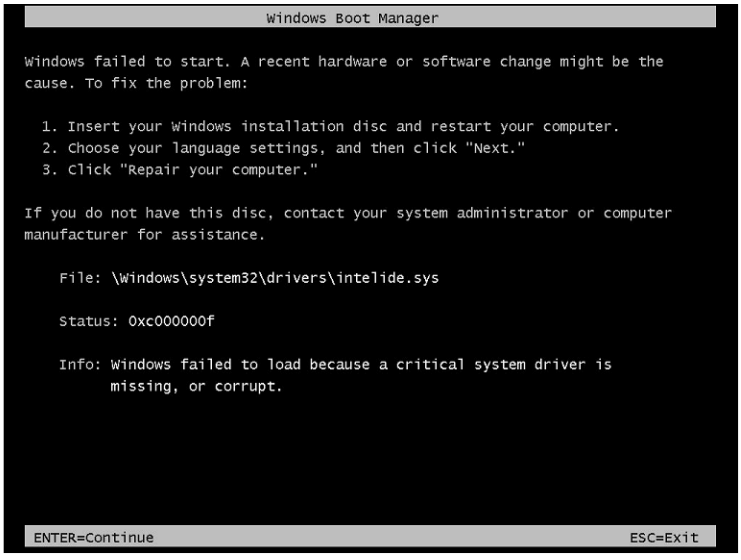
```
bcdedit /store Drive Letter:\boot\bcd /set {default} bootstatuspolicy
 ignoreallfailures
```

4. Ricollegare il volume all'istanza irraggiungibile e avviare nuovamente l'istanza.

Schermata Windows Boot Manager

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.



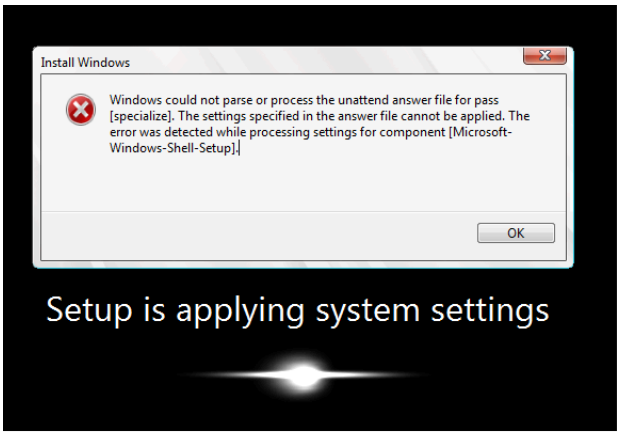


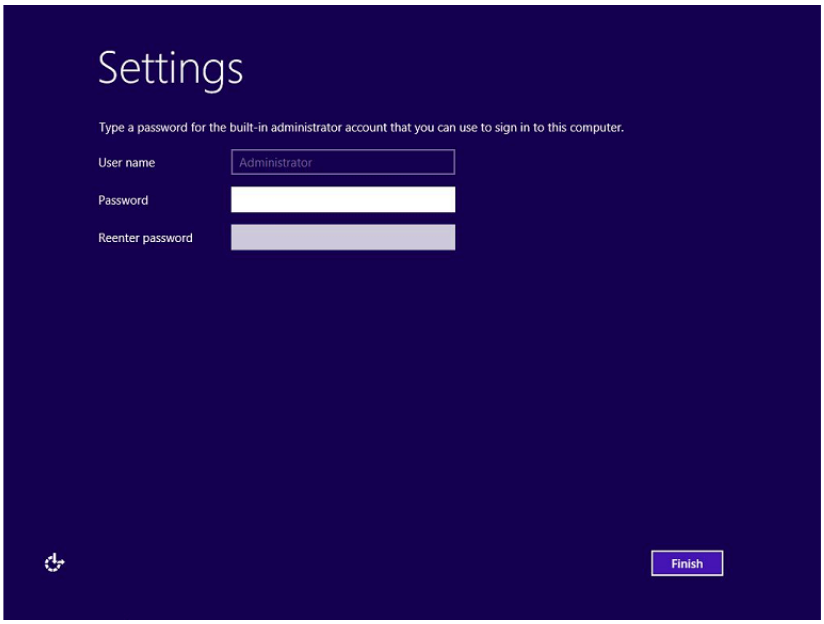
Il sistema operativo ha subito un danneggiamento irreversibile del file di sistema, and/or il registro. Quando un'istanza è bloccata in questo stato, puoi recuperarla da un'AMI di backup recente o avviare

un'istanza di sostituzione. Se è necessario accedere ai dati dell'istanza, distacca qualsiasi volume root dall'istanza irraggiungibile, acquisisci una snapshot di tali volumi o crea un'AMI da essi, quindi collegali a un'altra istanza nella stessa zona di disponibilità come volume secondario.

Schermata Sysprep

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.

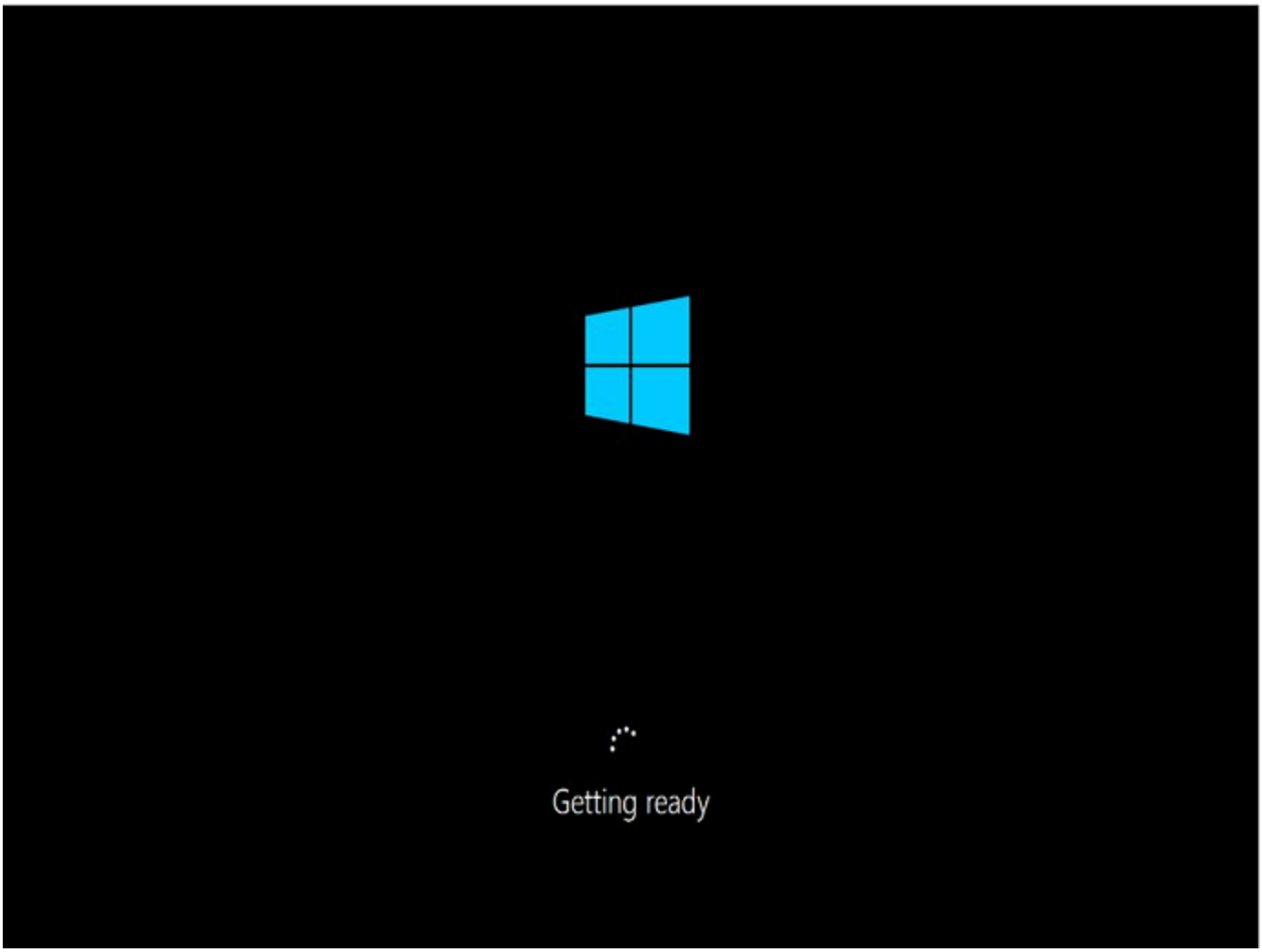




Potresti visualizzare questa schermata se non hai utilizzato il servizio EC2Config per chiamare Sysprep o se il sistema operativo ha riscontrato un errore nell'esecuzione di Sysprep. È possibile reimpostare la password utilizzando EC2Rescue. In caso contrario, consulta Creare un'AMI Amazon EC2 utilizzando Windows Sysprep.

Schermata di preparazione

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.



Aggiorna il servizio di acquisizione di screenshot della console dell'istanza ripetutamente per verificare che l'anello di avanzamento stia girando. In tal caso, attendi che il sistema operativo si avvii. Puoi anche controllare la metrica di utilizzo della CPU (massimo) sulla tua istanza utilizzando Amazon CloudWatch per vedere se il sistema operativo è attivo. Se l'anello di avanzamento non sta girando, l'istanza potrebbe essere bloccata a livello del processo di avvio. Riavviare l'istanza. Se il riavvio non risolve il problema, recupera l'istanza da un'AMI di backup recente o avvia un'istanza di sostituzione. Se è necessario accedere ai dati dell'istanza, distacca il volume root dall'istanza irraggiungibile, acquisisci una snapshot del volume o crea un'AMI da esso. Quindi, collegalo a un'altra istanza nella stessa zona di disponibilità come volume secondario.

Schermata Windows Update

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.

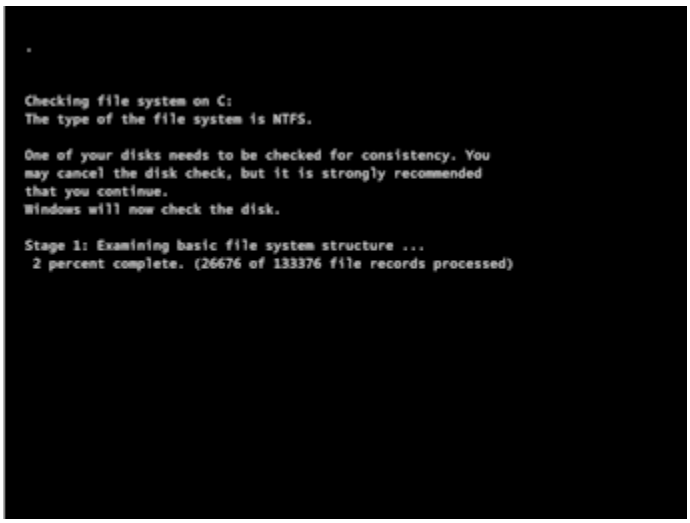


Il processo Windows Update sta aggiornando il registro. Attendi la fine dell'aggiornamento. Non riavviare o arrestare l'istanza perché ciò potrebbe danneggiare i dati durante l'aggiornamento.

> **Note**
>
> Il processo Windows Update può utilizzare le risorse sul server durante l'aggiornamento. Se riscontri spesso questo problema, considera la possibilità di usare tipi di istanza e volumi EBS più veloci.

Chkdsk

Il servizio di acquisizione di screenshot della console ha restituito quanto segue.



Windows sta eseguendo lo strumento di sistema chkdsk sull'unità per verificare l'integrità del file system e correggerne gli errori logici Attendi il completamento del processo.

Ripristino delle istanze in caso di errori del computer host

Se si presenta un problema irrecuperabile con l'hardware di un computer host sottostante, è possibile che AWS pianifichi un evento di arresto delle istanze. Tale evento ti viene notificato in anticipo tramite e-mail.

Per ripristinare un' EBS-backed istanza Amazon in esecuzione su un computer host che ha avuto un errore

1. Eseguire il backup di tutti i dati importanti contenuti nei volumi instance store in Amazon EBS o Amazon S3.
2. Arrestare l'istanza.
3. Avviare l'istanza.
4. Ripristinare i dati importanti.

Per ulteriori informazioni, consulta Avvio e arresto di un'istanza Amazon EC2.

Per ripristinare un'istanza con un volume root dell'archivio dell'istanza in esecuzione su un computer host in stato di errore

1. Creare un'AMI dall'istanza.
2. Caricare l'immagine su Amazon S3.
3. Eseguire il backup dei dati importanti in Amazon EBS o Amazon S3.
4. Terminare l'istanza.
5. Avviare una nuova istanza dall'AMI.
6. Ripristinare i dati importanti sulla nuova istanza.

L'istanza è apparsa offline ed è stata inaspettatamente riavviata

Se sembra che l'istanza sia stata offline e poi riavviata inaspettatamente, è possibile che sia stata ripristinata automaticamente. Ciò si verifica quando AWS rileva che l'istanza non è disponibile a causa di un problema hardware o software sottostante e sull'istanza è abilitato il ripristino automatico semplificato o il ripristino basato su CloudWatch azioni.

Durante il processo di ripristino, AWS tenta di ripristinare la disponibilità dell'istanza migrandola su un hardware diverso. Per verificare se per la tua istanza è stato eseguito il recupero automatico dell'istanza, consulta Verificare se è avvenuto il ripristino automatico dell'istanza.

> **Note**
>
> Se il carico di lavoro o l'applicazione non risponde, controlla se è in esecuzione sull'istanza. Nel caso non lo sia, avvialo manualmente. Per prevenire questo problema in futuro, implementa un piano di recupero per garantire il corretto funzionamento del carico di lavoro o dell'applicazione dopo il recupero dell'istanza.

Risoluzione dei problemi di connessione all'istanza Linux di Amazon EC2

Le informazioni e gli errori comuni seguenti possono essere utili per risolvere i problemi di connessione all'istanza Linux.

Problemi di connessione

- Cause comuni dei problemi di connessione
- Errore di connessione all'istanza: Connection timed out
- Errore: impossibile caricare la chiave... Valore previsto: QUALSIASI CHIAVE PRIVATA
- Errore: User key not recognized by server
- Errore: autorizzazione negata o connessione chiusa dalla porta 22 [istanza]
- Errore: Unprotected Private Key File (File della chiave privata non protetto)
- Errore: la chiave privata deve iniziare con "-----BEGIN RSA PRIVATE KEY-----" e finire con "-----END RSA PRIVATE KEY-----"
- Errore: verifica della chiave host non riuscita
- Errore: il server ha rifiutato la nostra chiave or Nessun metodo di autenticazione supportato disponibile
- Cannot Ping Instance (Impossibile eseguire il ping dell'istanza)
- Errore: il server ha chiuso inaspettatamente la connessione di rete
- Errore: convalida della chiave host non riuscita per EC2 Instance Connect

- Impossibile connettersi all'istanza Ubuntu tramite EC2 Instance Connect
- Ho perso la mia chiave privata. Come posso connettermi alla mia istanza?

Cause comuni dei problemi di connessione

Ti consigliamo di iniziare a risolvere i problemi di connessione delle istanze verificando di aver eseguito con precisione le seguenti attività.

Verifica il nome utente per l'istanza

È possibile connettersi all'istanza utilizzando il nome utente dell'account utente o il nome utente predefinito per l'AMI utilizzato per avviare l'istanza.

- Ottenere il nome utente per il proprio account utente.

  Per ulteriori informazioni su come creare un account utente, consulta Gestione degli utenti del sistema sull'istanza Amazon EC2 Linux.
- Ottieni il nome utente predefinito per l'AMI che hai utilizzato per avviare l'istanza.

AMI utilizzata per avviare l'istanza	Nome utente predefinito
Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`
FreeBSD	`ec2-user`
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`

AMI utilizzata per avviare l'istanza	Nome utente predefinito
Rocky Linux	`rocky`
Altro	Verifica con il provider dell'AMI

Verificare che le regole del gruppo di sicurezza consentano il traffico

Verificare che il gruppo di sicurezza associato alla tua istanza consenta il traffico SSH in entrata dal tuo indirizzo IP. Per impostazione predefinita, il gruppo di sicurezza predefinito per il VPC non consente il traffico SSH in entrata. Per impostazione predefinita, il gruppo di sicurezza creato dalla procedura guidata di avvio abilita il traffico SSH. Per i passaggi per aggiungere una regola per il traffico SSH in entrata alla tua istanza Linux, consulta Regole per la connessione alle istanze dal computer in uso. Per le fasi di verifica, consulta Errore di connessione all'istanza: Connection timed out.

Verificare che l'istanza sia pronta

Dopo aver avviato un'istanza, possono essere necessari alcuni minuti affinché sia pronta ad accettare richieste di connessione. Controllare l'istanza per assicurarsi che sia in esecuzione e che abbia superato i controlli di stato.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza desiderata.
3. Verificare quanto segue:
   a. Nella colonna Instance state (Stato istanza), verificare che l'istanza sia nello stato `running`.
   b. Nella colonna Controllo stato, verifica che l'istanza abbia superato tutti i controlli di stato.

Verifica che siano soddisfatto tutti i prerequisiti per connetterti

Assicurarsi di avere tutte le informazioni necessarie per la connessione. Per ulteriori informazioni, consulta Connessione a un'istanza Linux tramite SSH.

Connessione da Linux o macOS X

Se il sistema operativo del computer locale è Linux o macOS X, consultare i seguenti prerequisiti specifici per connettersi a un'istanza Linux:

- Client SSH
- EC2 Instance Connect
- AWS Systems Manager Gestore delle sessioni

Connettersi da Windows

Se il sistema operativo del computer locale è Microsoft, consulta i seguenti prerequisiti specifici per connettersi a un'istanza Linux:

- OpenSSH
- PuTTY
- AWS Systems Manager Gestore delle sessioni
- Sottosistema Windows per Linux

Verificare se l'istanza è un'istanza gestita

User-initiated le connessioni alle istanze gestite non sono consentite. Per determinare se l'istanza è gestita, trovare il campo Gestito relativo all'istanza. Se il valore è vero, si tratta di un'istanza gestita. Per ulteriori informazioni, consulta Istanze gestite di Amazon EC2.

Errore di connessione all'istanza: Connection timed out

Se si tenta di connettersi all'istanza e si riceve il messaggio di errore `Network error: Connection timed out` o `Error connecting to [instance], reason: -> Connection timed out: connect`, provare a procedere come segue:

Verificare le regole del gruppo di sicurezza.

È necessaria una regola del gruppo di sicurezza che consenta il traffico in entrata dall'indirizzo IPv4 pubblico del computer locale sulla porta corretta.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza desiderata.
3. Nella scheda Security (Sicurezza) nella parte inferiore della pagina della console, in Inbound rules (Regole in entrata) controllare l'elenco delle regole in vigore per l'istanza selezionata. Verificare che sia presente una regola che consente il traffico dal computer locale alla porta 22 (SSH).

Se il gruppo di sicurezza non dispone di una regola che consente il traffico in entrata dal computer locale, aggiungi una regola al gruppo di sicurezza. Per ulteriori informazioni, consulta Regole per la connessione alle istanze dal computer in uso.

4. Per la regola che consente il traffico in entrata, controlla il campo Source (Origine). Se il valore è un singolo indirizzo IP e se l'indirizzo IP non è statico, verrà assegnato un nuovo indirizzo IP ogni volta che si riavvia il computer. Ciò farà sì che la regola non includa il traffico di indirizzi IP del tuo computer. L'indirizzo IP potrebbe non essere statico se il computer si trova su una rete aziendale o se si sta effettuando la connessione tramite un fornitore di servizi Internet (ISP) o l'indirizzo IP del computer è dinamico e cambia ogni volta che si riavvia il computer. Per essere certi che la regola del gruppo di sicurezza consenta il traffico in entrata dal computer locale, anziché specificare un singolo indirizzo IP per il campo Source (Origine) specifica l'intervallo di indirizzi IP utilizzati dai computer client.

   Per ulteriori informazioni sulle regole dei gruppi di sicurezza, consulta Regole sui gruppi di sicurezza nella Guida per l'utente di Amazon VPC.

Verificare la tabella di routing per la sottorete.

È necessario adottare un instradamento che invii tutto il traffico destinato al di fuori del VPC all'Internet gateway per il VPC.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza desiderata.
3. Nella scheda Networking (Rete), prendere nota dei valori per VPC ID e subnet (sottorete).
4. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
5. Nel riquadro di navigazione, scegliere Internet Gateways. Verificare che al VPC sia associato un Internet gateway. In caso contrario, scegliere Create internet gateway (Crea gateway Internet), immettere un nome per il gateway Internet e scegliere Create internet gateway (Crea gateway Internet). Quindi, per il gateway Internet creato, scegliere Actions (Operazioni), Attach to VPC (Collega a VPC), selezionare il VPC e quindi scegliere Attach internet gateway (Collega gateway Internet) per collegarlo al VPC.
6. Nel riquadro di navigazione scegliere Subnets (Sottoreti) e selezionare la sottorete desiderata.
7. Nella scheda Route table (Tabella di routing), verificare che sia presente un instradamento con `0.0.0.0/0` come destinazione e il gateway Internet del VPC come target. Se si sta effettuando la connessione all'istanza utilizzando il relativo indirizzo IPv6, verificare che sia disponibile un

instradamento per tutto il traffico IPv6 (`::/0`) che punti all'Internet gateway. In caso contrario, eseguire le seguenti operazioni:

a. Selezionare l'ID per la tabella di routing (rtb-xxxxxxxx) per navigare alla tabella di routing.
b. Nella scheda Routes (Route), scegliere Edit routes (Modifica route). Selezionare Add route (Aggiungi route), utilizzare `0.0.0.0/0` come destinazione e il gateway internet come target. Per IPv6, selezionare Add route (Aggiungi route), utilizzare `::/0` come destinazione e il gateway internet come target.
c. Selezionare Save routes (Salva route).

Verificare la lista di controllo accessi (ACL) di rete della sottorete.

Le liste di controllo degli accessi di rete devono consentire il traffico in entrata dall'indirizzo IP locale sulla porta 22. Deve inoltre consentire il traffico in uscita alle porte effimere (1024-65535).

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Sottoreti.
3. Seleziona la sottorete.
4. Nella scheda Lista di controllo accessi di rete, per Regole in entrata verifica che le regole permettano il traffico in entrata dal computer in uso sulla porta richiesta. Altrimenti, elimina o modifica la regola che blocca il traffico.
5. Per Regole in uscita, verifica che le regole permettano il traffico verso computer in uso sulle porte effimere. Altrimenti, elimina o modifica la regola che blocca il traffico.

Se il computer si trova su una rete aziendale

Chiedere all'amministratore di rete se il firewall interno permette il traffico in entrata e in uscita dal computer in uso sulla porta 22.

Se sul computer è presente un firewall, verificare che consenta il traffico in entrata e in uscita dal computer in uso sulla porta 22.

Controllare che l'istanza abbia un indirizzo IPv4 pubblico.

Se non lo ha, è possibile associare un indirizzo IP elastico all'istanza. Per ulteriori informazioni, consulta Indirizzi IP elastici.

Verificare il carico della CPU sull'istanza; è possibile che il server sia in sovraccarico.

AWS fornisce automaticamente dati come le CloudWatch metriche di Amazon e lo stato dell'istanza, che puoi utilizzare per vedere il carico di CPU sulla tua istanza e, se necessario, modificare la modalità di gestione dei carichi. Per ulteriori informazioni, consulta Monitora le tue istanze utilizzando CloudWatch.

- Se il carico è variabile, è possibile aumentare o diminuire automaticamente le istanze utilizzando Auto Scaling ed Elastic Load Balancing.
- Se il carico è in crescita stabile, è possibile passare a un tipo di istanza più grande. Per ulteriori informazioni, consulta Modifiche del tipo di istanza Amazon EC2.

Per connettersi all'istanza utilizzando un indirizzo IPv6, verificare quanto riportato di seguito:

- La sottorete deve essere associata a una tabella di routing che prevede un instradamento per il traffico IPv6 (`::/0`) a un Internet gateway.
- Le regole del gruppo di sicurezza devono permettere il traffico in entrata dall'indirizzo IPv6 locale sulla porta 22.
- Le regole dell'ACL di rete devono permettere il traffico IPv6 in entrata e in uscita.
- Se l'istanza è stata avviata da un'AMI meno recente, potrebbe non essere configurata per DHCPv6 (gli indirizzi IPv6 non vengono riconosciuti automaticamente sull'interfaccia di rete). Per ulteriori informazioni, consulta Configurazione di IPv6 sulle istanze nella Guida per l'utente di Amazon VPC.
- Il tuo computer locale deve avere un indirizzo IPv6 ed essere configurato per utilizzare IPv6.

Errore: impossibile caricare la chiave... Valore previsto: QUALSIASI CHIAVE PRIVATA

Se tenti di connetterti all'istanza e ricevi il messaggio di errore, `unable to load key ... Expecting: ANY PRIVATE KEY`, il file in cui è archiviata la chiave privata non è configurato correttamente. Se il file della chiave privata termina con `.pem`, potrebbe comunque essere configurato in modo errato. Una possibile causa di una configurazione errata di un file della chiave privata è la mancanza di un certificato.

Se il file della chiave privata non è configurato correttamente, segui questi passaggi per risolvere l'errore

1. Creazione di una nuova coppia di chiavi. Per ulteriori informazioni, consulta Creazione di una coppia di chiavi utilizzando Amazon EC2.

> **Note**
>
> In alternativa, è possibile creare una nuova coppia di chiavi tramite uno strumento di terze parti. Per ulteriori informazioni, consulta Creazione di una coppia di chiavi tramite uno strumento di terza parte e importazione della chiave pubblica in Amazon EC2.

2. Aggiungi la nuova coppia di chiavi all'istanza. Per ulteriori informazioni, consulta Ho perso la mia chiave privata. Come posso connettermi alla mia istanza?.
3. Connettiti all'istanza utilizzando la nuova coppia di chiavi.

Errore: User key not recognized by server

Se per connettersi all'istanza si utilizza SSH

- Utilizzare `ssh -vvv` per recuperare le informazioni sul debug triple verbose durante la connessione:

```
ssh -vvv -i path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Il seguente output di esempio mostra quanto visualizzato se si è tentato di connettersi all'istanza con una chiave che non è stata riconosciuta dal server:

```
open/ANT/myusername/.ssh/known_hosts).
debug2: bits set: 504/1024
debug1: ssh_rsa_verify: signature correct
debug2: kex_derive_keys
debug2: set_newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug2: key: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
```

```
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-
interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied (publickey).
```

Se per connettersi all'istanza si utilizza PuTTY

- Verificare che il file della chiave privata (.pem) sia stato convertito nel formato riconosciuto da PuTTY (.ppk). Per ulteriori informazioni sulla conversione della chiave privata, consultare Connessione a un'istanza Linux tramite PuTTY.

  > **Note**
  >
  > In PuTTYgen caricare il file della chiave privata e selezionare Save Private Key (Salva chiave privata) anziché Generate (Genera).

- Accertarsi di connettersi con il nome utente corretto dell'AMI in uso. Immettere il nome utente nella casella Nome host nella finestra Configurazione PuTTY.

AMI utilizzata per avviare l'istanza	Nome utente predefinito
Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`
FreeBSD	`ec2-user`

AMI utilizzata per avviare l'istanza	Nome utente predefinito
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Altro	Verifica con il provider dell'AMI

- Accertarsi di disporre di una regola del gruppo di sicurezza che permetta il traffico in entrata verso la porta corretta. Per ulteriori informazioni, consulta Regole per la connessione alle istanze dal computer in uso.

Errore: autorizzazione negata o connessione chiusa dalla porta 22 [istanza]

Se esegui la connessione all'istanza usando SSH e ricevi uno degli errori seguenti, `Host key not found in [directory]`, `Permission denied (publickey)`, `Authentication failed, permission denied` o `Connection closed by [instance] port 22`, assicurati di connetterti con il nome utente corretto dell'AMI e di avere specificato il file della chiave privata corretto (`.pem`) per l'istanza in uso.

I nomi utente appropriati sono i seguenti:

AMI utilizzata per avviare l'istanza	Nome utente predefinito
Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`

AMI utilizzata per avviare l'istanza	Nome utente predefinito
FreeBSD	`ec2-user`
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Altro	Verifica con il provider dell'AMI

Ad esempio, per utilizzare un client SSH per connettersi a un'istanza Amazon Linux, utilizzare il seguente comando:

```
ssh -i /path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Controllare di utilizzare il file della chiave privata corrispondente alla coppia di chiavi selezionata all'avvio dell'istanza.

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze) e selezionare l'istanza desiderata.
3. Nella scheda Details (Dettagli), in Instance details (Dettagli istanza), verificare il valore Key pair name (Nome della coppia di chiavi).
4. Se all'avvio dell'istanza non è stata specificata una coppia di chiavi, è possibile terminare l'istanza e avviarne una nuova, accertandosi di specificare una coppia di chiavi. Se si tratta di un'istanza già utilizzata ma non si dispone più del file `.pem`, è possibile sostituire la coppia di chiavi con una nuova. Per ulteriori informazioni, consulta Ho perso la mia chiave privata. Come posso connettermi alla mia istanza?.

Se è stata generata una coppia di chiavi, accertarsi che il relativo generatore sia configurato per la creazione delle chiavi RSA. Le chiavi DSA non sono accettate.

Se si riceve un errore `Permission denied (publickey)` e nessuna delle condizioni sopra indicate è applicabile (ad esempio, è stato possibile connettersi in precedenza), è possibile che siano state modificate le autorizzazioni della home directory. Le autorizzazioni per `/home/`*`instance-user-name`*`/.ssh/authorized_keys` devono essere limitate esclusivamente al proprietario.

Per verificare le autorizzazioni dell'istanza

1. Arrestare l'istanza e distaccare il volume radice. Per ulteriori informazioni, consulta Avvio e arresto di un'istanza Amazon EC2.
2. Avviare un'istanza temporanea nella stessa zona di disponibilità dell'istanza corrente (utilizzare la medesima AMI utilizzata per l'istanza corrente o una simile), quindi collegare il volume radice all'istanza temporanea.
3. Connettersi all'istanza temporanea, creare un punto di montaggio e montare il volume che è stato collegato.
4. Dall'istanza temporanea, controllare le autorizzazioni della directory `/home/`*`instance-user-name`*`/` del volume collegato. Se necessario, adeguare le autorizzazioni nel modo seguente:

   ```
   [ec2-user ~]$ chmod 600 mount_point/home/instance-user-name/.ssh/authorized_keys
   ```

   ```
   [ec2-user ~]$ chmod 700 mount_point/home/instance-user-name/.ssh
   ```

   ```
   [ec2-user ~]$ chmod 700 mount_point/home/instance-user-name
   ```
5. Smontare il volume, distaccarlo dall'istanza temporanea e ricollegarlo all'istanza originale. Accertarsi di specificare il nome di dispositivo corretto per il volume radice, ad esempi, `/dev/xvda`.
6. Avviare l'istanza. Se l'istanza temporanea non è più necessaria, è possibile terminarla.

Errore: Unprotected Private Key File (File della chiave privata non protetto)

Il file della chiave privata deve essere protetto dalle operazioni di lettura e scrittura eseguite dagli altri utenti. Se la chiave privata può essere letta o scritta da altri utenti, SSH ignora la chiave in uso e viene visualizzato il seguente messaggio di avviso.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for '.ssh/my_private_key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: .ssh/my_private_key.pem
Permission denied (publickey).
```

Se viene visualizzato un messaggio simile quando si tenta di accedere all'istanza, esaminare la prima riga del messaggio di errore per verificare se si sta utilizzando la chiave pubblica corretta per l'istanza. L'esempio sopra utilizza la chiave privata `.ssh/my_private_key.pem` con le autorizzazioni di file `0777`, che consentono a chiunque di leggere o scrivere in questo file. Trattandosi di un livello di autorizzazione estremamente non sicuro, SSH ignora questa chiave.

Se ti connetti da MacOS o Linux, per risolvere l'errore esegui il seguente comando, sostituendo il percorso del file con quello della chiave privata.

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

Se ti connetti a un'istanza Linux da Windows, completa la seguente procedura sul computer locale.

1. Individuare il file .pem.
2. Apri il menu contestuale (clic con il pulsante destro del mouse) per il file .pem e seleziona Proprietà.
3. Scegliere la scheda Sicurezza.
4. Selezionare Advanced (Avanzate).
5. Verificare di essere il proprietario del file. In caso contrario, cambiare il proprietario con il proprio nome utente.
6. Selezionare Disable inheritance (Disabilita l'ereditarietà) e Remove all inherited permissions from this object (Rimuovi tutte le autorizzazioni ereditate da questo oggetto).
7. Selezionare Add (Aggiungi), Select a principal (Seleziona un'entità principale), inserire il proprio nome utente e selezionare OK.
8. Dalla finestra Permission Entry (Voce di autorizzazione), concedere le autorizzazioni Read (Lettura) e selezionare OK.
9. Fai clic su Apply (Applica) per assicurarti che tutte le impostazioni vengano salvate.

10. Selezionare OK per chiudere la finestra Advanced Security Settings (Impostazioni di sicurezza avanzate).
11. Selezionare OK per chiudere la finestra Properties (Proprietà).
12. Dovrebbe essere possibile stabilire una connessione a un'istanza Linux da Windows utilizzando SSH.

Da una finestra del prompt dei comandi Windows, esegui il comando seguente:

1. Dal prompt dei comandi, passare al percorso del file .pem.
2. Eseguire il seguente comando per reimpostare e rimuovere le autorizzazioni esplicite:

```
icacls.exe $path /reset
```

3. Eseguire il seguente comando per concedere le autorizzazioni di lettura all'utente attuale:

```
icacls.exe $path /GRANT:R "$($env:USERNAME):(R)"
```

4. Eseguire il seguente comando per disabilitare l'ereditarietà e rimuovere le autorizzazioni ereditate.

```
icacls.exe $path /inheritance:r
```

5. Dovrebbe essere possibile stabilire una connessione a un'istanza Linux da Windows utilizzando SSH.

Errore: la chiave privata deve iniziare con "-----BEGIN RSA PRIVATE KEY-----" e finire con "-----END RSA PRIVATE KEY-----"

Se utilizzi uno strumento di terze parti, ad esempio ssh-keygen, per creare una coppia di chiavi RSA, genera la chiave privata nel formato chiave OpenSSH. Quando esegui la connessione all'istanza, se utilizzi la chiave privata nel formato OpenSSH per decrittografare la password, riceverai l'errore `Private key must begin with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----"`.

Per risolvere l'errore, la chiave privata deve essere nel formato PEM. Utilizza il seguente comando per creare la chiave privata nel formato PEM:

```
ssh-keygen -m PEM
```

Errore: verifica della chiave host non riuscita

Questo errore verifica se vi sia una mancata corrispondenza tra la chiave host memorizzata sull'istanza nel file `known_hosts` e sul client. Ad esempio, potrebbe verificarsi una mancata corrispondenza se ci si connette a un'istanza utilizzando un indirizzo IP pubblico, quindi si tenta di riconnettersi a tale istanza utilizzando un indirizzo IP pubblico diverso. Ciò può verificarsi dopo aver aggiunto o rimosso un indirizzo IP Elastic, poiché in tal modo modifica l'indirizzo IP pubblico di un'istanza.

Per risolvere questo errore, inizia confermando che è stata prevista una modifica alla chiave host o alla configurazione di rete dell'istanza. Prima di connetterti all'istanza, potresti anche voler verificare l'impronta host. Dopo esserti connesso all'istanza, puoi rimuovere la vecchia chiave host dal file `known_hosts`. Per istruzioni, consulta la documentazione per la distribuzione Linux in uso sull'istanza.

Errore: il server ha rifiutato la nostra chiave or Nessun metodo di autenticazione supportato disponibile

Se si effettua la connessione all'istanza utilizzando PuTTY e si ricevono gli errori, Errore: Il server ha rifiutato la chiave o Errore: Nessun metodo di autenticazione supportato disponibile, accertarsi di connettersi con il nome utente corretto dell'AMI. Digitare il nome utente in Nome utente nella finestra Configurazione PuTTY.

I nomi utente appropriati sono i seguenti:

AMI utilizzata per avviare l'istanza	Nome utente predefinito
Amazon Linux	`ec2-user`
CentOS	`centos` o `ec2-user`
Debian	`admin`
Fedora	`fedora` o `ec2-user`
FreeBSD	`ec2-user`

AMI utilizzata per avviare l'istanza	Nome utente predefinito
RHEL	`ec2-user` o `root`
SUSE	`ec2-user` o `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Altro	Verifica con il provider dell'AMI

Devi anche verificare che:

- Stai usando la versione più recente di PuTTY. Per ulteriori informazioni, consulta la pagina Web di PuTTY.
- Il file della chiave privata (.pem) deve essere stato convertito nel formato riconosciuto da PuTTY (.ppk). Per ulteriori informazioni sulla conversione della chiave privata, consultare Connessione a un'istanza Linux tramite PuTTY.

Cannot Ping Instance (Impossibile eseguire il ping dell'istanza)

Il comando `ping` è un tipo di traffico ICMP; se non è possibile effettuare il ping dell'istanza, accertarsi che le regole del gruppo di sicurezza relative al traffico in entrata permettano il traffico ICMP per il messaggio `Echo Request` da tutte le origini oppure dal computer o dall'istanza da cui si sta eseguendo il comando.

Se non è possibile eseguire un comando `ping` dall'istanza, accertarsi che le regole del gruppo di sicurezza relative al traffico in uscita permettano il traffico ICMP per il messaggio `Echo Request` verso tutte le destinazioni oppure verso l'host per il quale si sta tentando di effettuare il ping.

I comandi `Ping` possono anche essere bloccati da un firewall o timeout a causa di latenza di rete o problemi hardware. Per ulteriori informazioni sulla risoluzione dei problemi, consultare l'amministratore di rete locale o di sistema.

Errore: il server ha chiuso inaspettatamente la connessione di rete

Se ci si connette all'istanza con PuTTY e si riceve l'errore "Connessione di rete in attesa del server", verificare di aver abilitato i segnali keepalive nella pagina Connessione della configurazione PuTTY per evitare di essere disconnessi. Alcuni server disconnettono i client quando non ricevono dati entro un periodo di tempo specificato. Impostare i Secondi tra i segnali keepalive a 59 secondi.

Se i problemi persistono dopo l'abilitazione dei segnali keepalive, provare a disabilitare l'algoritmo di Nagle nella pagina Connessione della configurazione PuTTY.

Errore: convalida della chiave host non riuscita per EC2 Instance Connect

Se si ruotano le chiavi host dell'istanza, le nuove chiavi host non vengono caricate automaticamente nel database delle chiavi host AWS affidabili. Ciò fa sì che la convalida della chiave host fallisca quando si tenta di connettersi all'istanza utilizzando il client EC2 Instance Connect basato su browser e non si è in grado di connettersi all'istanza.

Per risolvere l'errore, è necessario eseguire lo script `eic_harvest_hostkeys` sull'istanza, che carica la nuova chiave host in EC2 Instance Connect. Lo script si trova in `/opt/aws/bin/` nelle istanze Amazon Linux 2 e in `/usr/share/ec2-instance-connect/` nelle istanze Ubuntu.

Amazon Linux 2

Per risolvere l'errore di convalida della chiave host non riuscita su un'istanza Amazon Linux 2

1. Connettiti all'istanza tramite SSH.

   È possibile connettersi utilizzando la CLI EC2 Instance Connect oppure tramite la coppia di chiavi SSH assegnata all'istanza al momento dell'avvio e il nome utente predefinito dell'AMI utilizzata per avviare l'istanza. Per Amazon Linux 2, il nome utente predefinito è `ec2-user`.

   Ad esempio, se l'istanza è stata avviata tramite Amazon Linux 2, il suo nome DNS pubblico è `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` e la coppia di chiavi è `my_ec2_private_key.pem`, utilizzare il comando seguente per accedere all'istanza tramite SSH:

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

Per ulteriori informazioni sulla connessione all'istanza, consulta Connessione all'istanza Linux tramite un client SSH.

2. Accedere alla cartella:

```
[ec2-user ~]$ cd /opt/aws/bin/
```

3. Eseguire il seguente comando sull'istanza.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Si noti che una chiamata riuscita non produce alcun risultato.

È ora possibile utilizzare il client EC2 Instance Connect basato su browser per connettersi all'istanza.

Ubuntu

Per risolvere l'errore di convalida della chiave host non riuscito su un'istanza Ubuntu

1. Connettiti all'istanza tramite SSH.

   È possibile connettersi utilizzando la CLI EC2 Instance Connect oppure tramite la coppia di chiavi SSH assegnata all'istanza al momento dell'avvio e il nome utente predefinito dell'AMI utilizzata per avviare l'istanza. Per Ubuntu, il nome utente predefinito è `ubuntu`.

   Ad esempio, se l'istanza è stata avviata tramite Ubuntu, il suo nome DNS pubblico è `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` e la coppia di chiavi è `my_ec2_private_key.pem`, utilizzare il comando seguente per accedere all'istanza tramite SSH:

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

   Per ulteriori informazioni sulla connessione all'istanza, consulta Connessione all'istanza Linux tramite un client SSH.

2. Accedere alla cartella:

```
[ec2-user ~]$ cd /usr/share/ec2-instance-connect/
```

3. Eseguire il seguente comando sull'istanza.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Si noti che una chiamata riuscita non produce alcun risultato.

È ora possibile utilizzare il client EC2 Instance Connect basato su browser per connettersi all'istanza.

Impossibile connettersi all'istanza Ubuntu tramite EC2 Instance Connect

Se utilizzi EC2 Instance Connect per connetterti all'istanza Ubuntu e visualizzi un errore durante il tentativo di connessione, puoi utilizzare le seguenti informazioni per provare a risolvere il problema.

Possibile causa

Il pacchetto `ec2-instance-connect` sull'istanza non è la versione più recente.

Soluzione

Aggiorna il pacchetto `ec2-instance-connect` sull'istanza alla versione più recente, come segue:

1. Collegati all'istanza utilizzando un metodo diverso da EC2 Instance Connect.
2. Esegui il comando seguente sull'istanza per aggiornare alla versione più recente il pacchetto `ec2-instance-connect`.

```
apt update && apt upgrade
```

Ho perso la mia chiave privata. Come posso connettermi alla mia istanza?

Se perdi la chiave privata per un' EBS-backed istanza, puoi riottenere l'accesso alla tua istanza. Arrestare l'istanza, distaccarne il volume root e collegarlo a un'altra istanza come volume dati, modificare il file `authorized_keys` con una nuova chiave pubblica, riportare il volume all'istanza originale e riavviare l'istanza. Per ulteriori informazioni sull'avvio, la connessione e l'arresto delle istanze, consulta Cambio di stato di un'istanza Amazon EC2.

Questa procedura è supportata solo per le istanze con volumi root EBS. Se l'istanza ha un volume root dell'archivio dell'istanza, non puoi utilizzare questa procedura per riconquistare l'accesso all'istanza; è necessario disporre della chiave privata per connettersi all'istanza. Per determinare il tipo di volume root dell'istanza, apri la console Amazon EC2, scegli Istanze, seleziona l'istanza, scegli la scheda Archiviazione e nella sezione Dettagli del dispositivo root controlla il valore Tipo di dispositivo root.

Il valore è `EBS` o `INSTANCE-STORE`.

In aggiunta ai passaggi seguenti, esistono altri modi per connettersi all'istanza Linux in caso di perdita della chiave privata. Per ulteriori informazioni, consulta Come posso connettermi alla mia istanza Amazon EC2 se ho perso la mia coppia di chiavi SSH dopo il suo avvio iniziale?

Passaggi per connettersi a un' EBS-backed istanza con una coppia di chiavi diversa

- Fase 1: creazione di una nuova coppia di chiavi
- Fase 2: Ottenere informazioni sull'istanza originale e il relativo volume radice
- Fase 3: Arrestare l'istanza originale
- Fase 4: Avviare un'istanza temporanea
- Fase 5: scollegare il volume radice dall'istanza originale e collegarlo all'istanza temporanea
- Passaggio 6: aggiungi la nuova chiave pubblica a authorized_keys sul volume originale montato sull'istanza temporanea
- Fase 7: smontare e scollegare il volume originale dall'istanza temporanea e ricollegarlo all'istanza originale
- Fase 8: connettersi all'istanza originale utilizzando la nuova coppia di chiavi
- Fase 9: pulizia

Fase 1: creazione di una nuova coppia di chiavi

Creare una nuova coppia di chiavi tramite la console Amazon EC2 o uno strumento di terza parte. Se si vuole assegnare alla nuova coppia di chiavi lo stesso nome della chiave privata persa, bisogna prima eliminare la coppia di chiavi esistente. Per informazioni su come creare una coppia di chiavi, consulta Creazione di una coppia di chiavi utilizzando Amazon EC2 o Creazione di una coppia di chiavi tramite uno strumento di terza parte e importazione della chiave pubblica in Amazon EC2.

Fase 2: Ottenere informazioni sull'istanza originale e il relativo volume radice

Prendere nota delle seguenti informazioni perché sono necessarie per completare questa procedura.

Per ottenere informazioni sull'istanza originale

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza a cui ci si vuole connettere. (Ci si riferirà a questa come istanza originale).
3. Nella scheda Details (Dettagli), prendere nota dell'ID istanza e dell'ID AMI.
4. Nella scheda Networking (Reti), prendere nota della zona di disponibilità.
5. Nella scheda Storage (Archiviazione), sotto Root device name (Nome dispositivo root) annotare il nome del dispositivo per il volume root (ad esempio `/dev/xvda`). Quindi, trova il nome di questo dispositivo in Block devices (Dispositivi a blocchi) e annota l'ID volume (ad esempio, vol-0a1234b5678c910de).

Fase 3: Arrestare l'istanza originale

Scegli Instance state (Stato istanza), Stop instance (Arresta istanza). Se questa opzione è disabilitata, l'istanza è già arrestata oppure il suo volume root è un volume di archivio dell'istanza.

> **Warning**
>
> Quando si arresta un'istanza, i dati sui volumi dell'archivio delle istanze vengono persi. Per preservare questi dati, esegui il backup su uno storage persistente.

Fase 4: Avviare un'istanza temporanea

Per avviare un'istanza temporanea

1. Nel riquadro di navigazione, selezionare Instances (Istanze), quindi selezionare Launch Instance (Avvia istanza).
2. Nella sezione Name and tags (Nome e tag), per Name (Nome) inserisci Temporary.
3. Nella sezione Application and OS Images (Immagini di applicazioni e sistema operativo), seleziona la stessa AMI utilizzata per avviare l'istanza originale. Se questa AMI non è disponibile, è possibile creare un'AMI che può essere utilizzata dall'istanza arrestata. Per ulteriori informazioni, consulta Crea un' EBS-backed AMI Amazon.
4. Nella sezione Instance type (Tipo di istanza), mantieni il tipo di istanza di default.

5. Nella sezione Key pair (Coppia di chiavi), per Key pair name (Nome della coppia di chiavi) seleziona una coppia di chiavi esistente o creane una nuova.
6. Nella sezione Network settings (Impostazioni di rete), scegli Edit (Modifica), quindi per Subnet (Sottorete) seleziona una sottorete nella stessa zona di disponibilità dell'istanza originale.
7. Nel pannello Summary (Riepilogo), scegli Launch (Avvia).

Fase 5: scollegare il volume radice dall'istanza originale e collegarlo all'istanza temporanea

1. Nel riquadro di navigazione, scegli Volumi, quindi seleziona il volume root per l'istanza originale (hai annotato l'ID del volume in un passaggio precedente). Scegli Actions (Operazioni), Detach volume (Scollega volume), quindi scegli Detach (Scollega). Attendere che lo stato del volume diventi `available`. (Potrebbe essere necessario scegliere l'icona Refresh (Aggiorna)).
2. Con il volume ancora selezionato, scegli Actions (Operazioni), quindi scegli Attach volume (Collega volume). Seleziona l'ID istanza dell'istanza temporanea, prendi nota del nome del dispositivo specificato sotto Device name (Nome del dispositivo), ad esempio `/dev/sdf`, quindi scegli Attach volume (Collega volume).

> **Note**
>
> Se hai avviato l'istanza originale da un' Marketplace AWS AMI e il volume contiene Marketplace AWS codici, devi prima interrompere l'istanza temporanea prima di poter collegare il volume.

Passaggio 6: aggiungi la nuova chiave pubblica a **`authorized_keys`** sul volume originale montato sull'istanza temporanea

1. Connettersi all'istanza temporanea.
2. Dall'istanza temporanea, montare il volume collegato all'istanza in modo da poter accedere al file system. Ad esempio, se il nome del dispositivo è `/dev/sdf`, utilizzare i seguenti comandi per montare il volume come `/mnt/tempvol`.

> **Note**
>
> Il nome del dispositivo potrebbe apparire in modo diverso nell'istanza. Ad esempio, i dispositivi montati come `/dev/sdf` potrebbero essere visualizzati come `/dev/xvdf` nell'istanza. Alcune versioni di Red Hat (o le relative varianti, come CentOS), potrebbero anche aggiungere alla lettera finale 4 caratteri, in modo che `/dev/sdf` diventi `/dev/xvdk`.

a. Utilizzare il comando lsblk per determinare se il volume è partizionato.

```
[ec2-user ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0    8G  0 disk
##xvda1 202:1    0    8G  0 part /
xvdf    202:80   0  101G  0 disk
##xvdf1 202:81   0  101G  0 part
xvdg    202:96   0   30G  0 disk
```

Nell'esempio precedente, `/dev/xvda` e `/dev/xvdf` sono volumi partizionati, mentre `/dev/xvdg` non lo è. Se il volume è partizionato, montare la partizione (`/dev/xvdf1`) invece del dispositivo raw (`/dev/xvdf`) nelle fasi successive.

b. Creare una directory temporanea per montare il volume.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

c. Montare il volume (o la partizione) nel punto di montaggio temporaneo, utilizzando il nome del volume o del dispositivo identificato in precedenza. Il comando necessario dipende dal file system del sistema operativo. Nota: il nome del dispositivo potrebbe apparire in modo diverso nell'istanza. Per ulteriori informazioni, consulta la sezione note nel passaggio 6.

- Amazon Linux, Ubuntu e Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 e RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Se si riceve un errore che indica che il file system è corrotto, eseguire il seguente comando per utilizzare l'utilità fsck per controllare il file system e risolvere qualsiasi guasto:
>
> ```
> [ec2-user ~]$ sudo fsck /dev/xvdf1
> ```

3. Dall'istanza temporanea, utilizzare il seguente comando per aggiornare `authorized_keys` nel volume montato con la nuova chiave pubblica da `authorized_keys` per l'istanza temporanea.

> **Important**
>
> Gli esempi seguenti utilizzano il nome utente di Amazon Linux `ec2-user`. Potrebbe essere necessario sostituire un nome utente diverso, ad esempio `ubuntu` per le istanze di Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Se la copia ha avuto successo, è possibile passare alla fase successiva.

(Facoltativo) Altrimenti, se non si ha il permesso di modificare i file in `/mnt/tempvol`, sarà necessario aggiornare il file utilizzando sudo, quindi occorrerà controllare le autorizzazioni sul file per verificare di poter accedere all'istanza originale. Utilizzare il comando seguente per verificare le autorizzazioni per il file:

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

In questo output di esempio, *222* è l'ID utente e *500* l'ID del gruppo. Quindi, utilizzare sudo per eseguire nuovamente il comando di copia non riuscito.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Eseguire nuovamente il comando seguente per stabilire se le autorizzazioni sono state modificate.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Se l'ID utente e l'ID gruppo sono stati modificati, utilizzare il seguente comando per ripristinarli.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Fase 7: smontare e scollegare il volume originale dall'istanza temporanea e ricollegarlo all'istanza originale

1. Dall'istanza temporanea, smontare il volume collegato all'istanza in modo da ricollegarlo all'istanza originale. Ad esempio, utilizzare il seguente comando per smontare il volume in `/mnt/tempvol`.

   ```
   [ec2-user ~]$ sudo umount /mnt/tempvol
   ```

2. Scollega il volume dall'istanza temporanea (l'hai smontato nel passaggio precedente): dalla console Amazon EC2, scegli Volumi nel riquadro di navigazione, seleziona il volume root per l'istanza originale (hai annotato l'ID del volume in un passaggio precedente), scegli Azioni, Scollega volume, quindi scegli Scollega. Attendere che lo stato del volume diventi `available`. (Potrebbe essere necessario scegliere l'icona Refresh (Aggiorna)).
3. Ricollega il volume all'istanza originale: con il volume ancora selezionato, scegli Actions (Operazioni), Attach volume (Collega volume). Seleziona l'ID dell'istanza originale, specifica il nome del dispositivo annotato in precedenza nel Passaggio 2 per il collegamento del volume root originale (`/dev/sda1` o `/dev/xvda`), quindi scegli Collega volume.

   > **Important**
   >
   > Se non si specifica lo stesso nome del dispositivo dell'allegato originale, non è possibile avviare l'istanza originale. Amazon EC2 prevede il volume root su `sda1` o `/dev/xvda`.

Fase 8: connettersi all'istanza originale utilizzando la nuova coppia di chiavi

Seleziona l'istanza originale, scegli Instance state (Stato istanza), Start instance (Avvia istanza). Dopo che l'istanza acquisisce lo stato `running`, è possibile connettersi a essa tramite il file della chiave privata per la nuova coppia di chiavi.

> **Note**
>
> Se il nome della nuova coppia di chiavi e del corrispondente file di chiave privata è diverso dal nome della coppia di chiavi originale, assicurarsi di specificare il nome del nuovo file della chiave privata quando ci si connette all'istanza.

Fase 9: pulizia

(Facoltativo) È possibile terminare l'istanza temporanea se non la si utilizza più. Selezionare l'istanza temporanea e scegliere Stato istanza, Termina (elimina) istanza.

Risoluzione dei problemi relativi alle istanze Amazon EC2 Linux con esito negativo delle verifiche dello stato

Le seguenti informazioni possono essere utili per risolvere i problemi se l'istanza Linux non supera una verifica dello stato. Determina innanzitutto se le applicazioni in uso presentano dei problemi. Se risulta che l'istanza non esegue le applicazioni come previsto, esamina le informazioni di verifica dello stato e i log di sistema.

Per vedere degli esempi di problemi che causano il mancato superamento dei controlli dello stato, vedere Verifiche dello stato delle istanze Amazon EC2.

Indice

- Esame delle informazioni di verifica dello stato
- Recupero dei log di sistema
- Risoluzione degli errori del log di sistema per le istanze Linux
- Out of memory: kill process
- ERROR: mmu_update failed (aggiornamento della gestione della memoria non riuscito)
- I/O errore (errore del dispositivo di blocco)

- I/O ERRORE: né disco locale né remoto (dispositivo a blocchi distribuiti danneggiato)
- request_module: runaway loop modprobe (looping del modprobe del kernel legacy sulle versioni precedenti di Linux)
- "FATAL: kernel too old" e "fsck: No such file or directory while trying to open /dev" (mancata corrispondenza di kernel e AMI)
- «IRREVERSIBILE: impossibile caricare/lib/modules" o BusyBox "(moduli del kernel mancanti)
- ERROR Invalid kernel (kernel non compatibile con EC2)
- fsck: No such file or directory while trying to open... file system non trovato
- General error mounting filesystems (errore di montaggio)
- VFS: Unable to mount root fs on unknown-block (mancata corrispondenza del file system root)
- Errore: impossibile determinare il major/minor numero di dispositivo root... (Mancata system/device corrispondenza del file principale)
- XENBUS: Device with no driver...
- ... days without being checked, check forced (verifica del file system richiesta)
- fsck died with exit status... (dispositivo mancante)
- Prompt di GRUB (grubdom>)
- Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (indirizzo MAC) Hard-coded
- Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (configurazione SELinux errata)
- XENBUS: Timeout connecting to devices (timeout di Xenbus)

Esame delle informazioni di verifica dello stato

Per analizzare le istanze danneggiate utilizzando la console di Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Instances (Istanze) e seleziona l'istanza desiderata.
3. Seleziona la scheda Stato e allarmi per visualizzare i risultati individuali di tutte le Verifiche dello stato del sistema, le Verifiche dello stato delle istanze e le Verifiche dello stato per EBS collegato.

Se una verifica dello stato ha avuto esito negativo, provare una delle seguenti opzioni:

- Creare un allarme per ripristinare l'istanza in risposta alla verifica dello stato con esito negativo. Per ulteriori informazioni, consulta Creazione di allarmi che arrestano, terminano, riavviano o recuperano un'istanza.
- (Controlli dello stato dell'istanza) Se hai cambiato il tipo di istanza in un'Nitro-based istanza, i controlli di stato hanno esito negativo se hai eseguito la migrazione da un'istanza che non dispone dei driver ENA e NVMe richiesti. Per ulteriori informazioni, consulta Compatibilità per la modifica del tipo di istanza.
- Per un'istanza con un volume root EBS, arresta e riavvia l'istanza. Per ulteriori informazioni, consulta Avvio e arresto di un'istanza Amazon EC2.
- Per un'istanza con un volume root dell'archivio dell'istanza, termina l'istanza e avviane una sostitutiva. Per ulteriori informazioni, consulta Terminare le istanze Amazon EC2.
- Attendere che Amazon EC2 risolva il problema.
- Contatta Supporto o pubblica il problema su re:POST. AWS
- Se l'istanza si trova in un gruppo Auto Scaling:
  - (Verifiche dello stato del sistema e verifiche dello stato delle istanze) Per impostazione predefinita, Amazon EC2 Auto Scaling avvia automaticamente un'istanza sostitutiva. Per ulteriori informazioni, consulta Controllo dell'integrità per istanze in un gruppo Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.
  - (Verifiche dello stato per EBS collegato) È necessario configurare Amazon EC2 Auto Scaling per avviare automaticamente un'istanza sostitutiva. Per ulteriori informazioni, consulta Monitorare e sostituire le istanze di Auto Scaling con volumi Amazon EBS danneggiati nella Guida per l'utente di Amazon EC2 Auto Scaling.
- Recuperare il log di sistema e individuare eventuali errori. Per ulteriori informazioni, consulta Recupero dei log di sistema.

Recupero dei log di sistema

Se la verifica dello stato di un'istanza ha esito negativo, è possibile riavviare l'istanza e recuperare i log di sistema. Questi log possono rivelare la presenza di un errore che può aiutare a risolvere il problema. Il riavvio elimina le informazioni inutili dai log.

Per riavviare un'istanza e recuperare il log di sistema

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione scegliere Instances (Istanze) e selezionare l'istanza desiderata.

3. Scegliere Instance state (Stato istanza), Reboot instance (Riavvia istanza). Per il riavvio dell'istanza possono essere necessari alcuni minuti.
4. Verificare se il problema è ancora presente; talvolta il riavvio consente di risolvere il problema.
5. Quando l'istanza è in stato `running`, selezionare Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), Get system log (Ottieni il log di sistema).
6. Esaminare il log visualizzato e utilizzare l'elenco delle dichiarazioni di errore note del log di sistema per risolvere il problema.
7. Se la problematica non si risolve, puoi pubblicare un post relativo a tale problematica su AWS re:Post.

Risoluzione degli errori del log di sistema per le istanze Linux

Per le istanze Linux che non hanno superato la verifica dello stato, come ad esempio la verifica di raggiungibilità dell'istanza, accertarsi di avere seguito le fasi di cui sopra per recuperare il log di sistema. L'elenco seguente contiene alcuni errori comuni del log di sistema e suggerisce alcune operazioni che potrebbero risolvere il problema di ogni errore.

Errori di memoria

- Out of memory: kill process
- ERROR: mmu_update failed (aggiornamento della gestione della memoria non riuscito)

Errori dei dispositivi

- I/O errore (errore del dispositivo di blocco)
- I/O ERRORE: né disco locale né remoto (dispositivo a blocchi distribuiti danneggiato)

Errori del kernel

- request_module: runaway loop modprobe (looping del modprobe del kernel legacy sulle versioni precedenti di Linux)
- "FATAL: kernel too old" e "fsck: No such file or directory while trying to open /dev" (mancata corrispondenza di kernel e AMI)
- «IRREVERSIBILE: impossibile caricare/lib/modules" o BusyBox "(moduli del kernel mancanti)
- ERROR Invalid kernel (kernel non compatibile con EC2)

Errori del file system

- fsck: No such file or directory while trying to open... file system non trovato
- General error mounting filesystems (errore di montaggio)
- VFS: Unable to mount root fs on unknown-block (mancata corrispondenza del file system root)
- Errore: impossibile determinare il major/minor numero di dispositivo root... (Mancata system/device corrispondenza del file principale)
- XENBUS: Device with no driver...
- ... days without being checked, check forced (verifica del file system richiesta)
- fsck died with exit status... (dispositivo mancante)

Errori del sistema operativo

- Prompt di GRUB (grubdom>)
- Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (indirizzo MAC) Hard-coded
- Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (configurazione SELinux errata)
- XENBUS: Timeout connecting to devices (timeout di Xenbus)

Out of memory: kill process

Un errore di memoria insufficiente viene indicato da una voce del log di sistema simile a quella mostrata sotto.

```
[115879.769795] Out of memory: kill process 20273 (httpd) score 1285879
or a child
[115879.769795] Killed process 1917 (php-cgi) vsz:467184kB, anon-
rss:101196kB, file-rss:204kB
```

Causa potenziale

Memoria esaurita

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Esegui una delle seguenti operazioni: • Arrestare l'istanza e modificarla per utilizzar ne un tipo diverso, quindi avviare nuovament e l'istanza. Ad esempio un tipo di istanza più grande o ottimizzata per la memoria. • Riavviare l'istanza affinché torni a uno stato non danneggiato. Se non si cambia il tipo di istanza, probabilmente il problema si ripeterà.
Supportata da instance store	Scegliere una delle seguenti operazioni: • Terminare l'istanza e avviarne una nuova, specificando un tipo di istanza diverso. Ad esempio un tipo di istanza più grande o ottimizzata per la memoria. • Riavviare l'istanza affinché torni a uno stato non danneggiato. Se non si cambia il tipo di istanza, probabilmente il problema si ripeterà.

ERROR: mmu_update failed (aggiornamento della gestione della memoria non riuscito)

Gli errori relativi all'aggiornamento della gestione della memoria sono indicati da una voce del log di sistema simile alla seguente:

```
...
Press `ESC' to enter the menu... 0   [H[J  Booting 'Amazon Linux 2011.09
 (2.6.35.14-95.38.amzn1.i686)'


root (hd0)

 Filesystem type is ext2fs, using whole disk
```

```
kernel /boot/vmlinuz-2.6.35.14-95.38.amzn1.i686 root=LABEL=/ console=hvc0 LANG=

en_US.UTF-8 KEYTABLE=us

initrd /boot/initramfs-2.6.35.14-95.38.amzn1.i686.img

ERROR: mmu_update failed with rc=-22
```

Causa potenziale

Problema con Amazon Linux

Operazione suggerita

Pubblica il tuo problema u AWS re:Post o contatta Supporto.

I/O errore (errore del dispositivo di blocco)

Un input/output errore è indicato da una voce del registro di sistema simile all'esempio seguente:

```
[9943662.053217] end_request: I/O error, dev sde, sector 52428288
[9943664.191262] end_request: I/O error, dev sde, sector 52428168
[9943664.191285] Buffer I/O error on device md0, logical block 209713024
[9943664.191297] Buffer I/O error on device md0, logical block 209713025
[9943664.191304] Buffer I/O error on device md0, logical block 209713026
[9943664.191310] Buffer I/O error on device md0, logical block 209713027
[9943664.191317] Buffer I/O error on device md0, logical block 209713028
[9943664.191324] Buffer I/O error on device md0, logical block 209713029
[9943664.191332] Buffer I/O error on device md0, logical block 209713030
[9943664.191339] Buffer I/O error on device md0, logical block 209713031
[9943664.191581] end_request: I/O error, dev sde, sector 52428280
[9943664.191590] Buffer I/O error on device md0, logical block 209713136
[9943664.191597] Buffer I/O error on device md0, logical block 209713137
[9943664.191767] end_request: I/O error, dev sde, sector 52428288
[9943664.191970] end_request: I/O error, dev sde, sector 52428288
[9943664.192143] end_request: I/O error, dev sde, sector 52428288
[9943664.192949] end_request: I/O error, dev sde, sector 52428288
[9943664.193112] end_request: I/O error, dev sde, sector 52428288
[9943664.193266] end_request: I/O error, dev sde, sector 52428288
...
```

Cause potenziali

Tipo di istanza	Causa potenziale
Amazon EBS-backed	Un volume Amazon EBS in stato di errore
Supportata da instance store	Un'unità fisica in stato di errore

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Attenersi alla seguente procedura: 1. Arrestare l'istanza. 2. Distaccare il volume. 3. Tentare di ripristinare il volume. **Note** È buona norma eseguire spesso una snapshot dei volumi Amazon EBS per ridurre notevolmente il rischio di perdite di dati dovuti a guasti. 4. Re-attach il volume dell'istanza. 5. Avviare l'istanza.
Supportata da instance store	Terminare l'istanza e avviarne una nuova. **Note** Non è possibile ripristinare i dati. Eseguire il ripristino dai backup.

Per questo tipo di istanza	Esegui questa operazione
	Note Per i backup, è buona norma utilizzare Amazon S3 o Amazon EBS. I volumi instance store sono legati direttamente agli errori dei singoli host e dei singoli dischi.

I/O ERRORE: né disco locale né remoto (dispositivo a blocchi distribuiti danneggiato)

Un input/output errore sul dispositivo è indicato da una voce del registro di sistema simile all'esempio seguente:

```
...
block drbd1: Local IO failed in request_timer_fn. Detaching...

Aborting journal on device drbd1-8.

block drbd1: IO ERROR: neither local nor remote disk

Buffer I/O error on device drbd1, logical block 557056

lost page write due to I/O error on drbd1

JBD2: I/O error detected when updating journal superblock for drbd1-8.
```

Cause potenziali

Tipo di istanza	Causa potenziale
Amazon EBS-backed	Un volume Amazon EBS in stato di errore
Supportata da instance store	Un'unità fisica in stato di errore

Operazione suggerita

Terminare l'istanza e avviarne una nuova.

Per un' EBS-backed istanza Amazon, puoi recuperare i dati da un'istantanea recente creando un'immagine da essa. I dati eventualmente aggiunti dopo la snapshot non possono essere ripristinati.

request_module: runaway loop modprobe (looping del modprobe del kernel legacy sulle versioni precedenti di Linux)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto. L'utilizzo di un kernel Linux instabile o datato (ad esempio 2.6.16-xenU) può causare una condizione di loop interminabile all'avvio.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007

BIOS-provided physical RAM map:

 Xen: 0000000000000000 - 0000000026700000 (usable)

0MB HIGHMEM available.
...

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c
```

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Usa un kernel più recente, GRUB-based sia esso statico, usando una delle seguenti opzioni:

Per questo tipo di istanza	Esegui questa operazione
	Opzione 1: terminare l'istanza e avviarne una nuova, specificando i parametri `-kernel` e `-ramdisk`. Opzione 2: 1. Arrestare l'istanza. 2. Modificare gli attributi di kernel e ramdisk per utilizzare un kernel più recente. 3. Avviare l'istanza.
Supportata da instance store	Terminare l'istanza e avviarne una nuova, specificando i parametri `-kernel` e `-ramdisk`.

"FATAL: kernel too old" e "fsck: No such file or directory while trying to open /dev" (mancata corrispondenza di kernel e AMI)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
Linux version 2.6.16.33-xenU (root@dom0-0-50-45-1-a4-ee.z-2.aes0.internal)
(gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #2 SMP Wed Aug 15 17:27:36 SAST 2007
...
FATAL: kernel too old
Kernel panic - not syncing: Attempted to kill init!
```

Cause potenziali

Kernel e userland non compatibili

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Attenersi alla seguente procedura:

Per questo tipo di istanza	Esegui questa operazione
	1. Arrestare l'istanza. 2. Modificare la configurazione per utilizzare un kernel più recente. 3. Avviare l'istanza.
Supportata da instance store	Attenersi alla seguente procedura: 1. Creare un'AMI che utilizza un kernel più recente. 2. Terminare l'istanza. 3. Avviare una nuova istanza dall'AMI creata.

«IRREVERSIBILE: impossibile caricare/lib/modules" o BusyBox "(moduli del kernel mancanti)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
[    0.370415] Freeing unused kernel memory: 1716k freed
Loading, please wait...
WARNING: Couldn't open directory /lib/modules/2.6.34-4-virtual: No such file or
 directory
FATAL: Could not open /lib/modules/2.6.34-4-virtual/modules.dep.temp for writing: No
 such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Couldn't get a file descriptor referring to the console
Begin: Loading essential drivers... ...
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Done.
Begin: Running /scripts/init-premount ...
Done.
Begin: Mounting root file system... ...
Begin: Running /scripts/local-top ...
Done.
```

```
Begin: Waiting for root file system... ...
Done.
Gave up waiting for root device.  Common problems:
 - Boot args (cat /proc/cmdline)
   - Check rootdelay= (did the system wait long enough?)
   - Check root= (did the system wait for the right device?)
 - Missing modules (cat /proc/modules; ls /dev)
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
ALERT! /dev/sda1 does not exist. Dropping to a shell!


BusyBox v1.13.3 (Ubuntu 1:1.13.3-1ubuntu5) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(initramfs)
```

Cause potenziali

Questo problema può essere causato da una o più delle condizioni seguenti:

- Ramdisk mancante
- Moduli corretti mancanti nel ramdisk
- Volume root Amazon EBS non collegato correttamente come `/dev/sda1`

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Attenersi alla seguente procedura: 1. Selezionare il ramdisk corretto per il volume Amazon EBS. 2. Arrestare l'istanza. 3. Distaccare il volume e ripararlo. 4. Collegare il volume all'istanza. 5. Avviare l'istanza.

Per questo tipo di istanza	Esegui questa operazione
	6. Modificare l'AMI per utilizzare il ramdisk corretto;
Supportata da instance store	Attenersi alla seguente procedura: 1. Terminare l'istanza e avviarne una nuova con il ramdisk corretto. 2. Creare una nuova AMI con il ramdisk corretto.

ERROR Invalid kernel (kernel non compatibile con EC2)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
...
root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz root=/dev/sda1 ro

initrd /initrd.img

ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

  Booting 'Fallback'

root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz.old root=/dev/sda1 ro

Error 15: File not found
```

Cause potenziali

Questo problema può essere causato da una o entrambe le condizioni seguenti:

- Il kernel fornito non è supportato da GRUB
- Il kernel di fallback non esiste

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Attenersi alla seguente procedura: 1. Arrestare l'istanza. 2. Sostituire con un kernel funzionante. 3. Installare un kernel di fallback. 4. Modificare l'AMI correggendo il kernel.
Supportata da instance store	Attenersi alla seguente procedura: 1. Terminare l'istanza e avviarne una nuova con il kernel corretto. 2. Creare un'AMI con il kernel corretto. 3. (Opzionale) Richiedere assistenza tecnica per il ripristino dei dati tramite Supporto.

fsck: No such file or directory while trying to open... file system non trovato

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
  Welcome to Fedora
  Press 'I' to enter interactive startup.
Setting clock : Wed Oct 26 05:52:05 EDT 2011 [  OK  ]

Starting udev: [  OK  ]

Setting hostname localhost:  [  OK  ]
```

```
No devices found
Setting up Logical Volume Management: File descriptor 7 left open
  No volume groups found
[  OK  ]

Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1: clean, 82081/1310720 files, 2141116/2621440 blocks
[/sbin/fsck.ext3 (1) -- /mnt/dbbackups] fsck.ext3 -a /dev/sdh
fsck.ext3: No such file or directory while trying to open /dev/sdh

/dev/sdh:
The superblock could not be read or does not describe a correct ext2
filesystem.  If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>

[FAILED]


*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue):
```

Cause potenziali

- Esiste un bug nelle definizioni del file system ramdisk/etc/fstab
- Definizioni di file system non configurate correttamente in/etc/fstab
- Missing/failed unità

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Attenersi alla seguente procedura:

Per questo tipo di istanza	Esegui questa operazione
	1. Arresta l'istanza, scollega il volume principal e repair/modify /etc/fstab il volume, collega il volume all'istanza e avvia l'istanza. 2. Correggi ramdisk per includere la modifica/etc/fstab (se applicabile). 3. Modificare l'AMI per utilizzare un ramdisk più recente. Il sesto campo nel file fstab definisce i requisiti di disponibilità del punto di montaggio (un valore diverso da zero implica l'esecuzione di un fsck su quel volume che deve avere esito positivo). L'uso di questo campo può risultare problematico in Amazon EC2 in quanto un errore solitamente comporta un prompt interatti vo della console che non è correntemente disponibile in Amazon EC2. Prestare attenzione a questa caratteristica e leggere la pagina man di Linux relativa al file fstab.
Supportata da instance store	Attenersi alla seguente procedura: 1. Terminare l'istanza e avviarne una nuova. 2. Distaccare eventuali volumi Amazon EBS errati e riavviare l'istanza. 3. (Opzionale) Richiedere assistenza tecnica per il ripristino dei dati tramite Supporto.

General error mounting filesystems (errore di montaggio)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
Loading xenblk.ko module
xen-vbd: registered block device major 8
```

```
Loading ehci-hcd.ko module
Loading ohci-hcd.ko module
Loading uhci-hcd.ko module
USB Universal Host Controller Interface driver v3.0

Loading mbcache.ko module
Loading jbd.ko module
Loading ext3.ko module
Creating root device.
Mounting root filesystem.
kjournald starting.  Commit interval 5 seconds

EXT3-fs: mounted filesystem with ordered data mode.

Setting up other filesystems.
Setting up new root fs
no fstab.sys, mounting internal defaults
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
mountall:/proc: unable to mount: Device or resource busy
mountall:/proc/self/mountinfo: No such file or directory
mountall: root filesystem isn't mounted
init: mountall main process (221) terminated with status 1

General error mounting filesystems.
A maintenance shell will now be started.
CONTROL-D will terminate this shell and re-try.
Press enter for maintenance
(or type Control-D to continue):
```

Cause potenziali

Tipo di istanza	Causa potenziale
Amazon EBS-backed	• Volume Amazon EBS distaccato o in stato di errore. • File system danneggiato.

Tipo di istanza	Causa potenziale
	• Combinazione di ramdisk e AMI non corrispondente (ad esempio, ramdisk Debian con AMI SUSE).
Supportata da instance store	• Unità in stato di errore. • File system danneggiato. • Combinazione di ramdisk e AMI non corrispondente (ad esempio, ramdisk Debian con AMI SUSE).

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Attenersi alla seguente procedura: 1. Arrestare l'istanza. 2. Distaccare il volume root. 3. Collegare il volume root a un'istanza funzionante nota. 4. Esegui il controllo del file system (fsck -a /dev/...). 5. Correggere eventuali errori. 6. Distaccare il volume dall'istanza funzionante nota. 7. Collegare il volume all'istanza arrestata. 8. Avviare l'istanza. 9. Verificare di nuovo lo stato dell'istanza.
Supportata da instance store	Provare con una delle seguenti operazioni: • Avviare una nuova istanza.

Per questo tipo di istanza	Esegui questa operazione
	• (Opzionale) Richiedere assistenza tecnica per il ripristino dei dati tramite Supporto.

VFS: Unable to mount root fs on unknown-block (mancata corrispondenza del file system root)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
 20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
Kernel command line:  root=/dev/sda1 ro 4
...
Registering block device major 8
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1)
```

Cause potenziali

Tipo di istanza	Causa potenziale
Amazon EBS-backed	• Dispositivo non collegato correttamente. • Dispositivo root non collegato al punto corretto. • File system non nel formato previsto. • Uso del kernel legacy (come 2.6.16-XenU). • Aggiornamento recente del kernel sull'istanza (aggiornamento errato o bug dell'aggiornamento).
Supportata da instance store	Errore dei dispositivi hardware.

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Esegui una delle seguenti operazioni: • Arrestare e riavviare l'istanza. • Modifica il volume principale per collegarlo al punto corretto del dispositivo, possibile/dev/sda1invece di/dev/sda. • Arrestare e modificare per usare un kernel moderno. • Per controllare i bug di aggiornamento noti, consultare la documentazione della distribuz ione Linux in uso. Cambiare o reinstallare il kernel.
Supportata da instance store	Terminare l'istanza e avviarne una nuova utilizzando un kernel moderno.

Errore: impossibile determinare il major/minor numero di dispositivo root... (Mancata system/device corrispondenza del file principale)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
...
XENBUS: Device with no driver: device/vif/0
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
```

```
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Cause potenziali

- Driver dispositivi a blocchi virtuali mancante o configurato in modo non corretto
- Conflitto di enumerazione dei dispositivi (sda versus xvda o sda invece di sda1)
- Scelta errata del kernel dell'istanza

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Attenersi alla seguente procedura: 1. Arrestare l'istanza. 2. Distaccare il volume. 3. Correggere il problema di mappatura dei dispositivi. 4. Avviare l'istanza. 5. Modificare l'AMI per risolvere i problemi di mappatura dei dispositivi.
Supportata da instance store	Attenersi alla seguente procedura: 1. Creare una nuova AMI con la soluzione appropriata (mappare correttamente il dispositivo a blocchi). 2. Terminare l'istanza e avviarne una nuova dall'AMI creata.

XENBUS: Device with no driver...

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Cause potenziali

- Driver dispositivi a blocchi virtuali mancante o configurato in modo non corretto
- Conflitto di enumerazione dei dispositivi (sda versus xvda)
- Scelta errata del kernel dell'istanza

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Attenersi alla seguente procedura: 1. Arrestare l'istanza. 2. Distaccare il volume. 3. Correggere il problema di mappatura dei dispositivi. 4. Avviare l'istanza.

Per questo tipo di istanza	Esegui questa operazione
	5. Modificare l'AMI per risolvere i problemi di mappatura dei dispositivi.
Supportata da instance store	Attenersi alla seguente procedura: 1. Creare un'AMI con la soluzione appropria ta (mappare correttamente il dispositivo a blocchi). 2. Terminare l'istanza e avviarne una nuova utilizzando l'AMI creata.

... days without being checked, check forced (verifica del file system richiesta)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
...
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1 has gone 361 days without being checked, check forced
```

Cause potenziali

Il momento della verifica del file system è trascorso; viene forzata una verifica del file system.

Operazioni suggerite

- Attendere il completamento della verifica del file system. Una verifica del file system può richiedere molto tempo a seconda delle dimensioni del file system root.
- Modificare i file system per rimuovere l'applicazione della relativa verifica (fsck) utilizzando tune2fs o strumenti appropriati al file system in uso.

fsck died with exit status... (dispositivo mancante)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
Cleaning up ifupdown....
Loading kernel modules...done.
...
Activating lvm and md swap...done.
Checking file systems...fsck from util-linux-ng 2.16.2
/sbin/fsck.xfs: /dev/sdh does not exist
fsck died with exit status 8
[31mfailed (code 8).[39;49m
```

Cause potenziali

- Ramdisk in cerca di unità mancante
- Verifica di consistenza del file system forzata
- Unità in stato di errore o distaccata

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Tentare una o più delle operazioni seguenti per risolvere il problema: • Arrestare l'istanza e collegare il volume a un'istanza in esecuzione esistente. • Eseguire manualmente le verifiche di coerenza. • Correggere il ramdisk per includere le utility pertinenti. • Modificare i parametri di ottimizzazione del file system per rimuovere i requisiti di coerenza (operazione non consigliata).
Supportata da instance store	Tentare una o più delle operazioni seguenti per risolvere il problema: • Ricompilare il ramdisk con gli strumenti corretti.

Per questo tipo di istanza	Esegui questa operazione
	• Modificare i parametri di ottimizzazione del file system per rimuovere i requisiti di coerenza (operazione non consigliata). • Terminare l'istanza e avviarne una nuova. • (Opzionale) Richiedere assistenza tecnica per il ripristino dei dati tramite Supporto.

Prompt di GRUB (grubdom>)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
    GNU GRUB  version 0.97  (629760K lower / 0K upper memory)

       [ Minimal BASH-like line editing is supported.   For

         the   first   word,  TAB  lists  possible  command

         completions.  Anywhere else TAB lists the possible

         completions of a device/filename. ]

grubdom>
```

Cause potenziali

Tipo di istanza	Cause potenziali
Amazon EBS-backed	• File di configurazione GRUB mancante. • Utilizzata immagine GRUB errata, in attesa di file di configurazione GRUB in un percorso diverso. • Usato file system non supportato per archiviare il file di configurazione GRUB (ad esempio, conversione del file system root in

Tipo di istanza	Cause potenziali
	un tipo non supportato da una precedente versione di GRUB).
Supportata da instance store	• File di configurazione GRUB mancante. • Utilizzata immagine GRUB errata, in attesa di file di configurazione GRUB in un percorso diverso. • Usato file system non supportato per archiviare il file di configurazione GRUB (ad esempio, conversione del file system root in un tipo non supportato da una precedente versione di GRUB).

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Opzione 1: modificare l'AMI e riavviare l'istanza: 1. Modifica l'AMI sorgente per creare un file di configurazione GRUB nella posizione standard (/boot/grub/menu.lst). 2. Verificare che la versione in uso di GRUB supporti il tipo di file system sottostante e, se necessario, aggiornare GRUB. 3. Scegliere l'immagine GRUB appropriata (hd0-1a unità o hd00 – 1a unità, 1a partizione). 4. Terminare l'istanza e avviarne una nuova utilizzando l'AMI creata. Opzione 2: correggere l'istanza esistente: 1. Arrestare l'istanza.

Per questo tipo di istanza	Esegui questa operazione
	2. Distaccare il file system root. 3. Collegare il file system root a un'istanza funzionante nota. 4. Montare il file system. 5. Creare un file di configurazione GRUB. 6. Verificare che la versione in uso di GRUB supporti il tipo di file system sottostante e, se necessario, aggiornare GRUB. 7. Distaccare il file system. 8. Collegare all'istanza originale. 9. Modificare l'attributo del kernel per utilizzare l'immagine GRUB appropriata (1a unità o 1a partizione sul 1° disco). 10 Avviare l'istanza.

Per questo tipo di istanza	Esegui questa operazione
Supportata da instance store	Opzione 1: modificare l'AMI e riavviare l'istanza: 1. Crea la nuova AMI con un file di configura zione di GRUB nella posizione standard (/// menu.lst). boot/grub 2. Scegliere l'immagine GRUB appropriata (hd0-1a unità o hd00 – 1a unità, 1a partizion e). 3. Verificare che la versione in uso di GRUB supporti il tipo di file system sottostante e, se necessario, aggiornare GRUB. 4. Terminare l'istanza e avviarne una nuova utilizzando l'AMI creata. Opzione 2: terminare l'istanza e avviarne una nuova specificando il kernel corretto. **Note** Per ripristinare i dati dell'istanza esistente, contatta Supporto.

Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (indirizzo MAC) Hard-coded

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
...
Bringing up loopback interface:  [  OK  ]

Bringing up interface eth0:  Device eth0 has different MAC address than expected,
 ignoring.
[FAILED]
```

```
Starting auditd: [  OK  ]
```

Cause potenziali

È presente un MAC con interfaccia hardcoded nella configurazione AMI.

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Esegui una delle seguenti operazioni: • Modificare l'AMI per rimuovere l'impostazione hardcoded e riavviare l'istanza. • Modificare l'istanza per rimuovere l'indirizzo MAC hardcoded. O Attenersi alla seguente procedura: 1. Arrestare l'istanza. 2. Distaccare il volume root. 3. Collegare il volume a un'altra istanza e modificare il volume per rimuovere l'indirizzo MAC hardcoded. 4. Collegare il volume all'istanza originale. 5. Avviare l'istanza.
Supportata da instance store	Scegliere una delle seguenti operazioni: • Modificare l'istanza per rimuovere l'indirizzo MAC hardcoded. • Terminare l'istanza e avviarne una nuova.

Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (configurazione SELinux errata)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
audit(1313445102.626:2): enforcing=1 old_enforcing=0 auid=4294967295
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now.
Kernel panic - not syncing: Attempted to kill init!
```

Cause potenziali

SELinux è stato abilitato per errore:

- Il kernel fornito non è supportato da GRUB
- Il kernel di fallback non esiste

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Attenersi alla seguente procedura: 1. Arrestare l'istanza non riuscita. 2. Distaccare il volume root dell'istanza non riuscita. 3. Collegare il volume root a un'altra istanza Linux in esecuzione (in seguito detta istanza di ripristino). 4. Connettersi all'istanza di ripristino e montare il volume root dell'istanza non riuscita. 5. Disabilitare SELinux sul volume root montato. Questo processo varia a seconda delle distribuzioni Linux; per ulteriori informazioni, consulta la OS-specific documentazione.

Per questo tipo di istanza	Esegui questa operazione
	Note Su alcuni sistemi, per disabilitare SELinux occorre impostare `SELINUX=disabled` nel file `/mount_point/etc/sysconfig/selinux`, dove *mount_point* è la posizione in cui il volume è stato montato sull'istanza di ripristino. 6. Smontare e distaccare il volume root dall'istanza di ripristino e ricollegarlo all'istanza originale. 7. Avviare l'istanza.
Supportata da instance store	Attenersi alla seguente procedura: 1. Terminare l'istanza e avviarne una nuova. 2. (Opzionale) Richiedere assistenza tecnica per il ripristino dei dati tramite Supporto.

XENBUS: Timeout connecting to devices (timeout di Xenbus)

Questa condizione viene indicata da un log di sistema simile a quello mostrato sotto.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
XENBUS: Timeout connecting to devices!
...
Kernel panic - not syncing: No init found.  Try passing init= option to kernel.
```

Cause potenziali

- Il dispositivo a blocchi non è connesso all'istanza
- L'istanza utilizza un kernel datato.

Operazioni suggerite

Per questo tipo di istanza	Esegui questa operazione
Amazon EBS-backed	Esegui una delle seguenti operazioni: • Modificare l'AMI e l'istanza per utilizzare un kernel moderno e riavviare l'istanza. • Riavviare l'istanza.
Supportata da instance store	Scegliere una delle seguenti operazioni: • Terminare l'istanza. • Modificare l'AMI per utilizzare un kernel moderno e avviare una nuova istanza utilizzando questa AMI.

Risoluzione dei problemi relativi all'avvio di un'istanza Amazon EC2 Linux dal volume sbagliato

In alcune situazioni, un volume diverso da quello collegato a `/dev/xvda` o `/dev/sda` diventa il volume root di un'istanza Linux. Questo può succedere se hai collegato il volume root di un'altra istanza o un volume creato dalla snapshot di un volume root a un'istanza con un volume root esistente.

Ciò è dovuto al modo in cui il ramdisk iniziale funziona in Linux: Sceglie il volume definito come `/` nel file `/etc/fstab`, e in alcune distribuzioni; ciò è determinato dall'etichetta collegata alla partizione di volume. Nello specifico, puoi notare che il file `/etc/fstab` si presenta nel modo seguente:

```
LABEL=/ / ext4 defaults,noatime 1 1
tmpfs /dev/shm tmpfs defaults 0 0
```

```
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
```

Se controlli l'etichetta di entrambi i volumi, vedrai che per tutti e due contiene `/`:

```
[ec2-user ~]$ sudo e2label /dev/xvda1
/
[ec2-user ~]$ sudo e2label /dev/xvdf1
/
```

In questo esempio, `/dev/xvdf1` potrebbe diventare il volume root su cui si avvia l'istanza dopo l'esecuzione iniziale del ramdisk, invece del volume `/dev/xvda1` da cui intendevi eseguire l'avvio. Per risolvere questo problema, utilizzare lo stesso comando e2label per modificare l'etichetta del volume collegato dal quale non si desidera eseguire l'avvio.

In alcuni casi, specificare un UUID in `/etc/fstab` può risolvere il problema. Tuttavia, se entrambi i volumi provengono dalla stessa snapshot o se quello secondario viene creato da una snapshot del volume principale, condivideranno un UUID.

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
/dev/xvdf1: LABEL="old/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

Per modificare l'etichetta di un volume ext4 collegato

1. Utilizzare il comando e2label per modificare l'etichetta del volume in modo diverso da `/`.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1 old/
   ```

2. Verificare che il volume abbia la nuova etichetta.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1
   old/
   ```

Per modificare l'etichetta di un volume xfs collegato

- Utilizzare il comando xfs_admin per modificare l'etichetta del volume in modo diverso da `/`.

```
[ec2-user ~]$ sudo xfs_admin -L old/ /dev/xvdf1
writing all SBs
new label = "old/"
```

Dopo avere modificato l'etichetta del volume come mostrato, è possibile riavviare l'istanza con il volume corretto selezionato dal ramdisk iniziale all'avvio dell'istanza.

> **Important**
>
> Se desideri distaccare il volume con la nuova etichetta e collegarlo a un'altra istanza per utilizzarlo come volume root, devi eseguire nuovamente la procedura di cui sopra e riportare l'etichetta del volume al suo valore originale. Diversamente, l'altra istanza non si avvia in quanto il ramdisk non è in grado di individuare il volume con l'etichetta `/`.

Risoluzione dei problemi di connessione all'istanza Windows di Amazon EC2

Le informazioni e gli errori comuni seguenti possono essere utili per risolvere i problemi di connessione all'istanza Windows.

Problemi di connessione

- Il desktop remoto non può connettersi al computer remoto
- Errore durante l'uso del client macOS RDP
- RDP mostra una schermata nera invece del desktop
- Impossibile accedere da remoto a un'istanza con un utente che non è un amministratore
- Risoluzione dei problemi di Remote Desktop utilizzando AWS Systems Manager
- Abilitazione di Desktop remoto in un'istanza EC2 con il Registro di sistema remoto
- Ho perso la mia chiave privata. Come posso connettermi alla mia istanza Windows?

Il desktop remoto non può connettersi al computer remoto

Prova a eseguire le operazioni seguenti per risolvere i problemi relativi alla connessione all'istanza:

- Verificare di utilizzare il nome host DNS pubblico corretto. (Nella console Amazon EC2 selezionare l'istanza, quindi scegliere DNS pubblico (IPv4) nel riquadro dei dettagli). Se l'istanza si trova in un VPC e non si visualizza un nome DNS pubblico, è necessario abilitare i nomi host DNS. Per ulteriori informazioni, consulta Attributi DNS per il VPC nella Guida per l'utente di Amazon VPC.
- Verificare che l'istanza abbia un indirizzo IPv4 pubblico. Se non lo ha, è possibile associare un indirizzo IP elastico all'istanza. Per ulteriori informazioni, consulta Indirizzi IP elastici.
- Per connettersi all'istanza utilizzando un indirizzo IPv6, controllare che il computer locale abbia un indirizzo IPv6 e che sia configurato per utilizzare IPv6. Per ulteriori informazioni, consulta Configurazione di IPv6 sulle istanze nella Guida per l'utente di Amazon VPC.
- Verificare che il gruppo di sicurezza abbia una regola che consente l'accesso RDP sulla porta 3389.
- Se si copia la password ma si verifica l'errore `Your credentials did not work`, provare a digitarla manualmente quando richiesto. È possibile che manchi un carattere o che sia stato inserito uno spazio vuoto aggiuntivo durante la copia della password.
- Verificare che l'istanza abbia superato i controlli dello stato. Per ulteriori informazioni, consultare Verifiche dello stato delle istanze Amazon EC2 e the section called “Istanza Linux con esito negativo delle verifiche dello stato”.
- Verificare che la tabella di routing per la sottorete abbia un percorso che instrada tutto il traffico destinato al di fuori del VPC al gateway Internet per il VPC. Per ulteriori informazioni, consulta Creazione di una tabella di routing personalizzata (gateway Internet) nella Guida per l'utente di Amazon VPC.
- Verificare che Windows Firewall, o un altro firewall, non stia bloccando il traffico RDP alla istanza. Si consiglia di disabilitare Windows Firewall e di controllare l'accesso all'istanza utilizzando le regole del gruppo di sicurezza. Tenta una delle opzioni seguenti:
  - Utilizza AWSSupport-TroubleshootRDP per disable the Windows Firewall profiles using SSM Agent. Questa opzione richiede che l'istanza sia configurata per AWS Systems Manager.
  - Utilizza AWSSupport-ExecuteEC2Rescue.
  - Arresta l'istanza, staccare il volume root e collega il volume a un'istanza temporanea come volume di dati. Connettiti all'istanza temporanea e porta il volume online. Carica l'hive del registro dal volume di dati. In `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicyStandardProfile`, imposta `EnableFirewall` su 0. Scarica hive del registro e porta il volume offline. Scollega il volume dall'istanza temporanea e collegalo all'istanza originale come volume root. Avvia l'istanza originale.

- Verifica che Network Level Authentication sia disabilitato per le istanze che non sono parte di un dominio Active Directory (utilizza AWSSupport-TroubleshootRDP per disable NLA).
- Verificare che il tipo di avvio di Remote Desktop Service (TermService) sia Automatico e che il servizio sia avviato (utilizzare AWSSupport-TroubleshootRDP perenable and start the RDP service).
- Assicurati di connetterti alla porta Remote Desktop Protocol corretta, che, per impostazione predefinita, è 3389 (utilizza AWSSupport-TroubleshootRDP per read the current RDP port e change it back to 3389).
- Verifica che le connessioni Remote Desktop siano consentite sull'istanza (utilizza AWSSupport-TroubleshootRDP per enable Remote Desktop connections).
- Verificare che la password non sia scaduta. Se la password è scaduta, è possibile reimpostarla. Per ulteriori informazioni, consulta Reimpostazione della password dell'amministratore Windows per un'istanza Amazon EC2 Windows.
- Se tenti di connetterti utilizzando un utente creato nell'istanza e ricevi l'errore `The user cannot connect to the server due to insufficient access privileges`, assicurati di aver garantito all'utente il diritto di accesso locale. Per ulteriori informazioni, consulta l'articolo su come garantire a un membro il diritto di accesso locale.
- Se si tenta di aprire un numero di sessioni RDP contemporanee superiore alla soglia massima consentita, la sessione viene terminata con il messaggio `Your Remote Desktop Services session has ended. Another user connected to the remote computer, so your connection was lost.` Per impostazione predefinita, sono consentite due sessioni RDP contemporanee sull'istanza.

Errore durante l'uso del client macOS RDP

Se si sta effettuando la connessione a un'istanza Windows Server tramite il client Remote Desktop Connection dal sito Web Microsoft, è possibile che venga restituito il seguente errore:

```
Remote Desktop Connection cannot verify the identity of the computer that you want to
 connect to.
```

Scaricare l'app Microsoft Remote Desktop dal Mac App Store e utilizzarla per connettersi all'istanza.

RDP mostra una schermata nera invece del desktop

Per risolvere il problema, prova a eseguire queste operazioni:

- Per ulteriori informazioni, controllare l'output della console. Per ottenere l'output della console per l'istanza utilizzando la console Amazon EC2, selezionare l'istanza, scegliere Operazioni, Monitoraggio e risoluzione dei problemi, quindi Ottieni il log di sistema.
- Verificare che sia in esecuzione la versione più recente del client RDP.
- Provare le impostazioni predefinite per il client RDP.
- Se si utilizza la connessione al desktop remoto, provare ad avviarla con l'opzione `/admin` come mostrato di seguito.

```
mstsc /v:instance /admin
```

- Se il server esegue un'applicazione a schermo intero, è possibile che abbia smesso di rispondere. Usare Ctrl+Maiusc+Esc per avviare Windows Task Manager, quindi chiudere l'applicazione.
- Se il server è sovrautilizzato, potrebbe aver smesso di rispondere. Per monitorare l'istanza che utilizza la console Amazon EC2, selezionare l'istanza e quindi la scheda Monitoraggio. Se è necessario cambiare il tipo di istanza con uno di dimensioni maggiori, consulta Modifiche del tipo di istanza Amazon EC2.

Impossibile accedere da remoto a un'istanza con un utente che non è un amministratore

Se non riesci ad accedere da remoto a un'istanza Windows con un utente che non è un account amministratore, verifica di aver concesso all'utente il diritto di accedere in locale. Consulta Garantire a un utente o a un gruppo il diritto di accesso locale ai controller di dominio.

Risoluzione dei problemi di Remote Desktop utilizzando AWS Systems Manager

È possibile utilizzarlo AWS Systems Manager per risolvere i problemi di connessione all'istanza di Windows tramite RDP.

AWSSupport-TroubleshootRDP

Il documento di AWSSupport-TroubleshootRDP automazione consente all'utente di controllare o modificare le impostazioni comuni sull'istanza di destinazione che possono influire sulle connessioni RDP (Remote Desktop Protocol), come la porta RDP, la Network Layer Authentication (NLA) e i profili Windows Firewall. Per impostazione predefinita, il documento legge e produce i valori di queste impostazioni.

Il documento di AWSSupport-TroubleshootRDP automazione può essere utilizzato con istanze EC2, istanze locali e macchine virtuali (VM) abilitate all'uso con (istanze gestite). AWS Systems Manager Inoltre, può essere utilizzato anche con istanze EC2 per Windows Server che non sono abilitate per l'utilizzo con Systems Manager. Per informazioni sull'abilitazione delle istanze da utilizzare con AWS Systems Manager, consulta Nodi gestiti nella Guida per l'utente. AWS Systems Manager

Per risolvere i problemi relativi all'utilizzo del documento AWSSupport-TroubleshootRDP

1. Accedere alla console Systems Manager.
2. Verificare di trovarsi nella stessa regione dell'istanza danneggiata.
3. Scegli Documenti nel riquadro di navigazione sinistro.
4. Nella scheda Di proprietà di Amazon, inserisci `AWSSupport-TroubleshootRDP` nel campo di ricerca. Quando appare il documento `AWSSupport-TroubleshootRDP`, selezionalo.
5. Scegliere Esegui automazione.
6. Per Modalità esecuzione, scegliere Esecuzione semplice.
7. Per i parametri di input InstanceId, abilita Mostra selettore di istanze interattivo.
8. Scegliere l'istanza Amazon EC2.
9. Rivedere gli esempi, quindi scegliere Esegui.
10. Per monitorare l'avanzamento dell'esecuzione, per Stato esecuzione, aspettare che lo stato cambi da In sospeso a Riuscito. Espandere Output per vedere i risultati. Per vedere l'output delle singole fasi, in Fasi eseguite, scegliere un elemento da ID fase.

AWSSupport-TroubleshootRDP esempi

Gli esempi seguenti mostrano come eseguire le attività di risoluzione dei problemi più comuni utilizzando. AWSSupport-TroubleshootRDP È possibile utilizzare il AWS CLI start-automation-execution comando di esempio o il collegamento fornito a. Console di gestione AWS

Example Esempio: verificare lo stato RDP attuale

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom" --region region_code
```

AWS Systems Manager console:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region#documentVersion=$LATEST
```

Example Esempio: disabilitare Windows Firewall

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=i-1234567890abcdef0, Action=Custom, Firewall=Disable" --
region region_code
```

AWS Systems Manager console:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&Firewall=Disable
```

Example Esempio: disabilitare Network Level Authentication

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, NLASettingAction=Disable" --
region region_code
```

AWS Systems Manager console:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion
```

Example Esempio: impostare RDP Service Startup Type su Automatico e avviare il servizio RDP

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, RDPServiceStartupType=Auto,
 RDPServiceAction=Start" --region region_code
```

AWS Systems Manager console:

```
https://console.aws.amazon.com/systems-manager/automation/execute/
AWSSupport-TroubleshootRDP?region=region_code#documentVersion=
$LATEST&RDPServiceStartupType=Auto&RDPServiceAction=Start
```

Example Esempio: ripristinare la porta RDP predefinita (3389)

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, RDPPortAction=Modify" --
region region_code
```

AWS Systems Manager console:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RDPPortAction=Modify
```

Example Esempio: consentire connessioni remote

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, RemoteConnections=Enable" --
region region_code
```

AWS Systems Manager console:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RemoteConnections=Enable
```

AWSSupport-ExecuteEC2Rescue

Il documento di AWSSupport-ExecuteEC2Rescue automazione utilizza EC2Rescue for Windows Server per risolvere e ripristinare automaticamente i problemi di connettività delle istanze EC2 e RDP. Per ulteriori informazioni, consulta Esecuzione dello strumento EC2Rescue su istanze non raggiungibili.

Il documento di AWSSupport-ExecuteEC2Rescue automazione richiede l'arresto e il riavvio dell'istanza. Systems Manager arresta l'istanza e crea un'Amazon Machine Image (AMI). I dati

archiviati nei volumi dell'instance store vengono persi. L'indirizzo IP pubblico viene modificato se non si utilizza un IP elastico. Per ulteriori informazioni, consulta Esecuzione dello strumento EC2Rescue su istanze non raggiungibili nella Guida per l'utente di AWS Systems Manager .

Per risolvere i problemi relativi all'utilizzo del documento AWSSupport-ExecuteEC2Rescue

1. Aprire la console Systems Manager.
2. Verificare di trovarsi nella stessa regione dell'istanza Amazon EC2 danneggiata.
3. Nel riquadro di navigazione, scegli Documenti.
4. Cerca e seleziona il documento `AWSSupport-ExecuteEC2Rescue`, quindi scegli Esegui automazione.
5. In Modalità esecuzione, scegliere Esecuzione semplice.
6. Nella sezione Parametri di input, per UnreachableInstanceId, inserisci l'ID dell'istanza Amazon EC2 dell'istanza irraggiungibile.
7. (Facoltativo) Per LogDestination, inserisci il nome del bucket Amazon Simple Storage Service (Amazon S3) se desideri raccogliere i log del sistema operativo per la risoluzione dei problemi della tua istanza Amazon EC2. I log vengono automaticamente caricati nel bucket specificato.
8. Selezionare Esegui.
9. Per monitorare l'avanzamento dell'esecuzione, nello stato Esecuzione, aspettare che lo stato cambi da In sospeso a Riuscito. Espandere Output per vedere i risultati. Per vedere l'output delle singole fasi, in Fasi eseguite, scegliere ID Fase.

Abilitazione di Desktop remoto in un'istanza EC2 con il Registro di sistema remoto

Se la tua istanza non raggiungibile non è gestita da AWS Systems Manager Session Manager, puoi utilizzare il registro remoto per abilitare Remote Desktop.

1. Dalla console EC2, arrestare l'istanza irraggiungibile.
2. Scollega il volume root dell'istanza non raggiungibile e collegalo a un'istanza raggiungibile nella stessa zona di disponibilità come volume di archiviazione. Se non disponi di un'istanza raggiungibile nella stessa zona di disponibilità, avviane una. Prendi nota del nome del dispositivo del volume root sull'istanza irraggiungibile.
3. Sull'istanza raggiungibile, apri Gestione disco. Ciò è possibile emettendo il comando seguente in una finestra di prompt dei comandi.

```
diskmgmt.msc
```

4. Apri il menu contestuale (clic con il pulsante destro del mouse) per il volume appena collegato proveniente dall'istanza irraggiungibile, quindi scegli Online.
5. Apri l'editor del Registro di Windows. Ciò è possibile emettendo il comando seguente in una finestra di prompt dei comandi.

```
regedit
```

6. Nell'Editor del registro di sistema, scegliere HKEY_LOCAL_MACHINE, quindi selezionare File, Carica Hive.
7. Selezionare l'unità del volume allegato, passare a `\Windows\System32\config\`, selezionare `SYSTEM`, quindi scegliere Apri.
8. Per Nome chiave, immettere un nome univoco per l'hive e scegliere OK.
9. Eseguire il backup dell'hive del Registro di sistema prima di apportare modifiche al Registro di sistema.
   a. Nell'albero della console del Registry Editor, seleziona l'hive che hai caricato: HKEY_LOCAL_MACHINE\. *`your-key-name`*
   b. Scegli File, Esporta.
   c. Nella finestra di dialogo Esporta file del Registro di sistema scegliere il percorso in cui si desidera salvare la copia di backup e quindi digitare un nome per il file di backup nel campo Nome file.
   d. Scegli Save (Salva).
10. Nell'Editor del Registro di sistema, accedi a, quindi`HKEY_LOCAL_MACHINE\`*`your key name`*`\ControlSet001\Control\Terminal Server`, nel riquadro dei dettagli, apri FDENYTSConnections.
11. Nella casella Modifica valore DWORD immettere `0` nel campo Dati valore.
12. Seleziona OK.

> **Note**
>
> Se il valore nel campo Dati valore è 1, l'istanza negherà le connessioni desktop remoto. Un valore di `0` consente connessioni desktop remoto.

13. Nell'Editor del Registro di sistema, scegliete HKEY_LOCAL_MACHINE\, quindi selezionate File, Unload Hive. *your-key-name*
14. Chiudere l'Editor del registro di sistema e Gestione disco.
15. Dalla console EC2, scollegare il volume root dall'istanza raggiungibile e collegarlo di nuovo all'istanza non raggiungibile. Quando si collega il volume all'istanza irraggiungibile, immettere il nome del dispositivo salvato in precedenza nel campo Dispositivo.
16. Riavviare l'istanza irraggiungibile.

Ho perso la mia chiave privata. Come posso connettermi alla mia istanza Windows?

Quando ci si connette a un'istanza di Windows appena avviata, decodificare la password per l'account amministratore utilizzando la chiave privata per la coppia di chiavi specificata all'avvio dell'istanza.

Se si perde la password dell'amministratore e non si dispone più della chiave privata, è necessario reimpostare la password o creare una nuova istanza. Per ulteriori informazioni, consulta Reimpostazione della password dell'amministratore Windows per un'istanza Amazon EC2 Windows. Per la procedura di reimpostazione della password utilizzando un documento Systems Manager, consulta Reimpostazione di password e chiavi SSH sulle istanze EC2 nella Guida per l'utente di AWS Systems Manager .

Risolvi i problemi relativi all'avvio delle istanze Windows di Amazon EC2

I suggerimenti riportati di seguito possono aiutarti a risolvere i problemi riguardanti le password e l'attivazione con le istanze Windows di Amazon EC2.

Problemi

- "La password non è disponibile"
- "Password non ancora disponibile"
- "Impossibile recuperare la password di Windows"
- "In attesa del servizio di metadati"
- "Impossibile attivare Windows"

- "Windows non è originale (0x80070005)"
- "Nessun server Terminal Server License disponibile per fornire una licenza"
- "Alcune impostazioni sono gestite dalla tua organizzazione"

"La password non è disponibile"

Per connetterti a un'istanza Windows tramite Remote Desktop, è necessario specificare un account e una password. Gli account e le password forniti si basano sull'AMI utilizzata per avviare l'istanza. Puoi recuperare la password generata automaticamente per l'account Amministratore oppure utilizzare l'account e la password in uso nell'istanza originale da cui è stata creata l'AMI.

Puoi generare una password per l'account amministratore per le istanze avviate utilizzando un'AMI Windows personalizzata. Per generare la password, devi configurare alcune impostazioni nel sistema operativo prima della creazione dell'AMI. Per ulteriori informazioni, consulta Crea un' EBS-backed AMI Amazon.

Se l'istanza Windows non è configurata per generare una password casuale, riceverai il messaggio seguente al momento del recupero della password generata automaticamente tramite la console:

```
Password is not available.
The instance was launched from a custom AMI, or the default password has changed. A
password cannot be retrieved for this instance. If you have forgotten your password,
 you can
reset it using the Amazon EC2 configuration service. For more information, see
 Passwords for a
Windows Server instance.
```

Verifica l'output della console per l'istanza per vedere se l'AMI utilizzata per avviarla era stata creata con la generazione di password disattivata. Se la generazione di password è disattivata, l'output della console contiene quanto segue:

```
Ec2SetPassword: Disabled
```

Se la generazione di password è disattivata e non ricordi la password dell'istanza originale, puoi reimpostarla per tale istanza. Per ulteriori informazioni, consulta Reimpostazione della password dell'amministratore Windows per un'istanza Amazon EC2 Windows.

"Password non ancora disponibile"

Per connetterti a un'istanza Windows tramite Remote Desktop, è necessario specificare un account e una password. Gli account e le password forniti si basano sull'AMI utilizzata per avviare l'istanza. Puoi recuperare la password generata automaticamente per l'account Amministratore oppure utilizzare l'account e la password in uso nell'istanza originale da cui è stata creata l'AMI.

La password dovrebbe essere disponibile in pochi minuti. Se la password non è disponibile, riceverai il messaggio seguente al momento del recupero della password generata automaticamente tramite la console:

```
Password not available yet.
Please wait at least 4 minutes after launching an instance before trying to retrieve
 the
auto-generated password.
```

Se sono trascorsi più di quattro minuti senza ricevere la password, è possibile che l'agente di avvio per la tua istanza non sia configurato per generare una password. Verifica controllando se l'output della console è vuoto. Per ulteriori informazioni, consulta Impossibile ottenere l'output della console.

Verifica inoltre che l'account AWS Identity and Access Management (IAM) utilizzato per accedere al portale di gestione abbia l'`ec2:GetPasswordData`azione consentita. Per ulteriori informazioni sulle autorizzazioni IAM, consulta l'articolo relativo alla descrizione di IAM.

"Impossibile recuperare la password di Windows"

Per recuperare la password generata automaticamente per l'account Amministratore, è necessario utilizzare la chiave privata per la coppia di chiavi specificata all'avvio dell'istanza. Se non specifichi una coppia di chiavi quando viene avviata l'istanza, riceverai il messaggio seguente.

```
Cannot retrieve Windows password
```

Puoi terminare l'istanza e avviarne una nuova utilizzando la stessa AMI, assicurandoti di specificare una coppia di chiavi.

"In attesa del servizio di metadati"

Un'istanza Windows deve ottenere informazioni dai suoi metadati prima di attivarsi. Per impostazione predefinita, il valore `WaitForMetaDataAvailable` assicura che il servizio EC2Config attenda

che i metadati dell'istanza siano accessibili prima di proseguire con il processo di avvio. Per ulteriori informazioni, consulta Utilizzo dei metadati dell'istanza per gestire l'istanza EC2.

Se l'istanza non supera la prova di raggiungibilità, prova a eseguire queste operazioni per risolvere il problema.

- Controllare il blocco CIDR per il VPC. Un'istanza Windows non può avviarsi correttamente se avviata in un VPC con un intervallo di indirizzi IP che varia da `224.0.0.0` a `255.255.255.255` (intervalli di indirizzi IP di classe D e classe E). Tali intervalli sono riservati e non devono essere assegnati ai dispositivi host. Si consiglia di creare un VPC con un blocco CIDR dagli intervalli di indirizzi IP privati (non instradabili pubblicamente), come specificato in RFC 1918.
- È possibile che il sistema sia stato configurato con un indirizzo IP statico. Provare a creare un'interfaccia di rete e a collegarla all'istanza.
- Per abilitare DHCP su un'istanza Windows con la quale non è possibile connettersi

  1. Arrestare l'istanza interessata e distaccarne il volume root.
  2. Avviare un'istanza temporanea nella stessa zona di disponibilità dell'istanza interessata.

     > **Warning**
     >
     > Se la tua istanza temporanea si basa sulla stessa AMI su cui si basa l'istanza originale, devi completare ulteriori operazioni o non sarai in grado di avviare l'istanza originale dopo aver ripristinato il volume radice a causa di una collisione di firme del disco. In alternativa, seleziona un'AMI diversa per l'istanza temporanea. Ad esempio, se l'istanza originale utilizza l'AMI AWS Windows per Windows Server 2016, avvia l'istanza temporanea utilizzando l'AMI AWS Windows per Windows Server 2019.

  3. Collegare il volume radice dall'istanza interessata all'istanza temporanea. Connettersi all'istanza temporanea, aprire l'utilità Disk Management (Gestione disco) e portare l'unità online.
  4. Dall'istanza temporanea aprire Regedit e selezionare HKEY_LOCAL_MACHINE. Dal menu File scegliere Load Hive (Carica Hive). Selezionare l'unità, aprire il file `Windows\System32\config\SYSTEM` e specificare un nome della chiave quando richiesto (è possibile utilizzare qualsiasi nome).
  5. Selezionare la chiave appena caricata e passare a `ControlSet001\Services\Tcpip\Parameters\Interfaces`. Ciascuna interfaccia di rete è elencata da una GUID. Selezionare l'interfaccia di rete corretta. Se DHCP è disattivato e un indirizzo IP statico è

assegnato, `EnableDHCP` è impostato su 0. Per abilitare DHCP, impostare `EnableDHCP` su 1, quindi eliminare le chiavi seguenti, se presenti: `NameServer`, `SubnetMask`, `IPAddress` e `DefaultGateway`. Selezionare nuovamente la chiave e, dal menu File, scegliere Unload Hive (Scarica Hive).

> **Note**
>
> In presenza di più interfacce di rete, sarà necessario identificare l'interfaccia corretta per attivare DHCP. Per identificare l'interfaccia di rete corretta, esaminare i seguenti valori della chiave `NameServer`, `SubnetMask`, `IPAddress` e `DefaultGateway`. Questi valori mostrano la configurazione statica della precedente istanza.

6. (Facoltativo) Se DHCP è già attivato, è possibile che non sia disponibile alcun percorso al servizio di metadati. È possibile risolvere questo problema aggiornando il servizio EC2Config.

   a. Scaricare e installare la versione più recente del servizio EC2Config. Per ulteriori informazioni sull'installazione di questo servizio, consulta the section called "Installazione di EC2Config".

   b. Estrarre i file dal file `.zip` nella directory `Temp` sull'unità collegata.

   c. Aprire Regedit e selezionare HKEY_LOCAL_MACHINE. Dal menu File scegliere Carica Hive. Selezionare l'unità, aprire il file `Windows\System32\config\SOFTWARE` e specificare un nome della chiave quando richiesto (è possibile utilizzare qualsiasi nome).

   d. Selezionare la chiave appena caricata e passare a `Microsoft\Windows \CurrentVersion`. Selezionare la chiave `RunOnce`. (Se questa chiave non esiste, fare clic con il pulsante destro del mouse su `CurrentVersion`, puntare su New (Nuovo), selezionare Key (Chiave) e nominare la chiave `RunOnce`). Apri il menu contestuale (clic con il pulsante destro del mouse), seleziona Nuovo e seleziona String Value. Immettere il nome `Ec2Install` e i dati `C:\Temp\Ec2Install.exe -q`.

   e. Selezionare nuovamente la chiave e, dal menu File, scegliere Unload Hive (Scarica Hive).

7. (Facoltativo) Se la tua istanza temporanea si basa sulla stessa AMI su cui si basa quella originale, devi completare ulteriori operazioni o non sarai in grado di avviare l'istanza originale dopo aver ripristinato il volume di root a causa di un conflitto di firme del disco.

> **Warning**
>
> Nella procedura seguente viene descritto come modificare il Registro di sistema di Windows utilizzando l'editor del Registro di sistema. Se non hai familiarità con il

Registro di sistema di Windows o non sai come apportare modifiche in modo sicuro utilizzando l'editor del Registro di sistema, consulta Configura il Registro di sistema.

a. Apri un prompt dei comandi, digita regedit.exe e premi Invio.

b. In Editor del Registro di sistema, scegli HKEY_LOCAL_MACHINE dal menu contestuale (tasto destro del mouse), quindi seleziona Cerca.

c. Digita Windows Boot Manager e quindi seleziona Trova successivo.

d. Scegli la chiave denominata `11000001`. Questa chiave è un pari livello della chiave trovata nella fase precedente.

e. Nel riquadro a destra, seleziona `Element` e quindi Modifica dal menu contestuale (tasto destro del mouse).

f. Individua la firma del disco a quattro byte con offset 0x38 nei dati. Inverti i byte per creare la firma del disco e annotala. Ad esempio, la firma del disco rappresentata dai seguenti dati è `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. In una finestra del prompt dei comandi, esegui il comando seguente per avviare Microsoft DiskPart.

```
diskpart
```

h. Esegui il DiskPart comando seguente per selezionare il volume. (È possibile verificare che il numero del disco sia 1 utilizzando l'utilità Gestione del disco.)

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

i. Esegui il DiskPart comando seguente per ottenere la firma del disco.

```
DISKPART>  uniqueid disk
```

```
Disk ID: 0C764FA8
```

j. Se la firma del disco mostrata nel passaggio precedente non corrisponde alla firma del disco contenuta nel BCD che hai annotato in precedenza, usa il DiskPart comando seguente per modificare la firma del disco in modo che corrisponda:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

8. Tramite l'utilità Gestione disco, portare l'unità offline.

> **Note**
>
> L'unità è automaticamente non in linea se l'istanza temporanea esegue lo stesso sistema operativo dell'istanza interessata, quindi non sarà necessario disconnetterla manualmente.

9. Distaccare il volume dall'istanza temporanea. Se non si utilizza più l'istanza temporanea, è possibile terminarla.
10. Ripristinare il volume root dell'istanza interessata collegandolo come `/dev/sda1`.
11. Avviare l'istanza interessata.

Se sei connesso all'istanza, apri un browser Internet dall'istanza e immetti l'URL seguente per il server di metadati:

```
http://169.254.169.254/latest/meta-data/
```

Se non riesci a contattare il server di metadati, prova a eseguire queste operazioni per risolvere il problema:

- Scaricare e installare la versione più recente del servizio EC2Config. Per ulteriori informazioni sull'installazione di questo servizio, consulta the section called "Installazione di EC2Config".
- Verifica se l'istanza Windows sta eseguendo i driver PV di Red Hat. In tal caso, aggiornare i driver PV di Citrix. Per ulteriori informazioni, consulta the section called "Aggiornamento dei driver PV".
- Verificare che le impostazioni di firewall, IPSec e proxy non blocchino il traffico in uscita verso il servizio di metadati (`169.254.169.254`) o i server AWS KMS (gli indirizzi sono specificati negli elementi `TargetKMSServer` in `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml`).

- Verificare che sia disponibile un percorso al servizio di metadati (`169.254.169.254`) utilizzando il comando seguente.

```
route print
```

- Verificare eventuali problemi di rete che potrebbero interessare la zona di disponibilità dell'istanza. Passa a http://status.aws.amazon.com/.

"Impossibile attivare Windows"

Le istanze Windows utilizzano l'attivazione di Windows AWS KMS . Puoi ricevere questo messaggio:`A problem occurred when Windows tried to activate. Error Code 0xC004F074`, se la tua istanza non riesce a raggiungere il AWS KMS server. Windows deve essere attivato ogni 180 giorni. EC2Config tenta di contattare il AWS KMS server prima della scadenza del periodo di attivazione per assicurarsi che Windows rimanga attivato.

Se riscontri un problema di attivazione di Windows, utilizza la procedura seguente per risolvere il problema.

Per EC2Config (AMI di Windows Server 2012 R2 e precedenti)

1. Scaricare e installare la versione più recente del servizio EC2Config. Per ulteriori informazioni sull'installazione di questo servizio, consulta the section called "Installazione di EC2Config".
2. Connettersi all'istanza e aprire il file seguente: `C:\Program Files\Amazon \Ec2ConfigService\Settings\config.xml`.
3. Individua il Ec2WindowsActivate plugin nel file. `config.xml` Modificare lo stato in Enabled (Abilitato) e salvare le modifiche.
4. Nell'applicazione Servizi di Windows, riavviare il servizio EC2Config o l'istanza.

Se la procedura non risolve il problema di attivazione, esegui queste operazioni aggiuntive.

1. Imposta l' AWS KMS obiettivo: C:\> slmgr.vbs /skms 169.254.169.250:1688
2. Attivare Windows: C:\> slmgr.vbs /ato

Per EC2Launch (AMI di Windows Server 2016 e successive)

1. Da un PowerShell prompt con diritti amministrativi, importa il modulo EC2Launch:

```
PS C:\> Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1"
```

2. Chiama la Add-Routes funzione per visualizzare l'elenco dei nuovi percorsi:

```
PS C:\> Add-Routes
```

3. Chiama la Set-ActivationSettings funzione:

```
PS C:\> Set-Activationsettings
```

4. Quindi, esegui lo script seguenti per attivare Windows:

```
PS C:\> cscript "${env:SYSTEMROOT}\system32\slmgr.vbs" /ato
```

Se continui a ricevere un errore di attivazione sia per EC2Config che per EC2Launch, verifica le informazioni seguenti.

- Verifica di disporre di percorsi verso i AWS KMS server. Apri `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml` e individua gli elementi `TargetKMSServer`. Esegui il comando seguente e controlla se gli indirizzi di questi AWS KMS server sono elencati.

  ```
  route print
  ```

- Verificate che la chiave AWS KMS client sia impostata. Esegui il comando seguente e controllare l'output.

  ```
  C:\Windows\System32\slmgr.vbs /dlv
  ```

  Se l'output contiene Error: product key not found, la chiave AWS KMS client non è impostata. Se la chiave AWS KMS client non è impostata, cerca la chiave client come descritto in questo articolo Microsoft: attivazione del AWS KMS client e codici prodotto, quindi esegui il comando seguente per impostare la chiave AWS KMS client.

  ```
  C:\Windows\System32\slmgr.vbs /ipk client_key
  ```

- Verifica l'ora e il fuso orario del sistema siano corretti. Se si utilizza un fuso orario diverso da UTC, aggiungi la seguente chiave di registro e impostala su 1 per garantire che l'ora sia corretta: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimeIsUniversal`.
- Se Windows Firewall è abilitato, disattivalo temporaneamente utilizzando il comando seguente.

```
netsh advfirewall set allprofiles state off
```

"Windows non è originale (0x80070005)"

Le istanze Windows utilizzano l' AWS KMS attivazione di Windows. Se un'istanza non è in grado di completare il processo di attivazione, segnala che la copia di Windows non è originale.

Segui i suggerimenti della sezione "Impossibile attivare Windows".

"Nessun server Terminal Server License disponibile per fornire una licenza"

Per impostazione predefinita, Windows Server prevede una licenza per due utenti simultanei tramite Desktop remoto. Se è necessario garantire a più di due utenti l'accesso simultaneo all'istanza Windows tramite Desktop remoto, puoi acquistare una licenza CAL per Servizi Desktop remoto e installare l'host della sessione di Desktop remoto e i ruoli del Server licenze di Desktop remoto.

Verifica i problemi seguenti:

- Hai superato il numero massimo di sessioni RDP simultanee.
- Hai installato il ruolo di Servizi Desktop remoto di Windows.
- La licenza è scaduta. Se la licenza è scaduta, non puoi connetterti con l'istanza Windows come utente. Puoi eseguire le operazioni indicate di seguito:
  - Connettiti all'istanza da una riga di comando utilizzando un parametro `/admin`, ad esempio:

    ```
    mstsc /v:instance /admin
    ```

    Per ulteriori informazioni, consulta il seguente articolo di Microsoft sull'Accesso al desktop remoto tramite riga di comando.
  - Arresta l'istanza, distaccane i volumi Amazon EBS e collegali a un'altra istanza nella stessa zona di disponibilità per recuperare i dati.

"Alcune impostazioni sono gestite dalla tua organizzazione"

Le istanze lanciate dalle ultime AMI di Windows Server potrebbero mostrare il seguente messaggio di Windows Update: "Alcune impostazioni sono gestite dalla tua organizzazione". Questo messaggio viene visualizzato a seguito di modifiche apportate a Windows Server e non influisce sul comportamento di Windows Update o sulla possibilità di gestire le impostazioni di aggiornamento.

Per rimuovere l'avviso

1. Aprire `gpedit.msc` e navigare su Computer Configuration (Configurazione computer), Administrative Templates (Modelli amministrativi), Windows Components (Computer Windows), Windows updates (Aggiornamenti Windows). Modifica Configure Automatic Update (Configura aggiornamento automatico) e impostalo su enabled (abilitato).
2. In un prompt dei comandi, aggiornare la policy di gruppo utilizzando gpupdate /force.
3. Chiudere e riaprire le impostazioni di Windows Update. Sarà visualizzato il messaggio riportato sopra riguardante la gestione delle impostazioni da parte dell'organizzazione, seguito da "Scaricheremo automaticamente gli aggiornamenti, tranne che nelle connessioni a consumo (dove potrebbero applicarsi costi). In quel caso, scaricheremo automaticamente gli aggiornamenti richiesti per il buon funzionamento di Windows".
4. Tornare a `gpedit.msc` e impostare nuovamente le policy di gruppo su not configured (non configurati). Eseguire nuovamente gpupdate /force.
5. Chiudere il prompt dei comandi e attendere alcuni minuti.
6. Riaprire le impostazioni di Windows Update. Non dovrebbe essere visualizzato il messaggio "Alcune impostazioni sono gestite dall'organizzazione".

Risolvi i problemi relativi alle istanze Windows di Amazon EC2

I suggerimenti riportati di seguito possono aiutarti a risolvere i problemi associati alle istanze Windows di Amazon EC2.

Problemi

- Impossibile connettersi AWS Systems Manager Sessions Manager su un'istanza di Windows Server 2025
- I volumi EBS non vengono inizializzati su Windows Server 2016 e 2019
- Avvio di un'istanza EC2 Windows in Directory Services Restore Mode (DSRM)

- L'istanza perde la connettività di rete oppure le attività programmate non vengono eseguite quando previsto
- Impossibile ottenere l'output della console
- Windows Server 2012 R2 non disponibile sulla rete
- Collisione della firma del disco

Impossibile connettersi AWS Systems Manager Sessions Manager su un'istanza di Windows Server 2025

È possibile che si verifichi un problema durante la connessione di AWS Systems Manager Sessions Manager a un'istanza di Windows Server 2025. Per risolvere questo problema, accedi all'istanza, quindi vai a `Settings > Apps > Optional Features` e aggiungi`WMIC`. Riavvia il servizio Agente SSM o riavvia l'istanza e Sessions Manager dovrebbe connettersi.

È inoltre possibile utilizzare il PowerShell comando seguente per eseguire la stessa azione:

```
Start-Process -FilePath "$env:SystemRoot\system32\Dism.exe" -ArgumentList @('/
Online', '/Add-Capability', '/CapabilityName:WMIC~~~~') -Wait; Restart-Service -Name
 AmazonSSMAgent
```

I volumi EBS non vengono inizializzati su Windows Server 2016 e 2019

Le istanze create da Amazon Machine Image (AMI) di Windows Server 2016 e 2019 utilizzano l'agente EC2Launch v1 per una serie di attività di avvio, inclusa l'inizializzazione dei volumi EBS. Per impostazione predefinita, EC2Launch v1 non inizializza i volumi secondari. Tuttavia, puoi configurare EC2Launch v1 in modo che inizializzi questi dischi automaticamente, come indicato di seguito.

Mappatura delle lettere di unità nei volumi

1. Connettersi all'istanza da configurare e aprire il file `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` in un editor di testo.
2. Specifica le impostazioni del volume, come indicato di seguito:

```
{
"driveLetterMapping": [
 {
   "volumeName": "sample volume",
```

```
   "driveLetter": "H"
 }]
}
```

3. Salvare le modifiche e chiudere il file.
4. Apri Windows PowerShell e usa il seguente comando per eseguire lo script EC2Launch v1 che inizializza i dischi:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Per inizializzare i dischi ogni volta che l'istanza si avvia, aggiungere il contrassegno `-Schedule` come segue:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

L'agente EC2Launch v1 può eseguire script di inizializzazione delle istanze, come `initializeDisks.ps1` in parallelo con lo script `InitializeInstance.ps1`. Se lo script `InitializeInstance.ps1` riavvia l'istanza, potrebbe interrompere altre attività pianificate eseguite all'avvio dell'istanza. Per evitare potenziali conflitti, consigliamo di aggiungere logica allo script `initializeDisks.ps1`per garantire che l'inizializzazione dell'istanza venga terminata per prima.

> **Note**
>
> Se lo script EC2Launch non inizializza i volumi, assicurati che i volumi siano online. In caso contrario, esegui il comando seguente per portarli online.
>
> ```
> PS C:\> Get-Disk | Where-Object IsOffline -Eq $True | Set-Disk -IsOffline
>  $False
> ```

Avvio di un'istanza EC2 Windows in Directory Services Restore Mode (DSRM)

Se un'istanza che esegue Microsoft Active Directory sperimenta un errore di sistema o altri problemi critici, puoi risolvere tali anomalie avviando l'istanza in una versione speciale della modalità

provvisoria denominata Directory Services Restore Mode (DSRM). Questa modalità ti permette di riparare o recuperare Active Directory.

Supporto driver per DSRM

Il modo di abilitare DSRM e avviare nell'istanza dipende dai driver che eseguono l'istanza. Nella console EC2 puoi visualizzare i dettagli della versione del driver per un'istanza dal log di sistema. La tabella seguente mostra quali driver sono supportati per DSRM.

Versioni driver	DSRM supportata?	Fasi successive
Citrix PV 5.9	No	Ripristina l'istanza da un backup. Non puoi abilitare DSRM.
AWS PV 7.2.0	No	Anche se la modalità DSRM non è supportata dal driver, puoi comunque distaccare il volume root dall'istanza, acquisire uno snapshot del volume o creare un'AMI da esso, quindi collegarlo a un'altra istanza nella stessa zona di disponibilità come volume secondario. Puoi quindi abilitare DSRM (come descritto in questa sezione).
AWS PV 7.2.2 e versioni successive	Sì	Distacca il volume root, collegalo a un'altra istanza e abilita DSRM (come descritto in questa sezione).
Reti avanzate	Sì	Distacca il volume root, collegalo a un'altra istanza e abilita DSRM (come descritto in questa sezione).

Per informazioni su come abilitare le reti avanzate, consulta the section called "Adattatore elastico di rete (ENA)". Per informazioni sull'aggiornamento dei driver PV, consulta Aggiornamento dei driver AWS PV sulle istanze Windows.

Configurazione di un'istanza da avviare in DSRM

Le istanze EC2 Windows non dispongono di una connessione di rete finché che il sistema operativo non è in esecuzione. Per questa ragione, non puoi premere il pulsante F8 sulla tastiera per

selezionare un'opzione di avvio. È necessario utilizzare una delle procedure seguenti per avviare un'istanza Windows Server EC2 in modalità DSRM.

Se sospetti che Active Directory sia stato danneggiato e che l'istanza sia ancora in esecuzione, puoi configurare l'istanza per l'avvio in modalità DSRM utilizzando sia la finestra di dialogo di configurazione del sistema o il prompt dei comandi.

Per avviare un'istanza online in modalità DSRM tramite la finestra di dialogo di configurazione del sistema

1. Nella finestra di dialogo Run (Esegui) digitare `msconfig` e premere Invio.
2. Scegliere la scheda Boot (Avvio).
3. In Boot options (Opzioni di avvio) scegliere Safe boot (Avvio sicuro).
4. Scegliere Active Directory repair (Riparazione di Active Directory), quindi OK. Il sistema ti invita a riavviare il server.

Per avviare un'istanza online in modalità DSRM utilizzando la riga di comando

Da una finestra del prompt dei comandi, esegui il comando seguente:

```
bcdedit /set safeboot dsrepair
```

Se un'istanza è offline e irraggiungibile, distacca il volume root e collegalo a un'altra istanza per abilitare la modalità DSRM.

Per avviare un'istanza offline in modalità DSRM

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Individua e seleziona l'istanza interessata. Scegli Instance state (Stato istanza), Stop instance (Arresta istanza).
4. Scegli Launch instances (Avvia le istanze) e crea un'istanza temporanea nella stessa Zona di disponibilità dell'istanza interessata. Scegliere un tipo di istanza che utilizzi una versione diversa di Windows. Ad esempio, se l'istanza è Windows Server 2016, scegliere un'istanza Windows Server 2019.

> **Important**
>
> Se non crei l'istanza nella stessa Zona di disponibilità dell'istanza interessata, non potrai collegare il volume root dell'istanza interessata sulla nuova istanza.

5. Nel riquadro di navigazione, selezionare Volumes (Volumi).
6. Individua il volume root dell'istanza interessata. Distaccare il volume e collegarlo all'istanza temporanea creata in precedenza. Collegala con il nome del dispositivo predefinito (xvdf).
7. Utilizzare Desktop remoto per collegarsi all'istanza temporanea, quindi usare l'utilità Disk Management (Gestione disco) per rendere il volume disponibile per l'uso.
8. Aprire un prompt dei comandi ed eseguire il comando seguente. Sostituire D con la lettera di unità effettiva del volume secondario appena collegato:

```
bcdedit /store D:\Boot\BCD /set {default} safeboot dsrepair
```

9. Nell'utilità Disk Management (Gestione disco), scegliere l'unità collegata in precedenza, aprire il menu contestuale (pulsante destro del mouse) e scegliere Offline.
10. Nella console EC2, distaccare il volume interessato dall'istanza temporanea e ricollegarlo all'istanza originale con il nome dispositivo `/dev/sda1`. Devi specificare questo nome del dispositivo per indicare il volume come volume root.
11. Avviare l'istanza.
12. Dopo che l'istanza ha superato i controlli dello stato nella console EC2, connettersi all'istanza tramite Desktop remoto e verificare che si avvii in modalità DSRM.
13. (Facoltativo) Eliminare o arrestare l'istanza temporanea creata in questa procedura.

L'istanza perde la connettività di rete oppure le attività programmate non vengono eseguite quando previsto

Se si riavvia l'istanza e si perde la connettività di rete, è possibile che l'ora dell'istanza sia errata.

Per impostazione predefinita, le istanze Windows utilizzano il formato UTC. Se si imposta l'ora dell'istanza su un fuso orario differente e successivamente la si riavvia, si produce una differenza oraria e l'istanza perde temporaneamente il suo indirizzo IP. L'istanza ristabilisce la connettività di rete alla fine, ma ciò può richiedere alcune ore. La quantità di tempo richiesta per tale recupero dipende dalla differenza tra UTC e l'altro fuso orario.

Lo stesso problema temporale può causare anche la mancata esecuzione di attività pianificate nel momento previsto. In questo caso, tali attività non vengono eseguite quando previsto perché l'ora dell'istanza è errata.

Per utilizzare un fuso orario diverso da UTC in modo persistente, è necessario impostare la chiave di registro. RealTimeIsUniversal Senza questa chiave, un'istanza utilizza UTC dopo il riavvio.

Per risolvere problemi temporali che causano la perdita della connettività di rete

1. Assicurarsi di eseguire i driver PV raccomandati. Per ulteriori informazioni, consulta the section called “Aggiornamento dei driver PV”.
2. Verificare che la seguente chiave di registro esista e sia impostata su1: HKEY_LOCAL_MACHINE\ SYSTEM\\ Control\\ CurrentControlSet TimeZoneInformation RealTimeIsUniversal

Impossibile ottenere l'output della console

Per le istanze Windows, la console dell'istanza mostra l'output delle attività eseguite durante il processo di avvio di Windows. Se Windows si avvia correttamente, l'ultimo messaggio registrato è `Windows is Ready to use`. È possibile anche visualizzare i messaggi del log eventi nella console, ma questa funzionalità potrebbe non essere abilitata per impostazione predefinita a seconda della versione di Windows utilizzata. Per ulteriori informazioni, consulta the section called “Agenti di avvio Windows”.

Per ottenere l'output della console per l'istanza utilizzando la console Amazon EC2, selezionare l'istanza, scegliere Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), quindi Get system log (Ottieni il log di sistema). Per ottenere l'output della console utilizzando la riga di comando, utilizzate uno dei seguenti comandi: https://docs.aws.amazon.com/cli/latest/reference/ec2/get-console-output.html get-console-output () o ().AWS CLI Get-EC2ConsoleOutput AWS Tools for Windows PowerShell

Per le istanze che eseguono Windows Server 2012 R2 e versioni precedenti, l'output della console vuoto potrebbe indicare un problema con il servizio EC2Config, come un file di configurazione configurato in modo errato o un errore di avvio di Windows. Per correggere il problema, scarica e installa la versione più recente del servizio EC2Config. Per ulteriori informazioni, consulta the section called “Installazione di EC2Config”.

Windows Server 2012 R2 non disponibile sulla rete

Per informazioni sulla risoluzione dei problemi di un'istanza Windows Server 2012 R2 che non è disponibile sulla rete, consulta Windows Server 2012 R2 perde la connettività di rete e storage dopo un riavvio dell'istanza.

Collisione della firma del disco

Puoi controllare e risolvere le collisioni della firma del disco utilizzando EC2Rescue per Windows Server. In alternativa, puoi risolvere manualmente i problemi di firma del disco completando la seguente procedura.

> **Warning**
>
> Nella procedura seguente viene descritto come modificare il Registro di sistema di Windows utilizzando l'editor del Registro di sistema. Se non hai familiarità con il Registro di sistema di Windows o non sai come apportare modifiche in modo sicuro utilizzando l'editor del Registro di sistema, consulta Configura il Registro di sistema.

1. Apri un prompt dei comandi, digita regedit.exe e premi Invio.
2. In Editor del Registro di sistema, scegli HKEY_LOCAL_MACHINE dal menu contestuale (tasto destro del mouse), quindi seleziona Cerca.
3. Digita Windows Boot Manager e quindi seleziona Trova successivo.
4. Scegli la chiave denominata `11000001`. Questa chiave è un pari livello della chiave trovata nella fase precedente.
5. Nel riquadro a destra, seleziona `Element` e quindi Modifica dal menu contestuale (tasto destro del mouse).
6. Individua la firma del disco a quattro byte con offset 0x38 nei dati. Questa è la firma BCD (Boot Configuration Database). Inverti i byte per creare la firma del disco e annotala. Ad esempio, la firma del disco rappresentata dai seguenti dati è `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

7. In una finestra del prompt dei comandi, esegui il comando seguente per avviare Microsoft. DiskPart

```
diskpart
```

8. Esegui il `select disk` DiskPart comando e specifica il numero del disco per il volume con la collisione della firma del disco.

> **Tip**
>
> Per verificare il numero del disco relativo al volume con la collisione della firma del disco, utilizza l'utilità Gestione disco. Apri un prompt dei comandi, digita `compmgmt.msc` e premi Invio. Nel pannello di navigazione a sinistra, apri Gestione disco. Nell'utilità Gestione disco, verifica il numero del disco per il volume offline con la collisione della firma del disco.

```
DISKPART> select disk 1
Disk 1 is now the selected disk.
```

9. Esegui il seguente DiskPart comando per ottenere la firma del disco.

```
DISKPART>  uniqueid disk
Disk ID: 0C764FA8
```

10. Se la firma del disco mostrata nel passaggio precedente non corrisponde alla firma del disco che hai annotato in precedenza, usa il DiskPart comando seguente per modificare la firma del disco in modo che corrisponda:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

Debug del kernel per le istanze di Windows sulla rete

Il KDNET Extensibility Module for Elastic Network Adapter (ENA) è un livello di supporto per i driver hardware che consente il debug del kernel di Windows sulla rete tramite ENA su istanze Amazon Elastic Compute Cloud. Puoi utilizzare il modulo di estensibilità con Windows Debugger () per eseguire il debug a livello di kernel su istanze EC2 che eseguono Windows. WinDbg

Il debugging del kernel consente di diagnosticare e risolvere problemi di basso livello del sistema operativo, come errori di schermata blu (BSOD), guasti dei driver e problemi di avvio sulle istanze EC2 Windows.

Indice

- Prerequisiti
- Passaggio 1: installare gli strumenti di debug di Windows sull'host di debug
- Fase 2: Impostare l'obiettivo di debug
- Passaggio 3: avviare la sessione di debug sull'host di debug
- Passaggio 4: riavviare la destinazione di debug
- Pulisci le impostazioni di debug dopo il debug
- Limitazioni
- Note aggiuntive

Prerequisiti

Prima di iniziare, assicurati di disporre di:

Due istanze EC2 per Windows, nella stessa sottorete:

- Un'istanza host di debug: esegue Windows Debugger (). WinDbg
- Un'istanza di destinazione di debug, l'istanza di cui si desidera eseguire il debug.

Per ulteriori informazioni sull'avvio delle istanze, consulta. Guida introduttiva

I gruppi di sicurezza per le istanze host e target devono consentire il traffico UDP in entrata e in uscita sulla porta utilizzata per il debug di KDNET (intervallo consigliato: 50000-50039). Il modo più semplice per configurarlo è creare un gruppo di sicurezza con una regola in entrata che consenta il traffico UDP proveniente da se stesso come origine e quindi collegare quel gruppo di sicurezza a entrambe le istanze. Per ulteriori informazioni, consulta Regole del gruppo di sicurezza nella Guida per l'utente di Amazon VPC.

L'istanza di destinazione di debug deve eseguire una delle seguenti versioni di Windows (o successive):

- Windows Server 2025 con numero di build 26100.7462 (patch di dicembre 2025)

- Windows 11 24H2 con numero di build 26100.7309
- Windows 11 25H2 con numero di build 26200.7309

> **Note**
>
> Il modulo di estensibilità KDNET per ENA è distribuito come parte di Windows e può essere aggiornato solo tramite aggiornamenti cumulativi mensili di Windows. Ti consigliamo di mantenere la versione più recente di Windows KB installata sulla destinazione di debug per assicurarti di averne la versione più recente.
> Per verificare che il modulo sia presente nella destinazione di debug, esegui il comando seguente in una sessione con privilegi elevati PowerShell :
>
> ```
> Test-Path C:\Windows\system32\kd_02_1d0f.dll
> ```
>
> Se il comando viene restituito`True`, il modulo è disponibile.

Passaggio 1: installare gli strumenti di debug di Windows sull'host di debug

Installa gli strumenti di debug di Windows sull'istanza dell'host di debug eseguendo il comando seguente in una sessione: PowerShell

```
winget install microsoft.windbg
```

Per istruzioni dettagliate sull'installazione, vedi Installare Windows Debugger nella documentazione Microsoft.

Dopo l'installazione, verifica che il debugger funzioni eseguendo il comando seguente in una sessione: PowerShell

```
windbgx
```

La WinDbg finestra dovrebbe aprirsi. In caso affermativo, l'installazione è andata a buon fine e puoi chiudere la finestra.

Fase 2: Impostare l'obiettivo di debug

> **Note**
>
> Quando il debug del kernel è attivo, il dispositivo ENA utilizzato per la sessione di debug è dedicato solo al traffico del debugger. Se devi mantenere l'accesso a Internet sull'istanza di destinazione di debug durante il debug, collega una seconda ENA all'istanza prima di iniziare.

Sulla destinazione di debug, apri una PowerShell sessione con privilegi elevati e configura il debug del kernel utilizzando i seguenti passaggi.

Eseguite il comando seguente per elencare il bus, il dispositivo e il numero di funzione dell'adattatore ENA collegato all'istanza:

```
Get-NetAdapter -Physical |
    Where-Object -Property PnPDeviceID -Match -Value '^PCI\\VEN_1D0F&DEV_EC2[01]&' |
    Get-NetAdapterHardwareInfo |
    Select-Object InterfaceDescription, BusNumber, DeviceNumber, FunctionNumber |
    Format-List
```

Se all'istanza sono collegati più adattatori ENA

Se all'istanza sono collegati più adattatori ENA, usa il comando seguente per mappare ogni adattatore fisico al relativo indirizzo IP privato. Puoi fare un riferimento incrociato a questi dettagli nella Console di gestione AWS sezione EC2 → Istanze → [ID istanza] → Rete → Interfacce di rete. Questo ti aiuta a correlare interfacce di rete specifiche IDs, gruppi privati IPs e di sicurezza con l'adattatore a livello di sistema operativo per un debug mirato.

```
Get-NetAdapter -Physical |
    Where-Object PnPDeviceID -Match '^PCI\\VEN_1D0F&DEV_EC2[01]&' |
    ForEach-Object {
        $adapter = $_
        $hwInfo = $adapter | Get-NetAdapterHardwareInfo
        $ipInfo = Get-NetIPAddress -InterfaceIndex $adapter.InterfaceIndex -
AddressFamily IPv4
        [PSCustomObject]@{
            InterfaceDescription = $adapter.InterfaceDescription
            IPAddress            = $ipInfo.IPAddress
            BusNumber            = $hwInfo.BusNumber
```

```
            DeviceNumber          = $hwInfo.DeviceNumber
            FunctionNumber        = $hwInfo.FunctionNumber
        }
    } | Format-List
```

Annotate i `FunctionNumber` valori `BusNumber``DeviceNumber`, e dell'adattatore ENA da utilizzare per il debug dall'output.

Eseguite i seguenti comandi per configurare il debug del kernel. Sostituisci i valori segnaposto con la tua configurazione specifica:

```
bcdedit /debug on
bcdedit /set loadoptions FORCEHVTONOTSHAREDEBUGDEVICE
bcdedit /dbgsettings net hostip:host-private-ip port:port-number key:encryption-key
 busparams:b.d.f
```

> **Note**
>
> Verifica se esiste `loadoptions` eseguendo il comando seguente. Se viene restituito un valore, copia quella stringa e `;FORCEHVTONOTSHAREDEBUGDEVICE` aggiungila.
>
> ```
> (bcdedit /enum) -match "loadoptions"
> ```

Dove:

- *`host-private-ip`*— L' IPv4 indirizzo privato dell'istanza dell'host di debug. Se le tue istanze vengono avviate in una sottorete IPv6 solo, consulta Configurazione di KDNET con nella documentazione di Microsoft per ulteriori informazioni IPv6 sull'utilizzo con KDNET. IPv6
- *`port-number`*— La porta da usare per la sessione di debug. L'intervallo consigliato è 50000-50039 (ad esempio,). `50000`
- *`encryption-key`*— Una chiave a 256 bit utilizzata per crittografare la connessione di debug, specificata come quattro valori a 64 bit separati da punti. Ogni valore a 64 bit può contenere fino a 13 caratteri utilizzando solo lettere minuscole a—z e cifre da 0 a 9. I caratteri speciali non sono consentiti. Esempio di chiave di crittografia:. `1kdnet2keys3.4kdnet5keys6.7kdnet8keys9.10kdnet11ke`
- *`b.d.f`*— I numeri di bus, dispositivo e funzione per il dispositivo ENA, formattati come `bus.device.function` (ad esempio`0.3.0`), utilizzati per il debug.

> **Tip**
>
> Per eseguire il debug del processo di avvio di Windows, esegui anche il seguente comando:
>
> ```
> bcdedit /bootdebug on
> ```

Passaggio 3: avviare la sessione di debug sull'host di debug

Per consentire il debug del traffico sull'host, puoi creare una regola firewall per l'applicazione o una porta UDP specifica. WinDbg

Opzione 1: consentire l'applicazione WinDbg

Esegui i seguenti comandi per autorizzare l' WinDbg eseguibile:

```
$WinDbgxPath = "$env:LocalAppData\Microsoft\WindowsApps\WinDbgX.exe"
New-NetFirewallRule -DisplayName "Allow Inbound KDNET Connection" -Action Allow -
Program $WinDbgxPath
```

Opzione 2: consentire una porta UDP specifica

In alternativa, puoi consentire il traffico UDP in entrata verso la porta configurata per il debug del kernel. Sostituisci con la porta *`port-number`* KDNET scelta:

```
$DebugPort = port-number
New-NetFirewallRule -DisplayName "Allow Inbound KDNET Connection" -Direction Inbound -
LocalPort $DebugPort -Protocol UDP -Action Allow
```

> **Note**
>
> Le configurazioni del firewall possono essere limitate dalla Domain Group Policy (GPO) o richiedere autorizzazioni di amministratore elevate. Se il comando fallisce, contatta l'amministratore di rete.

Inizia WinDbg con la porta e la chiave che corrispondono alla configurazione della destinazione di debug. È possibile specificare opzioni di debug del kernel aggiuntive documentate nel riferimento alla riga di comando di WinDbg Microsoft in base al proprio caso d'uso.

```
windbgx -k net:port=port-number,key=encryption-key
```

WinDbg si apre e attende che il target di debug si connetta.

Passaggio 4: riavviare la destinazione di debug

Sulla destinazione di debug, riavvia l'istanza per avviare la connessione di debug:

```
shutdown -r -t 0
```

Dopo il riavvio della destinazione di debug, WinDbg sull'host di debug si connette automaticamente alla destinazione. È ora possibile utilizzarlo WinDbg per controllare lo stato del kernel, impostare i breakpoint e diagnosticare i problemi.

Pulisci le impostazioni di debug dopo il debug

Sulla destinazione di debug

Al termine del debug, rimuovete la configurazione di debug del kernel dalla destinazione di debug per ripristinare il normale comportamento di avvio. Sulla destinazione di debug, aprite una sessione con privilegi elevati ed eseguite i seguenti comandi: PowerShell

```
bcdedit /debug off
bcdedit /dbgsettings LOCAL
bcdedit /deletevalue loadoptions
```

Se ne esistono di `loadoptions` diversi`FORCEHVTONOTSHAREDEBUGDEVICE`, è necessario ripristinare l'impostazione eseguendola `bcdedit /set loadoptions` con l'originale. `loadoptions`

Se hai abilitato il debug di avvio, esegui anche:

```
bcdedit /bootdebug off
```

Riavvia l'istanza per rendere effettive le modifiche.

Sull'host di debug

Rimuovi la regola del firewall eseguendo:

```
Remove-NetFirewallRule -DisplayName "Allow Inbound KDNET Connection"
```

Limitazioni

Il modulo di estensibilità KDNET per ENA attualmente non supporta:

- tipi di istanze x86_64 non in metallo di ottava generazione (ad esempio,) `m8a.xlarge`
- tipi di istanze x86_64 non metalliche 48xlarge di settima generazione (ad esempio,) `m7a.48xlarge`
- tipi di istanze u7i

Il modulo attualmente non supporta istanze con Secure Boot abilitato. È possibile verificare lo stato `Confirm-SecureBootUEFI` eseguendo una sessione con privilegi elevati. PowerShell Se l'output è`True`, Secure Boot è attivo. Tieni presente che tutte le immagini fornite da Amazon con un prefisso «TPM» hanno Secure Boot abilitato per impostazione predefinita.

Note aggiuntive

Se riscontri problemi di connessione del debugger all'istanza di destinazione, verifica quanto segue:

- Tutti i prerequisiti elencati in questa guida sono soddisfatti, inclusa la versione build di Windows Server richiesta e la presenza del modulo di estensibilità.
- I gruppi di sicurezza collegati a entrambe le istanze sono configurati correttamente per consentire il traffico tra di loro sulla porta di debug configurata.
- Le regole di Windows Firewall sulle istanze host non bloccano il traffico di rete tra le due istanze sulla porta configurata.

Per ulteriori indicazioni, consulta Configurare manualmente il debug del kernel di rete KDNET nella documentazione Microsoft.

Reimpostazione della password dell'amministratore Windows per un'istanza Amazon EC2 Windows

Se non è più possibile connettersi all'istanza Amazon EC2 Windows perché la password dell'amministratore di Windows è persa o scaduta, è possibile reimpostare la password.

> **Note**
>
> Esiste un documento di AWS Systems Manager automazione che applica automaticamente i passaggi manuali necessari per reimpostare la password dell'amministratore locale. Per ulteriori informazioni, consulta Reimpostazione di password e chiavi SSH sulle istanze EC2 nella Guida per l'utente di AWS Systems Manager .

I metodi manuali di reimpostazione della password amministratore utilizzano EC2Launch v2, EC2Config o EC2Launch.

- Per tutte le AMI di Windows supportate che includono l'agente EC2Launch v2, utilizza EC2Launch v2.
- Per le AMI Windows precedenti a Windows Server 2016, utilizza il servizio EC2Config.
- Per le AMI Windows Server 2016 e successive, utilizza il servizio EC2Launch.

Tali procedure descrivono inoltre come connettersi a un'istanza se hai perso la coppia di chiavi utilizzata per creare l'istanza. Amazon EC2 utilizza una chiave pubblica per crittografare un singolo dato, come una password, e una chiave privata per decrittografare i dati. La chiave pubblica e quella privata sono note come coppia di chiavi. Con le istanze Windows, puoi utilizzare una coppia di chiavi per ottenere la password amministratore e accedere tramite RDP.

> **Note**
>
> Se nell'istanza è stato disattivato l'account amministratore locale e l'istanza è configurata per Systems Manager, è inoltre possibile riattivare e reimpostare la password dell'amministratore locale utilizzando EC2Rescue e Run Command. Per ulteriori informazioni, consulta Usa EC2Rescue per Windows Server con Systems Manager Run Command.

Indice

- Reimpostazione password amministratore Windows per istanza EC2 tramite EC2Launch v2
- Reimpostazione password amministratore Windows per istanza EC2 tramite EC2Launch
- Reimpostazione password amministratore Windows per istanza EC2 tramite EC2Config

Reimpostazione password amministratore Windows per istanza EC2 tramite EC2Launch v2

Se hai perso la password amministratore Windows e utilizzi un'AMI Windows supportata che include l'agente EC2Launch v2, puoi utilizzare EC2Launch v2 per generare una nuova password.

Se utilizzi un'AMI Windows Server 2016 o versione successiva che non include l'agente EC2Launch v2, consulta la sezione Reimpostazione password amministratore Windows per istanza EC2 tramite EC2Launch.

Se utilizzi un'AMI Windows Server precedente a Windows Server 2016 che non include l'agente EC2Launch v2, consulta la sezione Reimpostazione password amministratore Windows per istanza EC2 tramite EC2Config.

> **Note**
>
> Se nell'istanza è stato disattivato l'account amministratore locale e l'istanza è configurata per Systems Manager, è inoltre possibile riattivare e reimpostare la password dell'amministratore locale utilizzando EC2Rescue e Run Command. Per ulteriori informazioni, consulta Usa EC2Rescue per Windows Server con Systems Manager Run Command.

> **Note**
>
> Esiste un documento di AWS Systems Manager automazione che applica automaticamente i passaggi manuali necessari per reimpostare la password dell'amministratore locale. Per ulteriori informazioni, consulta Reimpostazione di password e chiavi SSH sulle istanze EC2 nella Guida per l'utente di AWS Systems Manager .

Per reimpostare la password dell'amministratore di Windows usando EC2Launch v2, è necessario eseguire la seguente azione:

- Fase 1: Verifica che l'agente EC2Launch v2 sia in esecuzione
- Fase 2: Distaccare il volume radice dall'istanza
- Fase 3: Collegare il volume a un'istanza temporanea.
- Fase 4: Eliminare il .esegui una volta file

- Fase 5: Riavviare l'istanza originale.

Fase 1: Verifica che l'agente EC2Launch v2 sia in esecuzione

Prima di tentare di reimpostare la password amministratore, verifica che l'agente EC2Launch v2 sia installato e in esecuzione. Puoi utilizzare l'agente EC2Launch v2 per reimpostare la password amministratore più avanti in questa sezione.

Per verificare che l'agente EC2Launch v2 sia in esecuzione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Instances (Istanze), quindi selezionare l'istanza per la quale si desidera reimpostare la password. In questa procedura questa istanza viene chiamata istanza originale.
3. Scegliere Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), quindi Get system log (Ottieni il log di sistema).
4. Individua la voce di avvio di EC2, ad esempio Launch: EC2Launch v2 service v2.0.124. Se viene visualizzata questa voce, il servizio EC2Launch v2 è in esecuzione.

   Se l'output del log di sistema è vuoto, o se l'agente EC2Launch v2 non è in esecuzione, risolvi il problema dell'istanza con il servizio di acquisizione di screenshot della console dell'istanza. Per ulteriori informazioni, consulta Acquisizione di uno screenshot di un'istanza irraggiungibile.

Fase 2: Distaccare il volume radice dall'istanza

Non è possibile usare EC2Launch v2 per reimpostare una password amministratore se il volume in cui la password è archiviata è collegato a un'istanza come il volume root. È necessario distaccare il volume dall'istanza originale prima che sia possibile collegarlo a un'istanza temporanea come volume secondario.

Per distaccare il volume root dall'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza che richiede la reimpostazione della password e scegli Stato istanza, Arresta istanza. Dopo aver modificato lo stato dell'istanza in Stopped (Arrestato), passa alla fase successiva.

4. (Facoltativo) Se disponi della chiave privata specificata al momento dell'avvio dell'istanza, passa alla fase successiva. In caso contrario, attieniti alla seguente procedura per sostituire l'istanza con una nuova istanza avviata con una nuova coppia di chiavi.

   a. Creare una nuova coppia di chiavi tramite la console Amazon EC2. Per assegnare alla nuova coppia di chiavi lo stesso nome della chiave privata persa, bisogna prima eliminare la coppia di chiavi esistente.

   b. Selezionare l'istanza da sostituire. Prendere nota del tipo di istanza, del VPC, della sottorete, del gruppo di sicurezza e del ruolo IAM dell'istanza.

   c. Con l'istanza selezionata, scegli Operazioni, Immagine e modelli, Crea immagine. Digitare un nome e una descrizione dell'immagine, quindi selezionare Create image (Crea immagine).

   d. Nel riquadro di navigazione scegliere AMIs (AMI). Attendi che lo stato dell'immagine cambi a disponibile. Poi, seleziona l'immagine e scegli Avvia istanza da AMI.

   e. Completa i campi per avviare un'istanza, assicurandoti di selezionare lo stesso tipo di istanza, VPC, sottorete, gruppo di sicurezza e ruolo IAM dell'istanza da sostituire, poi scegli Avvia istanza.

   f. Al termine, scegli la coppia di chiavi creata per la nuova istanza, poi scegli Avvia istanza.

   g. (Facoltativo) Se l'istanza originale dispone di un indirizzo IP elastico associato, trasferirlo alla nuova istanza. Se l'istanza originale ha volumi EBS oltre al volume root, trasferirli nella nuova istanza.

5. Distaccare il volume root dall'istanza originale come indicato di seguito:

   a. Seleziona l'istanza originale e scegli la scheda Archiviazione. Annota il nome del dispositivo root in Nome dispositivo root. Trova il volume con questo nome di dispositivo in Dispositivi a blocchi e annota l'ID del volume.

   b. Nel riquadro di navigazione, selezionare Volumes (Volumi).

   c. Nell'elenco dei volumi, seleziona il volume annotato come dispositivo root e scegli Operazioni, Distacca il volume. Una volta modificato lo stato del volume su available (disponibile), passare alla fase successiva.

6. Se hai creato una nuova istanza per sostituire l'istanza originale, puoi interrompere ora l'istanza originale. Non è più necessaria. Per il resto di questa procedura, tutti i riferimenti all'istanza originale si applicano alla nuova istanza creata.

Fase 3: Collegare il volume a un'istanza temporanea.

Successivamente, avviare un'istanza temporanea e collegare il volume come volume secondario. Questa è l'istanza che viene usata per modificare il file di configurazione.

Per avviare un'istanza temporanea e collegare il volume

1. Avviare l'istanza temporanea come indicato di seguito:

   a. Nel pannello di navigazione, selezionare Instances (Istanze), selezionare Launch instances (Avvia istanze) e poi selezionare una AMI.

   > **Important**
   >
   > Per evitare collisioni di firme del disco è necessario selezionare un'AMI per una versione diversa di Windows. Ad esempio, se l'istanza originale esegue Windows Server 2019, avviare l'istanza temporanea utilizzando l'AMI di base per Windows Server 2016.

   b. Lasciare il tipo di istanza predefinito, quindi scegliere Next: Configure Instance Details (Successivo: configura dettagli dell'istanza).

   c. Alla pagina Configure Instance Details (Configura i dettagli dell'istanza), per Subnet (Sottorete) selezionare la stessa zona di disponibilità dell'istanza originale e scegliere Review and Launch (Rivedi e avvia).

   > **Important**
   >
   > L'istanza temporanea deve trovarsi nella stessa zona di disponibilità dell'istanza originale. Se l'istanza temporanea si trova in una zona di disponibilità diversa, non è possibile collegare il volume root dell'istanza originale.

   d. Nella pagina Review Instance Launch (Verifica avvio istanza), scegliere Launch (Avvia).

   e. Quando richiesto, creare una nuova coppia di chiavi, scaricarla su un percorso sicuro nel computer, quindi scegliere Launch Instances (Avvia istanze).

2. Collegare il volume all'istanza temporanea come volume secondario seguendo questi passaggi:

a. Nel pannello di navigazione, selezionare Volumes (Volumi), selezionare il volume che è stato scollegato dall'istanza originale e quindi scegliere Actions (Operazioni), Attach Volume (Collega volume).

b. Nella finestra di dialogo Attach Volume (Collega volume), sotto Instances (Istanze), iniziare a digitare il nome o l'ID dell'istanza temporanea, quindi selezionare l'istanza dall'elenco.

c. Per Device (Dispositivo), digitare **`xvdf`** (se non è già inserito) e scegliere Attach (Collega).

Fase 4: Eliminare il .esegui una volta file

È ora necessario eliminare il file `.run-once` dal volume offline allegato all'istanza. Questo indica a EC2Launch v2 di eseguire tutte le attività con una frequenza di `once`, che include l'impostazione della password amministratore. Il percorso del file nel volume secondario collegato sarà simile a `D:\ProgramData\Amazon\EC2Launch\state\.run-once`.

Per eliminare il file .run-once

1. Aprire l'utilità Gestione disco e portare l'unità online seguendo queste istruzioni: Rendere un volume Amazon EBS disponibile per l'uso.
2. Individua il file `.run-once` nel disco che hai portato online.
3. Elimina il file .run-once.

> **Important**
>
> Qualsiasi script impostato per un'esecuzione sarà attivato da questa azione.

Fase 5: Riavviare l'istanza originale.

Dopo aver eliminato il file `.run-once`, ricollegare il volume all'istanza originale come volume root e collegarlo all'istanza usando la sua coppia di chiavi per recuperare la password dell'amministratore.

1. Collegare nuovamente il volume all'istanza originale come segue:

   a. Nel pannello di navigazione, selezionare Volumes (Volumi), selezionare il volume che è stato scollegato dall'istanza e quindi scegliere Actions (Operazioni), Attach Volume (Collega volume).

b. Nella finestra di dialogo Attach Volume (Collega volume), sotto Instances (Istanze), iniziare a digitare il nome o l'ID dell'istanza originale, quindi selezionare l'istanza.

c. Per Device (Dispositivo), digitare **`/dev/sda1`**.

d. Scegliere Attach (Collega). Dopo che lo stato del volume cambia in `in-use`, passa alla fase successiva.

2. Nel riquadro di navigazione, seleziona Instances (Istanze). Selezionare l'istanza originale e scegliere Instance state (Stato istanza), Start instance (Avvia istanza). Dopo che lo stato dell'istanza cambia in `Running`, passa alla fase successiva.

3. Recuperare la nuova password di amministratore di Windows utilizzando la chiave privata per la nuova coppia di chiavi e connettersi all'istanza. Per ulteriori informazioni, consulta Connessione all'istanza Windows con il protocollo RDP.

> **Important**
>
> Quando viene arrestata e riavviata, l'istanza riceve un nuovo indirizzo IP pubblico. Assicurarsi di collegarsi all'istanza utilizzando il relativo nome DNS pubblico. Per ulteriori informazioni, consulta Cambio di stato di un'istanza Amazon EC2.

4. (Facoltativo) È possibile terminare l'istanza temporanea se non la si utilizza più. Selezionare l'istanza temporanea e scegliere Instance state (Stato istanza), Terminate instance (Termina istanza).

Reimpostazione password amministratore Windows per istanza EC2 tramite EC2Launch

Se hai perso la password amministratore Windows e utilizzi un'AMI Windows Server 2016 o successiva, puoi utilizzare lo strumento EC2Rescue, che utilizza il servizio EC2Launch per generare una nuova password.

Se utilizzi un'AMI Windows Server 2016 o versione successiva che non include l'agente EC2Launch v2, puoi utilizzare EC2Launch v2 per generare una nuova password.

Se utilizzi un'AMI Windows Server precedente a Windows Server 2016, consulta Reimpostazione password amministratore Windows per istanza EC2 tramite EC2Config.

> **Warning**
>
> Quando si arresta un'istanza, i dati sui volumi dell'Instance Store vengono persi. Per conservare questi dati, esegui il backup su una memoria persistente.

> **Note**
>
> Se nell'istanza è stato disattivato l'account amministratore locale e l'istanza è configurata per Systems Manager, è inoltre possibile riattivare e reimpostare la password dell'amministratore locale utilizzando EC2Rescue e Run Command. Per ulteriori informazioni, consulta Usa EC2Rescue per Windows Server con Systems Manager Run Command.

> **Note**
>
> Esiste un documento di AWS Systems Manager automazione che applica automaticamente i passaggi manuali necessari per reimpostare la password dell'amministratore locale. Per ulteriori informazioni, consulta Reimpostazione di password e chiavi SSH sulle istanze EC2 nella Guida per l'utente di AWS Systems Manager .

Per reimpostare la password dell'amministratore di Windows usando EC2Launch, è necessario eseguire la seguente azione:

- Fase 1: Distaccare il volume radice dall'istanza
- Fase 2: Collegare il volume a un'istanza temporanea.
- Fase 3: Reimpostare la password amministratore
- Fase 4: Riavviare l'istanza originale.

Fase 1: Distaccare il volume radice dall'istanza

Non è possibile usare EC2Launch per reimpostare una password amministratore se il volume in cui la password è archiviata è collegato a un'istanza come il volume root. È necessario distaccare il volume dall'istanza originale prima che sia possibile collegarlo a un'istanza temporanea come volume secondario.

Per distaccare il volume root dall'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza che richiede la reimpostazione della password e scegli Stato istanza, Arresta istanza. Dopo aver modificato lo stato dell'istanza in Stopped (Arrestato), passa alla fase successiva.
4. (Facoltativo) Se disponi della chiave privata specificata al momento dell'avvio dell'istanza, passa alla fase successiva. In caso contrario, attieniti alla seguente procedura per sostituire l'istanza con una nuova istanza avviata con una nuova coppia di chiavi.

   a. Creare una nuova coppia di chiavi tramite la console Amazon EC2. Per assegnare alla nuova coppia di chiavi lo stesso nome della chiave privata persa, bisogna prima eliminare la coppia di chiavi esistente.
   b. Selezionare l'istanza da sostituire. Prendere nota del tipo di istanza, del VPC, della sottorete, del gruppo di sicurezza e del ruolo IAM dell'istanza.
   c. Con l'istanza selezionata, scegli Operazioni, Immagine e modelli, Crea immagine. Digitare un nome e una descrizione dell'immagine, quindi selezionare Create image (Crea immagine).
   d. Nel riquadro di navigazione scegliere AMIs (AMI). Attendi che lo stato dell'immagine cambi a disponibile. Poi, seleziona l'immagine e scegli Avvia istanza da AMI.
   e. Completa i campi per avviare un'istanza, assicurandoti di selezionare lo stesso tipo di istanza, VPC, sottorete, gruppo di sicurezza e ruolo IAM dell'istanza da sostituire, poi scegli Avvia istanza.
   f. Al termine, scegli la coppia di chiavi creata per la nuova istanza, poi scegli Avvia istanza.
   g. (Facoltativo) Se l'istanza originale dispone di un indirizzo IP elastico associato, trasferirlo alla nuova istanza. Se l'istanza originale ha volumi EBS oltre al volume root, trasferirli nella nuova istanza.
5. Distaccare il volume root dall'istanza originale come indicato di seguito:

   a. Seleziona l'istanza originale e scegli la scheda Archiviazione. Annota il nome del dispositivo root in Nome dispositivo root. Trova il volume con questo nome di dispositivo in Dispositivi a blocchi e annota l'ID del volume.
   b. Nel riquadro di navigazione, selezionare Volumes (Volumi).

c. Nell'elenco dei volumi, seleziona il volume annotato come dispositivo root e scegli Operazioni, Distacca il volume. Una volta modificato lo stato del volume su available (disponibile), passare alla fase successiva.

6. Se hai creato una nuova istanza per sostituire l'istanza originale, puoi interrompere ora l'istanza originale. Non è più necessaria. Per il resto di questa procedura, tutti i riferimenti all'istanza originale si applicano alla nuova istanza creata.

Fase 2: Collegare il volume a un'istanza temporanea.

Successivamente, avviare un'istanza temporanea e collegare il volume come volume secondario. Questa è l'istanza che viene usata per eseguire EC2Launch.

Per avviare un'istanza temporanea e collegare il volume

1. Avviare l'istanza temporanea come indicato di seguito:

   a. Nel pannello di navigazione, selezionare Instances (Istanze), selezionare Launch instances (Avvia istanze) e poi selezionare una AMI.

   > **Important**
   >
   > Per evitare collisioni di firme del disco è necessario selezionare un'AMI per una versione diversa di Windows. Ad esempio, se l'istanza originale esegue Windows Server 2019, avviare l'istanza temporanea utilizzando l'AMI di base per Windows Server 2016.

   b. Lasciare il tipo di istanza predefinito, quindi scegliere Next: Configure Instance Details (Successivo: configura dettagli dell'istanza).

   c. Alla pagina Configure Instance Details (Configura i dettagli dell'istanza), per Subnet (Sottorete) selezionare la stessa zona di disponibilità dell'istanza originale e scegliere Review and Launch (Rivedi e avvia).

   > **Important**
   >
   > L'istanza temporanea deve trovarsi nella stessa zona di disponibilità dell'istanza originale. Se l'istanza temporanea si trova in una zona di disponibilità diversa, non è possibile collegare il volume root dell'istanza originale.

d. Nella pagina Review Instance Launch (Verifica avvio istanza), scegliere Launch (Avvia).

e. Quando richiesto, creare una nuova coppia di chiavi, scaricarla su un percorso sicuro nel computer, quindi scegliere Launch Instances (Avvia istanze).

2. Collegare il volume all'istanza temporanea come volume secondario seguendo questi passaggi:

a. Nel pannello di navigazione, selezionare Volumes (Volumi), selezionare il volume che è stato scollegato dall'istanza originale e quindi scegliere Actions (Operazioni), Attach Volume (Collega volume).

b. Nella finestra di dialogo Attach Volume (Collega volume), sotto Instances (Istanze), iniziare a digitare il nome o l'ID dell'istanza temporanea, quindi selezionare l'istanza dall'elenco.

c. Per Device (Dispositivo), digitare **`xvdf`** (se non è già inserito) e scegliere Attach (Collega).

Fase 3: Reimpostare la password amministratore

Successivamente, connettersi all'istanza temporanea e utilizzare EC2Launch per reimpostare la password amministratore.

Per reimpostare la password amministratore

1. Connettersi all'istanza temporanea e utilizzare lo strumento EC2Rescue for Windows Server sull'istanza per reimpostare la password amministratore come segue:

a. Scarica il file zip EC2Rescue per Windows Server, estrai il contenuto ed esegui. EC2Rescue.exe

b. Nella schermata License Agreement (Contratto di licenza), leggere il contratto di licenza e, se si accettano i relativi termini, selezionare I Agree (Accetto).

c. Nella schermata Welcome to EC2Rescue for Windows Server (Benvenuti in EC2Rescue), selezionare Next (Successivo).

d. Nella schermata Select mode (Seleziona modalità), scegliere Offline instance (Istanza offline).

e. Nella schermata Select a disk (Seleziona un disco), scegliere il dispositivo xvdf e selezionare Next (Successivo).

f. Confermare la selezione del disco e scegliere Yes (Sì).

g. Dopo aver caricato il volume, selezionare OK.

h. Nella schermata Select Offline Instance (Seleziona istanza offline), scegliere Diagnose and Rescue (Diagnosi e recupero).

i. Nella schermata Summary (Riepilogo), controllare le informazioni e scegliere Next (Successivo).

j. Nella schermata Detected possible issues (Probabili problemi rilevati), selezionare Reset Administrator Password (Reimposta password amministratore) e scegliere Next (Successivo).

k. Nella schermata Confirm (Conferma), selezionare Rescue (Ripristina), OK.

l. Nella schermata Done (Fatto), selezionare Finish (Fine).

m. Chiudere lo strumento EC2Rescue for Windows Server, scollegarsi dall'istanza temporanea e quindi tornare alla console Amazon EC2.

2. Distaccare il volume (`xvdf`) secondario dall'istanza temporanea come indicato di seguito:

a. Nel riquadro di navigazione, selezionare Instances (Istanze) e selezionare l'istanza temporanea.

b. Nella scheda Storage per l'istanza temporanea, prendere nota dell'ID del volume EBS elencato come xvdf.

c. Nel riquadro di navigazione, selezionare Volumes (Volumi).

d. Nell'elenco dei volumi, selezionare il volume annotato nella fase precedente e scegliere Actions (Operazioni), Detach Volume (Distacca il volume). Una volta modificato lo stato del volume su available (disponibile), passare alla fase successiva.

Fase 4: Riavviare l'istanza originale.

Dopo aver reimpostato la password amministratore usando EC2Launch, ricollegare il volume all'istanza originale come volume root e collegarlo all'istanza usando la sua coppia di chiavi per recuperare la password dell'amministratore.

Per riavviare l'istanza originale

1. Collegare nuovamente il volume all'istanza originale come segue:

a. Nel pannello di navigazione, selezionare Volumes (Volumi), selezionare il volume che è stato scollegato dall'istanza e quindi scegliere Actions (Operazioni), Attach Volume (Collega volume).

b. Nella finestra di dialogo Attach Volume (Collega volume), sotto Instances (Istanze), iniziare a digitare il nome o l'ID dell'istanza originale, quindi selezionare l'istanza.

c. Per Device (Dispositivo), digitare **`/dev/sda1`**.

d. Scegliere Attach (Collega). Dopo che lo stato del volume cambia in `in-use`, passa alla fase successiva.

2. Nel riquadro di navigazione, seleziona Instances (Istanze). Selezionare l'istanza originale e scegliere Instance state (Stato istanza), Start instance (Avvia istanza). Dopo che lo stato dell'istanza cambia in `Running`, passa alla fase successiva.

3. Recuperare la nuova password di amministratore di Windows utilizzando la chiave privata per la nuova coppia di chiavi e connettersi all'istanza. Per ulteriori informazioni, consulta Connessione all'istanza Windows con il protocollo RDP.

4. (Facoltativo) È possibile terminare l'istanza temporanea se non la si utilizza più. Selezionare l'istanza temporanea e scegliere Instance state (Stato istanza), Terminate instance (Termina istanza).

Reimpostazione password amministratore Windows per istanza EC2 tramite EC2Config

Se hai perso la password amministratore Windows e utilizzi un'AMI Windows precedente a Windows Server 2016, puoi utilizzare l'agente EC2Config per generare una nuova password.

Se hai perso la password amministratore Windows e utilizzi un'AMI Windows Server 2016 o successiva, consulta la sezione Reimpostazione password amministratore Windows per istanza EC2 tramite EC2Launch oppure utilizza lo strumento EC2Rescue, che utilizza il servizio EC2Launch per generare una nuova password.

> **Note**
>
> Se nell'istanza è stato disattivato l'account amministratore locale e l'istanza è configurata per Systems Manager, è inoltre possibile riattivare e reimpostare la password dell'amministratore locale utilizzando EC2Rescue e Run Command. Per ulteriori informazioni, consulta Usa EC2Rescue per Windows Server con Systems Manager Run Command.

> **Note**
>
> Esiste un documento di AWS Systems Manager automazione che applica automaticamente i passaggi manuali necessari per reimpostare la password dell'amministratore locale. Per ulteriori informazioni, consulta Reimpostazione di password e chiavi SSH sulle istanze EC2 nella Guida per l'utente di AWS Systems Manager .

Per reimpostare la password dell'amministratore di Windows usando EC2Config, è necessario eseguire la seguente azione:

- Fase 1: Verifica che il servizio EC2Config sia in esecuzione
- Fase 2: Distaccare il volume radice dall'istanza
- Fase 3: Collegare il volume a un'istanza temporanea.
- Fase 4: modificare il file di configurazione
- Fase 5: Riavviare l'istanza originale.

Fase 1: Verifica che il servizio EC2Config sia in esecuzione

Prima di tentare di reimpostare la password amministratore, verificare che il servizio EC2Config sia installato e in esecuzione. Puoi utilizzare il servizio EC2Config per reimpostare la password amministratore più avanti in questa sezione.

Per verificare che il servizio EC2Config sia in esecuzione

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, selezionare Instances (Istanze), quindi selezionare l'istanza per la quale si desidera reimpostare la password. In questa procedura questa istanza viene chiamata istanza originale.
3. Scegliere Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), quindi Get system log (Ottieni il log di sistema).
4. Individuare la voce dell'agente EC2, ad esempio EC2 Agent: Ec2Config service v3.18.1118 (Agente EC2: servizio Ec2Config v3.18.1118). Se questa voce viene visualizzata, il servizio EC2Config è in esecuzione.

Se l'output del log di sistema è vuoto, o se il servizio EC2Config non è in esecuzione, risolvere il problema dell'istanza con il servizio di acquisizione di screenshot della console dell'istanza. Per ulteriori informazioni, consulta Acquisizione di uno screenshot di un'istanza irraggiungibile.

Fase 2: Distaccare il volume radice dall'istanza

Non è possibile usare EC2Config per reimpostare una password amministratore se il volume in cui la password è archiviata è collegato a un'istanza come il volume della radice. È necessario distaccare il volume dall'istanza originale prima che sia possibile collegarlo a un'istanza temporanea come volume secondario.

Per distaccare il volume root dall'istanza

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Seleziona l'istanza che richiede la reimpostazione della password e scegli Stato istanza, Arresta istanza. Dopo aver modificato lo stato dell'istanza in Stopped (Arrestato), passa alla fase successiva.
4. (Facoltativo) Se disponi della chiave privata specificata al momento dell'avvio dell'istanza, passa alla fase successiva. In caso contrario, attieniti alla seguente procedura per sostituire l'istanza con una nuova istanza avviata con una nuova coppia di chiavi.

    a. Creare una nuova coppia di chiavi tramite la console Amazon EC2. Per assegnare alla nuova coppia di chiavi lo stesso nome della chiave privata persa, bisogna prima eliminare la coppia di chiavi esistente.

    b. Selezionare l'istanza da sostituire. Prendere nota del tipo di istanza, del VPC, della sottorete, del gruppo di sicurezza e del ruolo IAM dell'istanza.

    c. Con l'istanza selezionata, scegli Operazioni, Immagine e modelli, Crea immagine. Digitare un nome e una descrizione dell'immagine, quindi selezionare Create image (Crea immagine).

    d. Nel riquadro di navigazione scegliere AMIs (AMI). Attendi che lo stato dell'immagine cambi a disponibile. Poi, seleziona l'immagine e scegli Avvia istanza da AMI.

    e. Completa i campi per avviare un'istanza, assicurandoti di selezionare lo stesso tipo di istanza, VPC, sottorete, gruppo di sicurezza e ruolo IAM dell'istanza da sostituire, poi scegli Avvia istanza.

f. Al termine, scegli la coppia di chiavi creata per la nuova istanza, poi scegli Avvia istanza.

g. (Facoltativo) Se l'istanza originale dispone di un indirizzo IP elastico associato, trasferirlo alla nuova istanza. Se l'istanza originale ha volumi EBS oltre al volume root, trasferirli nella nuova istanza.

5. Distaccare il volume root dall'istanza originale come indicato di seguito:

   a. Seleziona l'istanza originale e scegli la scheda Archiviazione. Annota il nome del dispositivo root in Nome dispositivo root. Trova il volume con questo nome di dispositivo in Dispositivi a blocchi e annota l'ID del volume.

   b. Nel riquadro di navigazione, selezionare Volumes (Volumi).

   c. Nell'elenco dei volumi, seleziona il volume annotato come dispositivo root e scegli Operazioni, Distacca il volume. Una volta modificato lo stato del volume su available (disponibile), passare alla fase successiva.

6. Se hai creato una nuova istanza per sostituire l'istanza originale, puoi interrompere ora l'istanza originale. Non è più necessaria. Per il resto di questa procedura, tutti i riferimenti all'istanza originale si applicano alla nuova istanza creata.

Fase 3: Collegare il volume a un'istanza temporanea.

Successivamente, avviare un'istanza temporanea e collegare il volume come volume secondario. Questa è l'istanza che viene usata per modificare il file di configurazione.

Per avviare un'istanza temporanea e collegare il volume

1. Avviare l'istanza temporanea come indicato di seguito:

   a. Nel pannello di navigazione, selezionare Instances (Istanze), selezionare Launch instances (Avvia istanze) e poi selezionare una AMI.

> **Important**
>
> Per evitare collisioni di firme del disco è necessario selezionare un'AMI per una versione diversa di Windows. Ad esempio, se l'istanza originale esegue Windows Server 2019, avviare l'istanza temporanea utilizzando l'AMI di base per Windows Server 2016.

b. Lasciare il tipo di istanza predefinito, quindi scegliere Next: Configure Instance Details (Successivo: configura dettagli dell'istanza).

c. Alla pagina Configure Instance Details (Configura i dettagli dell'istanza), per Subnet (Sottorete) selezionare la stessa zona di disponibilità dell'istanza originale e scegliere Review and Launch (Rivedi e avvia).

> **Important**
>
> L'istanza temporanea deve trovarsi nella stessa zona di disponibilità dell'istanza originale. Se l'istanza temporanea si trova in una zona di disponibilità diversa, non è possibile collegare il volume root dell'istanza originale.

d. Nella pagina Review Instance Launch (Verifica avvio istanza), scegliere Launch (Avvia).

e. Quando richiesto, creare una nuova coppia di chiavi, scaricarla su un percorso sicuro nel computer, quindi scegliere Launch Instances (Avvia istanze).

2. Collegare il volume all'istanza temporanea come volume secondario seguendo questi passaggi:

a. Nel pannello di navigazione, selezionare Volumes (Volumi), selezionare il volume che è stato scollegato dall'istanza originale e quindi scegliere Actions (Operazioni), Attach Volume (Collega volume).

b. Nella finestra di dialogo Attach Volume (Collega volume), sotto Instances (Istanze), iniziare a digitare il nome o l'ID dell'istanza temporanea, quindi selezionare l'istanza dall'elenco.

c. Per Device (Dispositivo), digitare **`xvdf`** (se non è già inserito) e scegliere Attach (Collega).

Fase 4: modificare il file di configurazione

Dopo aver collegato il volume all'istanza temporanea come volume secondario, modificare il plugin `Ec2SetPassword` nel file di configurazione.

Per modificare il file di configurazione

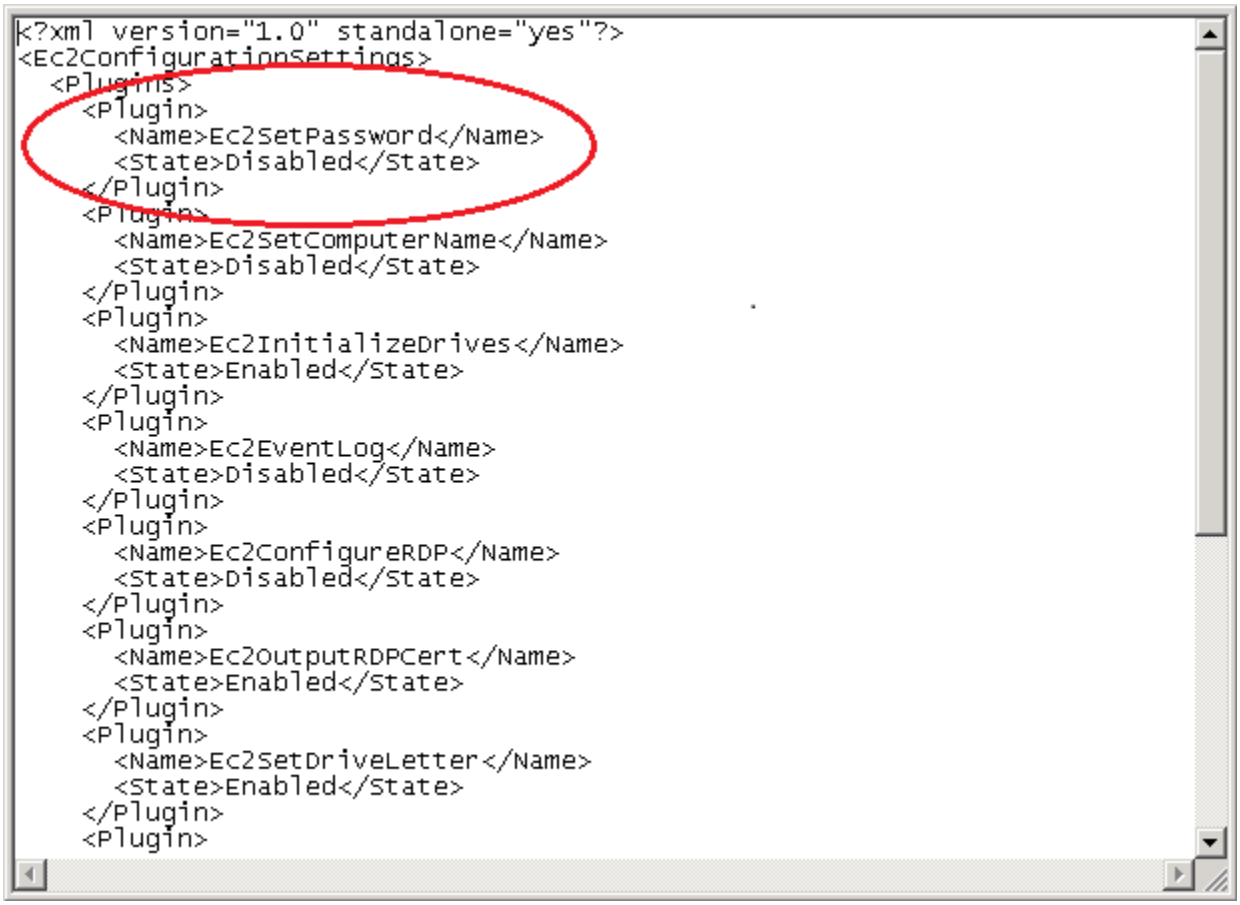
1. Dall'istanza temporanea, modificare il file di configurazione sul volume secondario come segue:

a. Avviare e collegare all'istanza temporanea.

b. Usa le seguenti istruzioni per portare l'unità online: Rendere un volume Amazon EBS disponibile per l'uso.

c. Andare al volume secondario e aprire `\Program Files\Amazon\Ec2ConfigService\Settings\config.xml` con un editor di testo come Notepad.

d. Nella parte superiore del file, cercare il plug-in con il nome `Ec2SetPassword`, come nella schermata. Modificare lo stato da `Disabled` a `Enabled` e salvare il file.



2. Dopo aver modificato il file di configurazione, distaccare il volume secondario dall'istanza temporanea come segue:

a. Tramite l'utilità Disk Management (Gestione disco), portare il volume offline.

b. Disconnettersi dall'istanza temporanea e tornare alla console Amazon EC2.

c. Nel riquadro di navigazione, selezionare Volumes (Volumi), selezionare il volume e quindi scegliere Actions (Operazioni), Detach Volume (Distacca volume). Una volta che lo stato del volume cambia in available (disponibile), continuare con la fase successiva.

Fase 5: Riavviare l'istanza originale.

Dopo aver modificato il file di configurazione, ricollegare il volume all'istanza originale come volume root e collegarlo all'istanza usando la sua coppia di chiavi per recuperare la password dell'amministratore.

1. Collegare nuovamente il volume all'istanza originale come segue:
   a. Nel pannello di navigazione, selezionare Volumes (Volumi), selezionare il volume che è stato scollegato dall'istanza e quindi scegliere Actions (Operazioni), Attach Volume (Collega volume).
   b. Nella finestra di dialogo Attach Volume (Collega volume), sotto Instances (Istanze), iniziare a digitare il nome o l'ID dell'istanza originale, quindi selezionare l'istanza.
   c. Per Device (Dispositivo), digitare **`/dev/sda1`**.
   d. Scegliere Attach (Collega). Dopo che lo stato del volume cambia in `in-use`, passa alla fase successiva.
2. Nel riquadro di navigazione, seleziona Instances (Istanze). Selezionare l'istanza originale e scegliere Instance state (Stato istanza), Start instance (Avvia istanza). Dopo che lo stato dell'istanza cambia in `Running`, passa alla fase successiva.
3. Recuperare la nuova password di amministratore di Windows utilizzando la chiave privata per la nuova coppia di chiavi e connettersi all'istanza. Per ulteriori informazioni, consulta Connessione all'istanza Windows con il protocollo RDP.

   > **Important**
   >
   > Quando viene arrestata e riavviata, l'istanza riceve un nuovo indirizzo IP pubblico. Assicurarsi di collegarsi all'istanza utilizzando il relativo nome DNS pubblico. Per ulteriori informazioni, consulta Cambio di stato di un'istanza Amazon EC2.

4. (Facoltativo) È possibile terminare l'istanza temporanea se non la si utilizza più. Selezionare l'istanza temporanea e scegliere Instance state (Stato istanza), Terminate instance (Termina istanza).

Risoluzione dei problemi di Sysprep relativi alle istanze Amazon EC2 Windows

Se si riscontrano problemi o si ricevono messaggi di errore durante la preparazione dell'immagine, analizzare i registri seguenti. Il percorso del log varia a seconda che si stia eseguendo EC2Config, EC2Launch v1 o EC2Launch v2 con Sysprep.

- `%WINDIR%\Panther\Unattendgc` (EC2Config, EC2Launch v1 e EC2Launch v2)
- `%WINDIR%\System32\Sysprep\Panther` (EC2Config, EC2Launch v1 e EC2Launch v2)
- `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` (solo EC2Config)
- `C:\ProgramData\Amazon\Ec2Config\Logs` (solo EC2Config)
- `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\EC2Launch.log` (solo EC2Launch v1)
- `%ProgramData%\Amazon\EC2Launch\log\agent.log` (solo EC2Launch v2)

Se si riceve un messaggio di errore durante la preparazione dell'immagine con Sysprep, il SO potrebbe non essere raggiungibile. Per rivedere i file di log, è necessario arrestare l'istanza, collegarne il volume principale a un'altra istanza sana come volume secondario, quindi analizzare i log menzionati in precedenza sul volume secondario. Per ulteriori informazioni sullo scopo dei file di registro in base al nome, consulta Windows Setup-Related Log Files nella documentazione Microsoft.

Se si individuano errori nel file di log Unattendgc, utilizzare Microsoft Error Lookup Tool (Strumento di ricerca errori Microsoft) per ulteriori dettagli sull'errore. Il seguente problema riportato nel file di log Unattendgc in genere è il risultato di uno o più profili utente danneggiati sull'istanza:

```
Error [Shell Unattend] _FindLatestProfile failed (0x80070003) [gle=0x00000003]
Error [Shell Unattend] CopyProfile failed (0x80070003) [gle=0x00000003]
```

Sono disponibili due opzioni per la risoluzione di questo problema:

Opzione 1

Utilizza Regedit sull'istanza per cercare la chiave seguente. Verifica che non vi siano chiavi di registro di profilo per un utente eliminato.

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\`

Opzione 2

1. Modifica il file come segue:
   - Windows Server 2012 R2 e versioni precedenti: modifica il file di risposta di EC2Config (`C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml`).
   - Windows Server 2016 e 2019: modifica il file di risposta unattend.xml (`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`).
   - Windows Server 2022: modifica il file di risposta unattend.xml (`C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml`).
2. Passare da `<CopyProfile>true</CopyProfile>` a `<CopyProfile>false</CopyProfile>`.
3. Eseguire Sysprep nuovamente. Questa modifica alla configurazione cancellerà il profilo utente amministratore integrato dopo il completamento di Sysprep.

Risoluzione dei problemi relativi all'istanza Amazon EC2 Linux danneggiata utilizzando EC2Rescue

EC2Rescue per Linux è uno strumento open-source facile da utilizzare che è possibile eseguire sulle istanze Linux Amazon EC2 per diagnosticare, risolvere i problemi e apportare rimedi a errori comuni grazie alla libreria composta da più di 100 moduli. I moduli sono file YAML che contengono uno script BASH o Python e i metadati necessari.

Alcuni casi d'uso generalizzati per le istanze EC2Rescue per Linux includono:

- Raccolta di log di syslog e del gestore di pacchetti
- Raccolta di dati sull'utilizzo delle risorse
- Diagnosi e correzione di parametri problematici noti del kernel e problemi comuni di OpenSSH

> **Note**
>
> Il runbook di `AWSSupport-TroubleshootSSH` AWS Systems Manager Automation installa EC2Rescue per Linux e quindi utilizza lo strumento per verificare o tentare di risolvere i

problemi comuni che impediscono una connessione SSH a un'istanza Linux. Per ulteriori informazioni, consulta AWSSupport-TroubleshootSSH.

Se utilizzi un'istanza Windows, vedi the section called "EC2Rescue per istanze Windows".

Argomenti

- Installazione di EC2Rescue per un'istanza Linux Amazon EC2
- Esecuzione di comandi EC2Rescue su un'istanza Linux Amazon EC2
- Sviluppo dei moduli EC2Rescue per le istanze Linux Amazon EC2

Installazione di EC2Rescue per un'istanza Linux Amazon EC2

Lo strumento EC2Rescue per Linux può essere installato su un'istanza Linux Amazon EC2 in grado di rispettare i prerequisiti seguenti.

Prerequisiti

- Sistemi operativi supportati:
  - Amazon Linux 2
  - Amazon Linux 2016.09+
  - SUSE Linux Enterprise Server 12+
  - RHEL 7 e versioni successive
  - Ubuntu 16.04+
- Requisiti software:
  - Python 2.7.9 e versioni successive o 3.2 e versioni successive

Installazione di EC2Rescue

Il `AWSSupport-TroubleshootSSH` runbook installa EC2Rescue for Linux e quindi utilizza lo strumento per verificare o tentare di risolvere i problemi comuni che impediscono una connessione remota a una macchina Linux tramite SSH. Per ulteriori informazioni e per eseguire questa automazione, consulta Supporto-TroubleshootSSH.

Se il sistema ha la versione Python richiesta, puoi installare la build standard. Altrimenti, puoi installare la build in bundle, che include una copia minima di Python.

Per installare la build standard

1. Da un'istanza Linux attiva, scaricare lo strumento EC2Rescue per Linux:

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz
```

2. (Facoltativo) Verifica della firma del file di installazione di EC2Rescue per Linux. Per ulteriori informazioni, consulta (Facoltativo) Verifica della firma di EC2Rescue per Linux.
3. Scaricare il file di hash sha256:

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sha256
```

4. Verificare l'identità del tarball:

```
sha256sum -c ec2rl.tgz.sha256
```

5. Decomprimere il tarball:

```
tar -xzvf ec2rl.tgz
```

6. Verificare l'installazione elencando il file della guida:

```
cd ec2rl-<version_number>
./ec2rl help
```

Per installare la build in bundle

Per il collegamento di download e l'elenco delle limitazioni, consulta EC2Rescue per Linux su Github.

(Facoltativo) Verifica della firma di EC2Rescue per Linux

Di seguito è riportato il processo consigliato per verificare la validità del pacchetto EC2Rescue for Linux per sistemi operativi. Linux-based

Quando si esegue il download di un'applicazione da Internet, ti consigliamo di autenticare l'identità dell'autore del software e di controllare che l'applicazione non risulti modificata o danneggiata rispetto alla versione pubblicata. Ciò consente di evitare di installare una versione dell'applicazione contenente un virus o altro malware.

Se dopo aver eseguito la procedura descritta in questo argomento risulta che il software di EC2Rescue per Linux è alterato o danneggiato, non eseguire il file di installazione. In caso contrario, contatta Amazon Web Services.

I file EC2Rescue per Linux per sistemi Linux-based operativi sono firmati utilizzando GnuPG, un'implementazione open source dello standard Pretty Good Privacy (OpenPGP) per le firme digitali sicure. GnuPG (noto anche come GPG) fornisce l'autenticazione e il controllo dell'integrità tramite una firma digitale. AWS pubblica una chiave pubblica e delle firme che è possibile utilizzare per verificare il pacchetto EC2Rescue per Linux scaricato. Per ulteriori informazioni su PGP e GnuPG (GPG), vedere. https://www.gnupg.org/

La prima fase prevede la verifica dell'affidabilità dell'autore del software. Scarica la chiave pubblica dell'autore del software, controlla l'autenticità di tale proprietario e quindi aggiungi la chiave pubblica al keyring. Il keyring è una raccolta di chiavi pubbliche nota. Dopo aver confermato l'autenticità della chiave pubblica, puoi usarla per verificare la firma dell'applicazione.

Processi

- Autenticazione e importazione della chiave pubblica
- Verifica della firma del pacchetto

Autenticazione e importazione della chiave pubblica

La successiva fase del processo prevede l'autenticazione della chiave pubblica di EC2Rescue per Linux e la sua aggiunta come chiave affidabile nel keyring GPG.

Per eseguire l'autenticazione e l'importazione della chiave pubblica di EC2Rescue per Linux

1. In un prompt dei comandi, utilizzare il comando seguente per ottenere una copia della chiave pubblica GPG:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.key
   ```

2. In un prompt dei comandi, nella directory in cui è stata salvata `ec2rl.key`, utilizzare il comando seguente per importare la chiave pubblica di EC2Rescue per Linux nel keyring:

   ```
   gpg2 --import ec2rl.key
   ```

   Il comando restituisce risultati simili ai seguenti:

```
gpg: /home/ec2-user/.gnupg/trustdb.gpg: trustdb created
gpg: key 2FAE2A1C: public key "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
 imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

> **Tip**
>
> Se vedi un errore che indica che il comando non può essere trovato, installa l'utilità GnuPG con `apt-get install gnupg2` (Debian-based Linux) o `yum install gnupg2` (Linux basato su Red Hat).

Verifica della firma del pacchetto

Dopo aver installato gli strumenti GPG, avere autenticato e importato la chiave pubblica di EC2Rescue per Linux e avere verificato che la chiave pubblica di EC2Rescue per Linux sia affidabile, puoi verificare la firma dello script di installazione di EC2Rescue per Linux.

Per verificare la firma dello script di installazione di EC2Rescue per Linux

1. Al prompt dei comandi esegui il comando seguente per scaricare il file SIGNATURE per lo script di installazione:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sig
   ```

2. Verifica la firma utilizzando il comando seguente al prompt dei comandi nella directory in cui hai salvato `ec2rl.tgz.sig` e il file di installazione EC2Rescue per Linux. Entrambi i file devono essere presenti.

   ```
   gpg2 --verify ./ec2rl.tgz.sig
   ```

   L'output deve essere simile al seguente:

   ```
   gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
   gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C  C36A F780 4843 2FAE 2A1C
   ```

```
Subkey fingerprint: 966B 0D27 85E9 AEEC 1146  7A9D 8851 1153 6991 ED45
```

Se l'output contiene la frase `Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"`, significa che la firma è stata verificata correttamente ed è possibile eseguire lo script di installazione di EC2Rescue per Linux.

Se l'output include la frase `BAD signature`, controlla di avere eseguito la procedura correttamente. Se il problema persiste, contatta Amazon Web Services e non eseguire il file di installazione scaricato in precedenza.

Di seguito sono elencati i dettagli sugli avvisi che potrebbero comparire:

- WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner. Questo messaggio fa riferimento al livello di affidabilità valutato personalmente in merito al possesso di una chiave pubblica autentica per EC2Rescue per Linux. In un mondo ideale, l'utente visita un ufficio Amazon Web Services e riceve la chiave personalmente. Tuttavia, la prassi normale è scaricare la chiave da un sito Web. In questo caso, il sito Web è un sito Web di Amazon Web Services.
- gpg2: no ultimately trusted keys found. Questo messaggio indica che la chiave specifica non è ritenuta affidabile da te o da un'altra persona da te considerata affidabile.

Per ulteriori informazioni, consulta https://www.gnupg.org/.

Esecuzione di comandi EC2Rescue su un'istanza Linux Amazon EC2

EC2Rescue è uno strumento a riga di comando. Dopo aver installato EC2Rescue sulla tua istanza Linux, puoi ottenere assistenza generale su come utilizzare lo strumento eseguendo `./ec2rl help`. Puoi visualizzare i moduli disponibili eseguendo `./ec2rl list` e puoi ottenere assistenza su un modulo specifico eseguendo `./ec2rl help` *`module_name`*.

Di seguito sono riportate le attività più comuni che puoi eseguire per prendere dimestichezza con questo strumento.

Processi

- Esegui i moduli EC2Rescue
- Carica i risultati del modulo EC2Rescue
- Creare backup di un'istanza Linux Amazon EC2

Esegui i moduli EC2Rescue

Per eseguire tutti i moduli EC2Rescue

Utilizza il comando ./ec2rl run senza specificare parametri aggiuntivi. Alcuni moduli richiedono l'accesso root. Se non sei un utente root, utilizza sudo quando esegui il comando.

```
./ec2rl run
```

Per eseguire un modulo EC2Rescue specifico

Usa il ./ec2rl run comando e per `--only-modules`, specifica il nome del modulo da eseguire. Alcuni moduli richiedono argomenti per utilizzarli.

```
./ec2rl run --only-modules=module_name --arguments
```

Ad esempio, per eseguire il modulo dig per interrogare il dominio `amazon.com`, utilizza il seguente comando.

```
./ec2rl run --only-modules=dig --domain=amazon.com
```

Per visualizzare i risultati di un modulo EC2Rescue

Esegui il modulo, poi visualizza il file di log in `cat /var/tmp/ec2rl/`*`logfile_location`*. Ad esempio, il file di log per il modulo dig si trova nella seguente posizione:

```
cat /var/tmp/ec2rl/timestamp/mod_out/run/dig.log
```

Carica i risultati del modulo EC2Rescue

Se hai Supporto richiesto i risultati per un modulo EC2Rescue, puoi caricare il file di registro utilizzando lo strumento EC2Rescue. Puoi caricare i risultati in una posizione fornita da Supporto o in un bucket Amazon S3 di tua proprietà.

Per caricare i risultati in una posizione fornita da Supporto

Utilizza il comando ./ec2rl upload. Per `--upload-directory`, specifica la posizione del file di log. Per `--support-url`, specifica l'URL fornito da Supporto.

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/logfile_location --support-
url="url_provided_by_aws_support"
```

Per caricare i risultati in un bucket Amazon S3

Utilizza il comando ./ec2rl upload. Per `--upload-directory`, specifica la posizione del file di log. Per `--presigned-url`, specifica un URL predefinito per il bucket S3. Per ulteriori informazioni sulla generazione di URL prefirmati per Amazon S3, consulta Uploading Objects Using URLs. Pre-Signed

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/logfile_location --presigned-
url="presigned_s3_url"
```

Creare backup di un'istanza Linux Amazon EC2

Puoi usare EC2Rescue per eseguire il backup dell'istanza Linux creando un'AMI o creando snapshot dei volumi collegati.

Per creare un'AMI

Utilizza il comando `./ec2rl run` e per `--backup`, specifica `ami`.

```
./ec2rl run --backup=ami
```

Per creare snapshot a più volumi di tutti i volumi collegati

Utilizza il comando `./ec2rl run` e per `--backup`, specifica `allvolumes`.

```
./ec2rl run --backup=allvolumes
```

Per creare uno snapshot di uno specifico volume collegato

Usa il comando `./ec2rl run` e per `--backup`, specifica l'ID del volume di cui eseguire il backup.

```
./ec2rl run --backup=vol-01234567890abcdef
```

Sviluppo dei moduli EC2Rescue per le istanze Linux Amazon EC2

I moduli sono scritti in YAML, uno standard di serializzazione dei dati. Il file YAML di un modulo è formato da un singolo documento che rappresenta il modulo e i relativi attributi.

Aggiunta di attributi di modulo

Nella tabella seguente vengono elencati gli attributi di modulo disponibili.

Attributo	Descrizione
name	Il nome del modulo. Il nome non deve superare i 18 caratteri.
version	Il numero di versione del modulo.
title	Un breve titolo descrittivo del modulo. Questo valore non deve superare i 50 caratteri.

helptext	La descrizione estesa del modulo. Ogni riga non deve superare i 75 caratteri. Se il modulo consuma argomenti, obbligatori o facoltativi, includili nel valore helptext.
	
	Ad esempio:
	
	`helptext: !!str |`
	`  Collect output from ps for system analysis`
	`  Consumes --times= for number of times to repeat`
	`  Consumes --period= for time period between repetition`

placement	La fase in cui eseguire il modulo. Valori supportati: • prediagnostic • run • postdiagnostic
linguaggio	Il linguaggio in cui è scritto il codice del modulo. Valori supportati: • bash

Attributo	Descrizione
	• python **Note** Il codice Python deve essere compatibile con Python 2.7.9 e versioni successive e Python 3.2 e versioni successive.
remediation	Indica se il modulo supporta le azioni di correzione. I valori supportati sono `True` o `False`. Il modulo viene impostato su `False` per impostazione predefinita se questo valore è assente, rendendo l'attributo facoltativo per i moduli che non supportano le azioni di correzione.
content	L'interezza del codice dello script.
vincolo	Il nome dell'oggetto contenente i valori di vincolo.
domain	Un descrittore del raggruppamento o della classificazione del modulo. L'insieme dei moduli inclusi utilizza i domini seguenti: • applicazione • net • so • prestazioni

Attributo	Descrizione
classe	Un descrittore del tipo di attività effettuato dal modulo. L'insieme dei moduli inclusi utilizza le classi seguenti: • collect (raccoglie l'output dai programmi) • diagnosi (pass/fail basata su una serie di criteri) • gather (copia i file e li scrive su un file specifico)
distro	L'elenco delle distribuzioni Linux supportate da questo modulo. Il set di moduli inclusi utilizza le distribuzioni seguenti: • alami (Amazon Linux) • rhel • ubuntu • suse
obbligatorio	Gli argomenti obbligatori che il modulo consuma dalle opzioni della CLI.
facoltativo	Gli argomenti facoltativi che il modulo può utilizzare.
software	I file eseguibili del software utilizzati nel modulo. Questo attributo è progettato per specificare un software non installato per impostazione predefinita. La logica EC2Rescue per Linux assicura che tali programmi siano presenti ed eseguibili prima di eseguire il modulo.

Attributo	Descrizione
package	Il pacchetto software di origine di un file eseguibile. Questo attributo è progettato per fornire dettagli estesi sul pacchetto con il software, incluso un URL per ottenere o scaricare ulteriori informazioni.
sudo	Indica se l'accesso root è obbligatorio per l'esecuzione del modulo. Non è necessario implementare i controlli sudo nello script del modulo. Se il valore è true, la logica EC2Rescue per Linux esegue il modulo soltanto se l'utente che lo esegue dispone dell'accesso root.
perfimpact	Indica se il modulo può avere un significativo impatto sulle prestazioni nell'ambiente in cui viene eseguito. Se il valore è true e l'argomen to `--perfimpact=true` non è presente, il modulo viene ignorato.
parallelexclusive	Specifica un programma che richiede reciproca esclusività. Ad esempio, tutti i moduli con la specifica "bpf" vengono eseguiti in modo seriale.

Aggiunta di variabili di ambiente

Nella tabella seguente vengono elencate le variabili di ambiente disponibili.

Variabile di ambiente	Descrizione
`EC2RL_CALLPATH`	Il percorso a `ec2rl.py`. Questo percorso può essere utilizzato per individuare la directory lib

Variabile di ambiente	Descrizione
	e per utilizzare i moduli Python gestiti da un fornitore.
`EC2RL_WORKDIR`	La directory tmp principale dello strumento di diagnostica. Valore predefinito: `/var/tmp/ec2rl` .
`EC2RL_RUNDIR`	La directory in cui viene archiviato tutto l'output. Valore predefinito: `/var/tmp/ec2rl/<date&timestamp>` .
`EC2RL_GATHEREDDIR`	La directory root in cui inserire i dati raccolti sul modulo. Valore predefinito:`/var/tmp/ec2rl/<date&timestamp>/mod_out/gathered/` .
`EC2RL_NET_DRIVER`	Il driver in uso per la prima interfaccia di rete non virtuale sull'istanza (in ordine alfabetico). Esempi: • xen_netfront • ixgbevf • ena
`EC2RL_SUDO`	Impostato su true se EC2Rescue per Linux è in esecuzione come root; altrimenti, è impostato su false.

Variabile di ambiente	Descrizione
`EC2RL_VIRT_TYPE`	Il tipo di virtualizzazione fornito dai metadati dell'istanza. Esempi: • default-hvm • default-paravirtual
`EC2RL_INTERFACES`	Un elenco enumerato delle interfacce sul sistema. Il valore è una stringa contenente nomi, ad esempio `eth0eth1`, e così via. Viene generato da `functions.bash` ed è disponibile solo per i moduli che lo hanno generato.

Utilizzo della sintassi YAML

Annota quanto riportato di seguito durante la costruzione dei file YAML del modulo:

- I trattini tripli (`---`) denotano l'inizio esplicito di un documento.
- Il tag `!ec2rlcore.module.Module` comunica al parser YAML il costruttore da richiamare durante la creazione dell'oggetto dal flusso di dati. È possibile trovare il costruttore nel file `module.py`.
- Il tag `!!str` comunica al parser YAML di non tentare di determinare il tipo di dati, ma di interpretare i contenuti come un valore letterale di stringa.
- Il carattere barra verticale (`|`) comunica al parser YAML che il valore è un valore scalare di stile letterale. In questo caso, il parser include tutti gli spazi vuoti. Ciò è importante per i moduli perché vengono mantenuti i caratteri di rientro e nuova riga.
- Come puoi vedere negli esempi seguenti, il rientro standard di YAML è di due spazi. Assicurati di mantenere il rientro standard (ad esempio, quattro spazi per Python) nello script e di far rientrare di due spazi tutto il contenuto all'interno del file del modulo.

Moduli di esempio

Esempio uno (`mod.d/ps.yaml`):

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
name: !!str ps
path: !!str
version: !!str 1.0
title: !!str Collect output from ps for system analysis
helptext: !!str |
  Collect output from ps for system analysis
  Requires --times= for number of times to repeat
  Requires --period= for time period between repetition
placement: !!str run
package:
  - !!str
language: !!str bash
content: !!str |
  #!/bin/bash
  error_trap()
  {
      printf "%0.s=" {1..80}
      echo -e "\nERROR: "$BASH_COMMAND" exited with an error on line ${BASH_LINENO[0]}"
      exit 0
  }
  trap error_trap ERR

  # read-in shared function
  source functions.bash
  echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every
 $period seconds."
  for i in $(seq 1 $times); do
      ps auxww
      sleep $period
  done
constraint:
  requires_ec2: !!str False
  domain: !!str performance
  class: !!str collect
  distro: !!str alami ubuntu rhel suse
  required: !!str period times
  optional: !!str
  software: !!str
  sudo: !!str False
  perfimpact: !!str False
  parallelexclusive: !!str
```

Risoluzione dei problemi relativi all'istanza Amazon EC2 Windows danneggiata utilizzando EC2Rescue

EC2Rescue for Windows Server è uno strumento facile da utilizzare che puoi eseguire sulle istanze Amazon EC2 Windows Server per diagnosticare e risolvere i possibili problemi rilevati. Si tratta di uno strumento utile per raccogliere i file di log e risolvere i problemi, nonché per individuare in modo proattivo le possibili aree problematiche. Consente inoltre di esaminare i volumi root Amazon EBS di altre istanze e raccogliere i log rilevanti per la risoluzione dei problemi delle istanze Windows Server che utilizzano tali volumi. Di seguito sono elencati alcuni problemi comuni che EC2Rescue può risolvere:

- Problemi di connettività delle istanze dovuti al firewall, al Remote Desktop Protocol (RDP) o alla configurazione dell'interfaccia di rete
- Problemi di avvio del sistema operativo dovuti a un errore di arresto, al ciclo di avvio o al registro danneggiato
- Problemi che potrebbero richiedere un'analisi e una risoluzione avanzate dei log

EC2Rescue per Windows Server dispone di due moduli diversi:

- Un modulo di raccolta dati che raccoglie dati da tutte le diverse fonti
- Un modulo di analisi che analizza i dati raccolti in base a una serie di regole predefinite per identificare gli eventuali problemi e fornire suggerimenti

Lo strumento EC2Rescue for Windows Server viene eseguito solo sulle istanze Amazon EC2 che eseguono Windows Server 2012 e versioni successive. All'avvio lo strumento controlla se viene eseguito su un'istanza Amazon EC2.

> **Note**
>
> Il runbook di `AWSSupport-ExecuteEC2Rescue` AWS Systems Manager automazione utilizza lo strumento EC2Rescue per risolvere i problemi e, ove possibile, risolvere i problemi di connettività comuni con l'istanza EC2 specificata. Per ulteriori informazioni e per eseguire questa automazione, vedere >. AWSSupport-ExecuteEC2Rescue

Se utilizzi un'istanza Linux, consulta the section called “EC2Rescue for istanze Linux”.

Argomenti

- Risoluzione dei problemi relativi alle istanze Windows danneggiate con la GUI EC2Rescue
- Risoluzione dei problemi relativi alle istanze Windows danneggiate con la CLI EC2Rescue
- Risoluzione dei problemi relativi alle istanze Windows danneggiate con CLI EC2Rescue e Systems Manager

Risoluzione dei problemi relativi alle istanze Windows danneggiate con la GUI EC2Rescue

EC2Rescue per Windows Server può eseguire le seguenti analisi su istanze offline:

Opzione	Descrizione

Diagnose and Rescue (Esegui diagnostica e recupero)	EC2Rescue for Windows Server può rilevare e risolvere dei problemi con le seguenti impostazioni del servizio:
	• System Time (Ora di sistema)
	  • RealTimeisUniversal- Rileva se la chiave di `RealTimeisUniversal` registro è abilitata. Se è disabilitata, l'ora del sistema Windows cambia quando il fuso orario viene impostato su un valore diverso da UTC.
	• Windows Firewall
	  • Domain networks (Reti di dominio): rileva se il profilo di Windows Firewall corrente è abilitato o disabilitato.
	  • Private networks (Reti private): rileva se il profilo di Windows Firewall corrente è abilitato o disabilitato.
	  • Guest or public networks (Guest o reti pubbliche): rileva se il profilo di Windows Firewall corrente è abilitato o disabilitato.

Opzione	Descrizione

	• Remote Desktop (Desktop remoto)
	  • Service Start (Avvio servizio): rileva se il servizio Remote Desktop (Desktop remoto) è abilitato.
	  • Connessione Desktop remoto: rileva se questo servizio è abilitato.
	  • TCP Port (Porta TCP): rileva su quale porta il Remote Desktop (Desktop remoto) è in ascolto.
	• EC2Config (Windows Server 2012 R2 e versioni precedenti)
	  • Installation (Installazione): rileva quale versione di EC2Config è installata.
	  • Service Start (Avvio servizio): rileva se il servizio EC2Config è abilitato.
	  • Ec2SetPassword- Genera una nuova password di amministratore.
	  • Ec2HandleUserData- Consente di eseguire uno script di dati utente al successivo avvio dell'istanza.
	• EC2Launch (Windows Server 2016 e versioni successive)
	  • Installation (Installazione): rileva quale versione di EC2Launch è installata.
	  • Ec2SetPassword- Genera una nuova password di amministratore.
	• Interfaccia di rete

Opzione	Descrizione
	• DHCP Service Startup (Avvio servizio DHCP): rileva se il servizio DHCP è abilitato. • Ethernet detail (Dettagli Ethernet): visualizza le informazioni sulla versione del driver di rete, se rilevata. • DHCP on Ethernet (DHCP su Ethernet): rileva se DHCP è abilitato. • Stato della firma su disco • Firma su disco e Firma sul database di configurazione di avvio (BCD): rileva se la firma del disco e la firma BCD sono uguali. Se i valori sono diversi, EC2Rescue prova a sovrascrivere la firma del disco con la firma su BCD.
Ripristino	Eseguire una delle seguenti operazioni: • Last Known Good Configuration (Ultima configurazione valida nota): cerca di avviare l'istanza con l'ultimo stato avviabile noto. • Restore registry from backup (Ripristina registro da backup): ripristina il registro da `\Windows\System32\config\RegBack` .
Capture Logs (Acquisisci log)	Permette di acquisire i log relativi all'istanza per l'analisi.

EC2Rescue for Windows Server può raccogliere i seguenti dati dalle istanze attive e offline:

Elemento	Descrizione
Event Log (Log eventi)	Raccoglie i log degli eventi relativi ad applicazione, sistema ed EC2Config.
Registry	Raccoglie gli hive `SYSTEM` e `SOFTWARE`.
Windows Update Log (Log aggiornamenti di Windows)	Raccoglie i file di log generati da Windows Update. **Note** In Windows Server 2016 e versioni successive, il log viene raccolto in formato Event Tracing for Windows (ETW).
Sysprep Log (Log Sysprep)	Raccoglie i file di log generati dallo strumento di preparazione del sistema Windows (Sysprep).
Driver Setup Log	Raccoglie i log di Windows SetupAPI (`setupapi.dev.log` e `setupapi.setup.log`).
Boot Configuration (Configurazione di avvio)	Raccoglie l'hive `HKEY_LOCAL_MACHINE\BCD00000000`.
Memory Dump (Dump memoria)	Raccoglie i file dei dump della memoria esistenti sull'istanza.
EC2Config File (File EC2Config)	Raccoglie i file di log generati dal servizio EC2Config.
EC2Launch File (File EC2Launch)	Raccoglie i file di log generati dagli script EC2Launch.
SSM Agent File (File agente SSM)	Raccoglie i file di log generati dai log SSM Agent e Patch Manager.

Elemento	Descrizione
File EC2 ElasticGPUs	Raccoglie i log degli eventi relativi alle GPU elastiche.
ECS	Raccoglie i log relativi ad Amazon ECS.
CloudEndure	Raccoglie i file di registro relativi all' CloudEndure agente.
AWS Replication Agent per file di registro MGN o DRS	Raccoglie i file di registro relativi a o. AWS Transform MGN AWS Elastic Disaster Recovery

EC2Rescue for Windows Server può raccogliere i seguenti dati aggiuntivi da istanze attive:

Elemento	Descrizione
System Information (Informazioni sul sistema)	Raccoglie MSInfo32.
Group Policy Result	Raccoglie un report relativo alle policy del gruppo.

Analisi di un'istanza offline

L'opzione Offline Instance (Istanza offline) risulta utile per eseguire il debug dei problemi di avvio con le istanze di Windows.

Per eseguire un'operazione su un'istanza offline

1. Da un'istanza di Windows Server in esecuzione, scaricare lo strumento EC2Rescue for Windows Server ed estrarre i file.

   È possibile eseguire il PowerShell comando seguente per scaricare EC2Rescue senza modificare la configurazione ESC (Enhanced Security Configuration) di Internet Explorer:

```
Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
```

Con questo comando verrà scaricato il file .zip EC2Rescue sul desktop dell'utente che ha attualmente eseguito l'accesso.

> **Note**
>
> Se si riceve un errore durante il download del file e si utilizza Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il terminale. PowerShell Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il comando seguente e riprovare:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

2. Arrestare l'istanza in errore, se non è già stata arrestata.
3. Scollegare il volume root EBS dall'istanza in errore e collegare il volume a un'istanza Windows in esecuzione in cui sia installato EC2Rescue for Windows Server.
4. Eseguire lo strumento EC2Rescue for Windows Server sull'istanza in esecuzione e scegliere Offline Instance (Istanza offline).
5. Selezionare il disco del volume appena montato e scegliere Next (Successivo).
6. Confermare la selezione del disco e scegliere Yes (Sì).
7. Scegliere l'opzione relativa all'istanza offline da eseguire e selezionare Next (Successivo).

Lo strumento EC2Rescue for Windows Server analizza il volume e raccoglie le informazioni relative alla risoluzione dei problemi in base ai file di log selezionati.

Raccolta di dati da un'istanza attiva

Puoi raccogliere i log e altri dati da un'istanza attiva.

Per raccogliere dati da un'istanza attiva

1. Connettersi all'istanza Windows.
2. Scaricare lo strumento EC2Rescue for Windows Server nell'istanza Windows corrente ed estrarre i file.

È possibile eseguire il PowerShell comando seguente per scaricare EC2Rescue senza modificare la configurazione ESC (Enhanced Security Configuration) di Internet Explorer:

```
Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
```

Con questo comando verrà scaricato il file .zip EC2Rescue sul desktop dell'utente che ha attualmente eseguito l'accesso.

> **Note**
>
> Se si riceve un errore durante il download del file e si utilizza Windows Server 2016 o versioni precedenti, potrebbe essere necessario abilitare TLS 1.2 per il terminale. PowerShell Puoi abilitare TLS 1.2 per la PowerShell sessione corrente con il comando seguente e riprovare:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

3. Aprire l'applicazione EC2Rescue for Windows Server e accettare l'accordo di licenza.
4. Scegliere Next (Successivo), Current instance (Istanza corrente), Capture logs (Acquisisci log).
5. Selezionare i tipi di dati da raccogliere e scegliere Collect... (Raccogli...). Leggere l'avviso e scegliere Yes (Sì) per continuare.
6. Scegliere un nome di file e la posizione per il file .zip, quindi selezionare Save (Salva).
7. Quando EC2Rescue for Windows Server ha completato l'operazione, scegliere Open Containing Folder (Apri cartella superiore) per visualizzare il file .zip file.
8. Scegliere Finish (Fine).

Risoluzione dei problemi relativi alle istanze Windows danneggiate con la CLI EC2Rescue

L'interfaccia a riga di comando (CLI) di EC2Rescue for Windows Server ti permette di eseguire un plugin EC2Rescue for Windows Server (noto anche come "operazione") a livello di programmazione.

Lo strumento EC2Rescue for Windows Server è caratterizzato da due modalità di esecuzione:

- /online – Permette di eseguire l'operazione sull'istanza su cui è installato EC2Rescue for Windows Server, ad esempio la raccolta dei file di log.
- /offline<device_id> – Permette di eseguire l'operazione sul volume root offline collegato a un'istanza Amazon EC2 di Windows distinta, su sui è installato EC2Rescue for Windows Server.

Scaricare lo strumento EC2Rescue for Windows Server nell'istanza Windows corrente ed estrarre i file. Puoi visualizzare il file di aiuto con il seguente comando:

```
EC2RescueCmd.exe /help
```

EC2Rescue for Windows Server può eseguire le seguenti operazioni su un'istanza Amazon EC2 di Windows:

- Operazione di raccolta
- Operazione di recupero
- Operazione di ripristino

Operazione di raccolta

> **Note**
>
> Puoi raccogliere tutti i log, un intero gruppo di log oppure un singolo log all'interno di un gruppo.

EC2Rescue for Windows Server può raccogliere i seguenti dati dalle istanze attive e offline.

Gruppo di log	Log disponibili	Descrizione
`all`		Raccoglie tutti i log disponibili.
`eventlog`	• `'Application'` • `'System'` • `'EC2ConfigService'`	Raccoglie i log degli eventi relativi ad applicazione, sistema ed EC2Config.

Gruppo di log	Log disponibili	Descrizione
memory-dump	• 'Memory Dump File' • 'Mini Dump Files'	Raccoglie i file dei dump della memoria esistenti sull'istanza.
ec2config	• 'Log Files' • 'Configuration Files'	Raccoglie i file di log generati dal servizio EC2Config.
ec2launch	• 'Logs' • 'Config'	Raccoglie i file di log generati dagli script EC2Launch.
ssm-agent	• 'Log Files' • 'Patch Baseline Logs' • 'InstanceData'	Raccoglie i file di log generati dai log SSM Agent e Patch Manager.
sysprep	'Log Files'	Raccoglie i file di log generati dallo strumento di preparazione del sistema Windows (Sysprep).
driver-setup	• 'SetupAPI Log Files' • 'DPInst Log File' • 'AWS PV Setup Log File'	Raccoglie i log di Windows SetupAPI (setupapi.dev.log e setupapi.setup.log).
registry	• 'SYSTEM' • 'SOFTWARE' • 'BCD'	Raccoglie gli hive SYSTEM e SOFTWARE.
egpu	• 'Event Log' • 'System Files'	Raccoglie i log degli eventi relativi alle GPU elastiche.
boot-config	'BCDEDIT Output'	Raccoglie l'hive HKEY_LOCAL_MACHINE\BCD00000000 .

Gruppo di log	Log disponibili	Descrizione
`windows-update`	`'Log Files'`	Raccoglie i file di log generati da Windows Update. **Note** In Windows Server 2016 e versioni successive, il log viene raccolto in formato Event Tracing for Windows (ETW).
`cloudendure`	• `'Migrate Script Logs'` • `'Driver Logs'` • `'CloudEndure File List'`	Raccoglie i file di registro relativi all'agente. CloudEndure

EC2Rescue for Windows Server può raccogliere i seguenti dati aggiuntivi da istanze attive.

Gruppo di log	Log disponibili	Descrizione
`system-info`	`'MSInfo32 Output'`	Raccoglie `MSInfo32`.
`gpresult`	`'GPResult Output'`	Raccoglie un report relativo alle policy del gruppo.

Sono disponibili le seguenti opzioni:

- /output: <output FilePath > - Posizione del percorso del file di destinazione richiesta per salvare i file di registro raccolti in formato zip.
- /no-offline: attributo opzionale utilizzato in modalità non in linea. Non imposta il volume sullo stato offline dopo il completamento dell'operazione.

- /no-fix-signature: attributo opzionale utilizzato in modalità non in linea. Non corregge un possibile conflitto di firma del disco dopo il completamento dell'operazione.

Esempi

Di seguito sono elencati alcuni esempi di utilizzo della CLI EC2Rescue for Windows Server.

Esempi della modalità online

Per raccogliere tutti i log disponibili:

```
EC2RescueCmd /accepteula /online /collect:all /output:<outputFilePath>
```

Per raccogliere solo un gruppo di log specifico:

```
EC2RescueCmd /accepteula /online /collect:ec2config /output:<outputFilePath>
```

Per raccogliere singoli log all'interno di un gruppo di log:

```
EC2RescueCmd /accepteula /online /collect:'ec2config.Log Files,driver-setup.SetupAPI
 Log Files' /output:<outputFilePath>
```

Esempi della modalità offline

Per raccogliere tutti i log disponibili da un volume EBS. Il volume è specificato dal valore device_id.

```
EC2RescueCmd /accepteula /offline:xvdf /collect:all /output:<outputFilePath>
```

Per raccogliere solo un gruppo di log specifico:

```
EC2RescueCmd /accepteula /offline:xvdf /collect:ec2config /output:<outputFilePath>
```

Operazione di recupero

EC2Rescue for Windows Server può rilevare e risolvere dei problemi con le seguenti impostazioni del servizio:

Gruppo di servizi	Operazioni disponibili	Descrizione
`all`		

Gruppo di servizi	Operazioni disponibili	Descrizione
`system-time`	`'RealTimeIsUniversal'`	System Time (Ora di sistema) • RealTimeisUniversal- Rileva se la chiave di `RealTimeisUniversal` registro è abilitata. Se è disabilitata, l'ora del sistema Windows cambia quando il fuso orario viene impostato su un valore diverso da UTC.
`firewall`	• `'Domain networks'` • `'Private networks'` • `'Guest or public networks'`	Windows Firewall • Domain networks (Reti di dominio): rileva se il profilo di Windows Firewall corrente è abilitato o disabilitato. • Private networks (Reti private): rileva se il profilo di Windows Firewall corrente è abilitato o disabilitato. • Guest or public networks (Guest o reti pubbliche): rileva se il profilo di Windows Firewall corrente è abilitato o disabilitato.

Gruppo di servizi	Operazioni disponibili	Descrizione
rdp	• 'Service Start' • 'Remote Desktop Connections' • 'TCP Port'	Remote Desktop (Desktop remoto) • Service Start (Avvio servizio): rileva se il servizio Remote Desktop (Desktop remoto) è abilitato. • Connessione Desktop remoto: rileva se questo servizio è abilitato. • TCP Port (Porta TCP): rileva su quale porta il Remote Desktop (Desktop remoto) è in ascolto.
ec2config	• 'Service Start' • 'Ec2SetPassword' • 'Ec2HandleUserData'	EC2Config • Service Start (Avvio servizio): rileva se il servizio EC2Config è abilitato. • Ec2SetPassword- Genera una nuova password di amministratore. • Ec2HandleUserData- Consente di eseguire uno script di dati utente al successivo avvio dell'ista nza.
ec2launch	'Reset Administrator Password'	Genera una nuova password per l'amministratore di Windows.

Gruppo di servizi	Operazioni disponibili	Descrizione
`network`	`'DHCP Service Startup'`	Interfaccia di rete • DHCP Service Startup (Avvio servizio DHCP): rileva se il servizio DHCP è abilitato.

Sono disponibili le seguenti opzioni:

- /level:<level>: attributo opzionale per il livello di controllo che l'operazione deve attivare. I valori consentiti sono: `information`, `warning`, `error`, `all`. Per impostazione predefinita, è impostato su `error`.
- /check-only: attributo opzionale che genera un report, ma non apporta modifiche al volume non in linea.

> **Note**
>
> Se EC2Rescue per Windows Server rileva un possibile conflitto di firma del disco, per impostazione predefinita corregge la firma dopo il completamento del processo offline, anche quando si utilizza l'opzione `/check-only`. Devi utilizzare l'opzione `/no-fix-signature` per impedire la correzione.

- /no-offline: attributo opzionale che impedisce l'impostazione del volume sullo stato non in linea dopo il completamento dell'operazione.
- /no-fix-signature: attributo opzionale che non corregge un possibile conflitto di firma del disco dopo il completamento dell'operazione.

Esempi di recupero

Di seguito sono elencati alcuni esempi di utilizzo della CLI EC2Rescue for Windows Server. Il volume è specificato dal valore device_id.

Per tentare di correggere tutti i problemi rilevati su un volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:all
```

Per tentare di correggere tutti i problemi all'interno di un gruppo di servizi su un volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:firewall
```

Per tentare di correggere un problema specifico all'interno di un gruppo di servizi su un volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:rdp.'Service Start'
```

Per specificare più problemi da risolvere su un volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:'system-
time.RealTimeIsUniversal,ec2config.Service Start'
```

Operazione di ripristino

EC2Rescue for Windows Server può rilevare e risolvere dei problemi con le seguenti impostazioni del servizio:

Gruppo di servizi	Operazioni disponibili	Descrizione
Restore Last Known Good Configuration (Ripristina ultima configurazione valida nota)	`lkgc`	Last Known Good Configuration (Ultima configurazione valida nota): cerca di avviare l'istanza con l'ultimo stato avviabile noto.
Restore Windows registry from latest backup (Ripristina registro di Windows da ultimo backup)	`regback`	Restore registry from backup (Ripristina registro da backup): ripristina il registro da `\Windows\System32\config\RegBack` .

Sono disponibili le seguenti opzioni:

- /no-offline – Attributo opzionale che impedisce l'impostazione del volume sullo stato offline dopo il completamento dell'operazione.
- /no-fix-signature – Attributo opzionale che non corregge un possibile conflitto di firma del disco dopo il completamento dell'operazione.

Esempi di ripristino

Di seguito sono elencati alcuni esempi di utilizzo della CLI EC2Rescue for Windows Server. Il volume è specificato dal valore device_id.

Per ripristinare l'ultima configurazione valida nota su un volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:lkgc
```

Per ripristinare l'ultimo backup del registro di Windows su un volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:regback
```

Risoluzione dei problemi relativi alle istanze Windows danneggiate con CLI EC2Rescue e Systems Manager

Supporto fornisce un documento Systems Manager Run Command per interfacciarsi con l' Manager-enabled istanza Systems per eseguire EC2Rescue per Windows Server. Il documento Run Command è denominato `AWSSupport-RunEC2RescueForWindowsTool`.

Questo documento Run Command per Systems Manager esegue le seguenti attività:

- Scarica e verifica EC2Rescue for Windows Server.
- Importa un PowerShell modulo per facilitare l'interazione con lo strumento.
- Viene eseguito EC2RescueCmd con il comando e i parametri forniti.

Il documento Run Command per Systems Manager accetta tre parametri:

- Comando – L'azione EC2Rescue for Windows Server. I valori consentiti correnti sono:
  - ResetAccess—Reimposta la password dell'amministratore locale. La password dell'amministratore locale dell'istanza corrente verrà reimpostata; la password generata casualmente verrà archiviata in modo sicuro in Parameter Store come `/EC2Rescue/Password/<INSTANCE_ID>`. Se selezioni questa operazione e non specifichi alcun parametro, le password vengono crittografate automaticamente con la Chiave KMS predefinita. Facoltativamente, puoi specificare l'ID Chiave KMS nel parametro Parameters per crittografare la password con una chiave personalizzata.

- CollectLogs—Esegue EC2Rescue for Windows Server con l'azione. `/collect:all` Se selezioni questa operazione, `Parameters` deve includere un nome bucket Amazon S3 in cui caricare i log.
- FixAll—Esegue EC2Rescue for Windows Server con l'azione. `/rescue:all` Se selezioni questa operazione, `Parameters` deve includere il nome del dispositivo a blocchi da recuperare.

- Parametri: i PowerShell parametri da passare per il comando specificato.

Requisiti

Per eseguire l'ResetAccessazione, alla tua istanza Amazon EC2 deve essere allegata una policy che conceda le autorizzazioni per scrivere la password crittografata in Parameter Store. Dopo aver collegato la policy, attendi alcuni minuti prima di provare a reimpostare la password di un'istanza dopo che hai associato questa policy al ruolo IAM correlato.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    }
  ]
}
```

Se utilizzi una chiave KMS personalizzata, non la chiave KMS predefinita, utilizza invece questa policy.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/<kmskeyid>"
      ]
    }
  ]
}
```

Visualizzazione del file JSON per il documento

La procedura seguente descrive come visualizzare il file JSON per questo documento.

Per visualizzare il file JSON per il documento Run Command per Systems Manager

1. Apri la console all' AWS Systems Manager indirizzo. https://console.aws.amazon.com/systems-manager/
2. Nel riquadro di navigazione, espandi Strumenti di gestione delle modifiche e scegli Documenti.
3. Nella barra di ricerca, inserisci `AWSSupport-RunEC2RescueForWindowsTool`, quindi seleziona il documento `AWSSupport-RunEC2RescueForWindowsTool`.
4. Scegli la scheda Contenuti.

Esempi

Di seguito sono descritti alcuni esempi su come utilizzare il documento Run Command di Systems Manager per eseguire EC2Rescue for Windows Server utilizzando AWS CLI. Per ulteriori informazioni sull'invio di comandi tramite AWS CLI, vedere https://docs.aws.amazon.com/cli/latest/reference/ssm/send-command.html send-command.

Esempi

- Tentare di correggere tutti i problemi rilevati su un volume root offline
- Raccolta dei log dall'istanza Amazon EC2 Windows corrente
- Reimpostazione della password dell'amministratore locale

Tentare di correggere tutti i problemi rilevati su un volume root offline

Tentare di correggere tutti i problemi rilevati su un volume root offline collegati a un'istanza Amazon EC2 Windows:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=FixAll, Parameters='xvdf'" --output
 text
```

Raccolta dei log dall'istanza Amazon EC2 Windows corrente

Raccogliere tutti i log dall'istanza di Amazon EC2 Windows online corrente e caricarli su un bucket Amazon S3:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=CollectLogs, Parameters='amzn-s3-
demo-bucket'" --output text
```

Reimpostazione della password dell'amministratore locale

Gli esempi seguenti illustrano i metodi che puoi utilizzare per reimpostare la password dell'amministratore locale. L'output restituisce un collegamento a Parameter Store, dove è disponibile la password sicura generata causalmente che potrai utilizzare per eseguire una connessione RDP all'istanza Amazon EC2 Windows come amministratore locale.

Reimposta la password dell'amministratore locale di un'istanza online utilizzando il file /ssm predefinito: AWS KMS key alias/aws

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=ResetAccess" --output text
```

Per reimpostare la password dell'amministratore locale di un'istanza online utilizzando una Chiave KMS:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=ResetAccess, Parameters=a133dc3c-
a2g4-4fc6-a873-6c0720104bf0" --output text
```

> **Note**
>
> In questo esempio la Chiave KMS è `a133dc3c-a2g4-4fc6-a873-6c0720104bf0`.

Console seriale EC2 per istanze

Con la console seriale EC2, è possibile accedere alla porta seriale dell'istanza Amazon EC2 e utilizzarla per risolvere problemi di avvio, configurazione di rete e di altro tipo. La console seriale non richiede che l'istanza abbia funzionalità di rete. Con la console seriale, è possibile immettere comandi a un'istanza come se la tastiera e il monitor fossero collegati direttamente alla porta seriale dell'istanza. La sessione della console seriale resta attiva durante il riavvio e l'arresto dell'istanza. Durante il riavvio, sarà possibile visualizzare tutti i messaggi di avvio dall'inizio.

L'accesso alla console seriale non è disponibile per impostazione predefinita. L'organizzazione deve concedere l'accesso dell'account alla console seriale e configurare le policy IAM per concedere agli utenti l'accesso alla console seriale. L'accesso alla console seriale può essere controllato a livello granulare utilizzando ID istanza, tag delle risorse e altre leve IAM. Per ulteriori informazioni, consulta Configurazione dell'accesso alla console seriale EC2.

È possibile accedere alla console seriale utilizzando la console EC2 o la console AWS CLI.

La console seriale è disponibile senza costi aggiuntivi.

Argomenti

- Prerequisiti per la console seriale EC2
- Configurazione dell'accesso alla console seriale EC2
- Connessione alla console seriale EC2

- Disconnettiti dalla console seriale EC2
- Risoluzione dei problemi relativi all'istanza Amazon EC2 utilizzando la console seriale EC2

Prerequisiti per la console seriale EC2

Per connettersi alla console seriale EC2 e utilizzare lo strumento scelto per la risoluzione dei problemi, devono sussistere i prerequisiti seguenti:

- Regioni AWS
- Zone Wavelength
- AWS Outposts
- Local Zones
- Tipi di istanza
- Concessione dell'accesso
- Supporto per client basati su browser
- Stato istanza
- Amazon EC2 Systems Manager
- Configura lo strumento di risoluzione dei problemi scelto

Regioni AWS

Supportato in tutti Regioni AWS tranne AWS European Sovereign Cloud (Germany).

Zone Wavelength

Non supportato.

AWS Outposts

Supportato su tutti gli AWS avamposti.

Local Zones

Supportato nelle zone locali.

Tipi di istanza

Tipi di istanze supportati:

- Linux
  - Tutte le istanze virtualizzate basate sul sistema Nitro.
  - Tutte le istanze bare metal eccetto:
    - Scopo generale:`a1.metal`,`mac1.metal`,`mac2.metal`,`mac2-m1ultra.metal`,`mac2-m2.metal`,`mac2-m2pro.metal`,,`mac-m3ultra.metal`, `mac-m4.metalmac-m4max.metal`, e `mac-m4pro.metal`
    - Calcolo accelerato: `g5g.metal`
    - Memoria ottimizzata: `u-6tb1.metalu-9tb1.metal`,`u-12tb1.metal`,`u-18tb1.metal`, e `u-24tb1.metal`
- Windows
  - Tutte le istanze virtualizzate basate sul sistema Nitro.
  - Tutte le istanze bare metal eccetto:
    - Scopo generale: `a1.metalmac1.metal`,`mac2.metal`,,`mac2-m1ultra.metal`,`mac2-m2.metal`,`mac2-m2pro.metal`,`mac-m3ultra.metal`,`mac-m4.metal`,`mac-m4max.metal`, e `mac-m4pro.metal`
    - Calcolo accelerato: `g5g.metal`
    - Memoria ottimizzata: `u-6tb1.metalu-9tb1.metal`,`u-12tb1.metal`,`u-18tb1.metal`, e `u-24tb1.metal`

Concessione dell'accesso

Per concedere l'accesso alla Console seriale EC2 è necessario completare le seguenti attività di configurazione. Per ulteriori informazioni, consulta Configurazione dell'accesso alla console seriale EC2.

Supporto per client basati su browser

Per connettersi alla console seriale utilizzando il client basato su browser, il browser deve supportare. WebSocket Se il tuo browser non supporta WebSocket, connettiti alla console seriale utilizzando la tua chiave e un client SSH.

Il client basato su browser si connette sulla porta 443 all'endpoint proxy EC2 Instance Connect per la tua regione. Il formato dell'endpoint dipende dalla partizione: https://docs.aws.amazon.com/glossary/latest/reference/glos-chap.html#partition

- Le regioni AWS commerciali e le regioni AWS GovCloud (Stati Uniti) utilizzano il formato degli endpoint:. `prod.region.oneclickv2-proxy.ec2.aws.dev`
- Le regioni cinesi utilizzano il formato degli endpoint:. `prod.region.oneclickv2-proxy.ec2.a2z.org.cn`

Gli esempi seguenti mostrano l'endpoint per ogni partizione:

- Per la regione Stati Uniti orientali (Virginia settentrionale), l'endpoint è. `prod.us-east-1.oneclickv2-proxy.ec2.aws.dev`
- Per la regione Cina (Pechino), l'endpoint è. `prod.cn-north-1.oneclickv2-proxy.ec2.a2z.org.cn`

> **Note**
>
> Il browser deve essere in grado di raggiungere questo endpoint. Se un firewall o una VPN bloccano la connessione, la connessione fallisce.

Stato istanza

Deve essere `running`.

Non è possibile connettersi alla console seriale se l'istanza è nello stato `pending`, `stopping`, `stopped`, `shutting-down` o `terminated`.

Per ulteriori informazioni sugli stati delle istanze, consulta Cambio di stato di un'istanza Amazon EC2.

Amazon EC2 Systems Manager

Se l'istanza utilizza Amazon EC2 Systems Manager, nell'istanza deve essere installato SSM Agent versione 3.0.854.0 o successiva. Per ulteriori informazioni su SSM Agent, consulta Utilizzo di SSM Agent nella Guida per l'utente di AWS Systems Manager .

Configura lo strumento di risoluzione dei problemi scelto

Per risolvere i problemi della tua istanza usando la console seriale, puoi usare GRUB o SysRq sulle istanze Linux e la Special Admin Console (SAC) sulle istanze Windows. Prima di poter utilizzare questi strumenti, devi prima eseguire i passaggi di configurazione su ogni istanza in cui li utilizzerai.

Consulta le istruzioni relative al sistema operativo della tua istanza per configurare lo strumento di risoluzione dei problemi scelto.

(Istanze Linux) Configura GRUB

Per configurare GRUB, seleziona una delle procedure seguenti in base all'AMI utilizzata per avviare l'istanza.

Amazon Linux 2

Per configurare GRUB su un'istanza Amazon Linux 2

1. Connessione a un'istanza Linux tramite SSH
2. Aggiungi o modifica le seguenti opzioni in `/etc/default/grub`:
   - Imposta `GRUB_TIMEOUT=1`.
   - Add `GRUB_TERMINAL="console serial"`.
   - Add `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Di seguito è riportato un esempio di `/etc/default/grub`. Potrebbe essere necessario modificare la configurazione in base alle impostazioni del sistema.

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
    biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0"
   GRUB_TIMEOUT=1
   GRUB_DISABLE_RECOVERY="true"
   GRUB_TERMINAL="console serial"
   GRUB_SERIAL_COMMAND="serial --speed=115200"
   ```
3. Applica la configurazione aggiornata emettendo il comando seguente.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

Ubuntu

Per configurare GRUB su un'istanza Ubuntu

1. Connettiti alla tua istanza.

2. Aggiungi o modifica le seguenti opzioni in `/etc/default/grub.d/50-cloudimg-settings.cfg`:

   - Imposta `GRUB_TIMEOUT=1`.
   - Add `GRUB_TIMEOUT_STYLE=menu`.
   - Add `GRUB_TERMINAL="console serial"`.
   - Remove `GRUB_HIDDEN_TIMEOUT`.
   - Add `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Di seguito è riportato un esempio di `/etc/default/grub.d/50-cloudimg-settings.cfg`. Potrebbe essere necessario modificare la configurazione in base alle impostazioni del sistema.

```
# Cloud Image specific Grub settings for Generic Cloud Images
# CLOUD_IMG: This file was created/modified by the Cloud Image build process

# Set the recordfail timeout
GRUB_RECORDFAIL_TIMEOUT=0

# Do not wait on grub prompt
GRUB_TIMEOUT=1
GRUB_TIMEOUT_STYLE=menu

# Set the default commandline
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295"

# Set the grub console type
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed 115200"
```

3. Applica la configurazione aggiornata emettendo il comando seguente.

```
[ec2-user ~]$ sudo update-grub
```

RHEL

Per configurare GRUB su un'istanza RHEL

1. Connettiti alla tua istanza.
2. Aggiungi o modifica le seguenti opzioni in `/etc/default/grub`:
   - Remove `GRUB_TERMINAL_OUTPUT`.
   - Add `GRUB_TERMINAL="console serial"`.
   - Add `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

   Di seguito è riportato un esempio di `/etc/default/grub`. Potrebbe essere necessario modificare la configurazione in base alle impostazioni del sistema.

   ```
   GRUB_TIMEOUT=1
   GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
   GRUB_DEFAULT=saved
   GRUB_DISABLE_SUBMENU=true
   GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8 net.ifnames=0
    rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto"
   GRUB_DISABLE_RECOVERY="true"
   GRUB_ENABLE_BLSCFG=true
   GRUB_TERMINAL="console serial"
   GRUB_SERIAL_COMMAND="serial --speed=115200"
   ```
3. Applica la configurazione aggiornata emettendo il comando seguente.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg --update-bls-cmdline
   ```

   Per RHEL 9.2 e precedenti, utilizza il seguente comando.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

CentOS

Per le istanze avviate utilizzando un'AMI CentOS, GRUB per la console seriale è configurato per impostazione predefinita.

Di seguito è riportato un esempio di `/etc/default/grub`. La configurazione potrebbe essere diversa in base alle impostazioni del sistema.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto console=ttyS0,115200"
GRUB_DISABLE_RECOVERY="true"
```

(istanze Linux) Configura SysRq

Per configurare SysRq, si abilitano i SysRq comandi per il ciclo di avvio corrente. Per rendere la configurazione persistente, puoi anche abilitare i SysRq comandi per gli avvii successivi.

Per abilitare tutti SysRq i comandi per il ciclo di avvio corrente

1. Connettiti alla tua istanza.
2. Esegui il comando riportato qui di seguito.

   ```
   [ec2-user ~]$ sudo sysctl -w kernel.sysrq=1
   ```

   Questa impostazione sarà cancellata al riavvio successivo.

Per abilitare tutti i SysRq comandi per gli avvii successivi

1. Crea il file `/etc/sysctl.d/99-sysrq.conf` e aprilo nel tuo editor preferito.

   ```
   [ec2-user ~]$ sudo vi /etc/sysctl.d/99-sysrq.conf
   ```
2. Aggiungi la seguente riga.

   ```
   kernel.sysrq=1
   ```
3. Riavvia l'istanza per applicare le modifiche.

   ```
   [ec2-user ~]$ sudo reboot
   ```

4. Al prompt di `login`, specifica il nome utente dell'utente con password configurato in precedenza quindi premi Invio.
5. Al prompt di `Password`, specifica la password e premi Invio.

(Istanze Windows) Abilitare SAC e il menu di avvio

> **Note**
>
> Se si abilita SAC su un'istanza, i servizi EC2 che si basano sul recupero della password non funzioneranno dalla console Amazon EC2. Gli agenti di avvio di Windows su Amazon EC2 (EC2Config, EC2Launch v1 e EC2Launch v2) si affidano alla console seriale per eseguire varie attività. Queste attività non vengono eseguite correttamente quando si abilita SAC su un'istanza. Per ulteriori informazioni sugli agenti di avvio di Windows su Amazon EC2, consulta the section called "Configurazione di istanze Windows". Se abiliti SAC, puoi disabilitarlo in un secondo momento. Per ulteriori informazioni, consulta Disabilitazione di SAC e del menu di avvio.

Utilizzare uno dei seguenti metodi per abilitare SAC e il menu di avvio su un'istanza.

PowerShell

Per abilitare SAC e il menu di avvio in un'istanza di Windows

1. Connettiti alla tua istanza ed esegui i seguenti passaggi da una riga di PowerShell comando con privilegi elevati.
2. Abilita SAC.

```
bcdedit /ems '{current}' on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Abilita il menu di avvio.

```
bcdedit /set '{bootmgr}' displaybootmenu yes
bcdedit /set '{bootmgr}' timeout 15
bcdedit /set '{bootmgr}' bootems yes
```

4. Applica la configurazione aggiornata riavviando l'istanza.

```
shutdown -r -t 0
```

Command prompt

Per abilitare SAC e il menu di avvio in un'istanza di Windows

1. Connettiti all'istanza ed esegui la procedura dal prompt dei comandi.
2. Abilita SAC.

```
bcdedit /ems {current} on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Abilita il menu di avvio.

```
bcdedit /set {bootmgr} displaybootmenu yes
bcdedit /set {bootmgr} timeout 15
bcdedit /set {bootmgr} bootems yes
```

4. Applica la configurazione aggiornata riavviando l'istanza.

```
shutdown -r -t 0
```

Configurazione dell'accesso alla console seriale EC2

Per configurare l'accesso alla console seriale, è necessario concedere l'accesso alla console a livello di account e quindi configurare le policy IAM per concedere l'accesso agli utenti. Per le istanze Linux è inoltre necessario configurare un utente con password su ogni istanza in modo che gli utenti possano utilizzare la console seriale per la risoluzione dei problemi.

La console seriale EC2 utilizza una connessione a porta seriale virtuale per interagire con un'istanza. Questa connessione è indipendente dal VPC dell'istanza, quindi puoi lavorare con il sistema operativo dell'istanza e avviare gli strumenti di risoluzione dei problemi anche in caso di errori di avvio o problemi di configurazione della rete. Poiché questa connessione è esterna alla rete VPC, la console seriale EC2 non utilizza il gruppo di sicurezza dell'istanza o l'ACL della rete di sottorete per autorizzare il traffico verso l'istanza.

Prima di iniziare

Verifica che i prerequisiti siano soddisfatti.

Indice

- Livelli di accesso alla console seriale EC2
- Gestione dell'accesso con account alla console seriale EC2
- Configurazione di policy IAM per l'accesso alla console seriale EC2
- Imposta una password utente del sistema operativo su un'istanza Linux

Livelli di accesso alla console seriale EC2

Per impostazione predefinita, non è possibile accedere alla console seriale a livello di account. L'accesso alla console seriale a livello di account va concesso esplicitamente. Per ulteriori informazioni, consulta Gestione dell'accesso con account alla console seriale EC2.

È possibile utilizzare una policy di controllo dei servizi (SCP) per consentire l'accesso alla console seriale all'interno dell'organizzazione. È quindi possibile avere un controllo di accesso granulare a livello utente utilizzando una policy IAM per il controllo dell'accesso. Utilizzando una combinazione di policy SCP e IAM, si avranno diversi livelli di controllo dell'accesso alla console seriale.

Livello di organizzazione

È possibile utilizzare una policy di controllo dei servizi (SCP) per consentire l'accesso alla console seriale per gli account membri all'interno dell'organizzazione. Per ulteriori informazioni sulle SCP, consulta Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

Livello di istanza

È possibile configurare le politiche di accesso alla console seriale utilizzando IAM PrincipalTag e le ResourceTag costruzioni e specificando le istanze in base al loro ID. Per ulteriori informazioni, consulta Configurazione di policy IAM per l'accesso alla console seriale EC2.

Livello utente

È possibile configurare l'accesso a livello di utente configurando una policy IAM per consentire o negare a un utente specificato l'autorizzazione per eseguire il push della chiave pubblica SSH al servizio della console seriale di una determinata istanza. Per ulteriori informazioni, consulta Configurazione di policy IAM per l'accesso alla console seriale EC2.

Livello di sistema operativo (solo istanze Linux)

È possibile impostare una password utente a livello del sistema operativo guest. In questo modo è possibile accedere alla console seriale per alcuni casi d'uso. Tuttavia, per monitorare i log, non è necessario un utente con password. Per ulteriori informazioni, consulta Imposta una password utente del sistema operativo su un'istanza Linux.

Gestione dell'accesso con account alla console seriale EC2

Per impostazione predefinita, non è possibile accedere alla console seriale a livello di account. L'accesso alla console seriale a livello di account va concesso esplicitamente.

Questa impostazione è configurata a livello di account, direttamente nell'account o utilizzando una policy dichiarativa. Deve essere configurato in tutti i punti in Regione AWS cui si desidera concedere l'accesso alla console seriale. L'utilizzo di una policy dichiarativa consente di applicare l'impostazione contemporaneamente su più regioni, nonché su più account. Quando viene utilizzata una policy dichiarativa, non è possibile modificare l'impostazione direttamente all'interno di un account. Questo argomento illustra la modalità di configurazione dell'impostazione direttamente all'interno di un account. Per informazioni sull'utilizzo delle policy dichiarative, consulta Policy dichiarative nella Guida per l'utente di AWS Organizations .

Indice

- Concessione dell'autorizzazione agli utenti per gestire l'accesso con account
- Visualizzazione dello stato di accesso account alla console seriale
- Concessione dell'accesso con account alla console seriale
- Negare l'accesso con account alla console seriale

Concessione dell'autorizzazione agli utenti per gestire l'accesso con account

Per consentire agli utenti di gestire l'accesso con account alla console seriale EC2, è necessario concedere loro le autorizzazioni IAM necessarie.

La policy seguente concede le autorizzazioni per visualizzare lo stato dell'account e per consentire e impedire l'accesso con account alla console seriale EC2.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:EnableSerialConsoleAccess",
                "ec2:DisableSerialConsoleAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

Per ulteriori informazioni, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Visualizzazione dello stato di accesso account alla console seriale

Console

Per visualizzare lo stato di accesso con account alla console seriale

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione seleziona Pannello di controllo.
3. Nella scheda Attributi dell'account, in Impostazioni, scegli Console seriale EC2.
4. Nella scheda Console seriale EC2, il valore dell'accesso alla console seriale EC2 è Consentito o Impedito.

AWS CLI

Per visualizzare lo stato di accesso con account alla console seriale

Utilizza il comando get-serial-console-access-status.

```
aws ec2 get-serial-console-access-status
```

Di seguito è riportato un output di esempio. Un valore di `true` indica che all'account è consentito accedere alla console seriale.

```
{
    "SerialConsoleAccessEnabled": true,
    "ManagedBy": "account"
}
```

Il campo `ManagedBy` indica l'entità che ha configurato l'impostazione. I valori possibili sono `account` (configurati direttamente) o `declarative-policy`. Per ulteriori informazioni, consulta Policy dichiarative nella Guida per l'utente di AWS Organizations .

PowerShell

Per visualizzare lo stato di accesso con account alla console seriale

Utilizza il cmdlet Get-EC2SerialConsoleAccessStatus.

```
Get-EC2SerialConsoleAccessStatus -Select *
```

Di seguito è riportato un output di esempio. Un valore di `True` indica che all'account è consentito accedere alla console seriale.

```
ManagedBy SerialConsoleAccessEnabled
--------- --------------------------
account   True
```

Il campo `ManagedBy` indica l'entità che ha configurato l'impostazione. I valori possibili sono `account` (configurati direttamente) o `declarative-policy`. Per ulteriori informazioni, consulta Policy dichiarative nella Guida per l'utente di AWS Organizations .

Concessione dell'accesso con account alla console seriale

Console

Per concedere l'accesso con account alla console seriale

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione seleziona Pannello di controllo.
3. Nella scheda Attributi dell'account, in Impostazioni, scegli Console seriale EC2.

4. Scegli Gestisci.
5. Per consentire l'accesso alla console seriale EC2 di tutte le istanze dell'account, seleziona la casella di controllo Consenti.
6. Scegliere Aggiorna.

AWS CLI

Per concedere l'accesso con account alla console seriale

Utilizza il comando enable-serial-console-access.

```
aws ec2 enable-serial-console-access
```

Di seguito è riportato un output di esempio.

```
{
    "SerialConsoleAccessEnabled": true
}
```

PowerShell

Per concedere l'accesso con account alla console seriale

Utilizza il cmdlet Enable-EC2SerialConsoleAccess.

```
Enable-EC2SerialConsoleAccess
```

Di seguito è riportato un output di esempio.

```
True
```

Negare l'accesso con account alla console seriale

Console

Per negare l'accesso con account alla console seriale

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nel pannello di navigazione seleziona Pannello di controllo.
3. Nella scheda Attributi dell'account, in Impostazioni, scegli Console seriale EC2.
4. Scegli Gestisci.
5. Per impedire l'accesso alla console seriale EC2 di tutte le istanze dell'account, deseleziona la casella di controllo Consenti.
6. Scegliere Aggiorna.

AWS CLI

Per negare l'accesso con account alla console seriale

Utilizza il comando disable-serial-console-access.

```
aws ec2 disable-serial-console-access
```

Di seguito è riportato un output di esempio.

```
{
    "SerialConsoleAccessEnabled": false
}
```

PowerShell

Per negare l'accesso con account alla console seriale

Utilizza il cmdlet Disable-EC2SerialConsoleAccess.

```
Disable-EC2SerialConsoleAccess
```

Di seguito è riportato un output di esempio.

```
False
```

Configurazione di policy IAM per l'accesso alla console seriale EC2

Per impostazione predefinita, gli utenti non hanno accesso alla console seriale. L'organizzazione deve configurare le policy IAM per concedere agli utenti di accedere. Per ulteriori informazioni, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per l'accesso alla console seriale, crea un documento di policy JSON che includa l'operazione `ec2-instance-connect:SendSerialConsoleSSHPublicKey`. Questa operazione concede a un utente l'autorizzazione per eseguire il push della chiave pubblica al servizio della console seriale, che avvia una sessione della console. Consigliamo di limitare l'accesso a specifiche istanze EC2. In caso contrario, tutti gli utenti con questa autorizzazione potranno connettersi alla console seriale di tutte le istanze EC2.

Policy IAM di esempio

- Consenti esplicitamente l'accesso alla console seriale
- Negare esplicitamente l'accesso alla console seriale
- Utilizzo di tag di risorse per controllare l'accesso alla console seriale

Consenti esplicitamente l'accesso alla console seriale

Per impostazione predefinita, nessuno ha accesso alla console seriale. Per concedere l'accesso alla console seriale, è necessario configurare una policy in modo da consentirlo esplicitamente. Si consiglia di configurare una policy che limiti l'accesso a istanze specifiche.

La seguente policy consente di accedere alla console seriale di un'istanza specifica, identificata dal relativo ID istanza.

Tieni presente che le operazioni `DescribeInstances`, `DescribeInstanceTypes` e `GetSerialConsoleAccessStatus` non supportano le autorizzazioni a livello di risorsa e pertanto tutte le risorse contrassegnate da `*` (asterisco) devono essere specificate per queste operazioni.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
             "Resource": "*"
```

```
        },
        {
            "Sid": "AllowinstanceBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:us-
east-1:111122223333:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Negare esplicitamente l'accesso alla console seriale

La seguente policy IAM consente l'accesso alla console seriale di tutte le istanze, indicata con * (asterisco), e nega esplicitamente l'accesso alla console seriale di un'istanza specifica, identificata dal relativo ID.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DenySerialConsoleAccess",
            "Effect": "Deny",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
```

```
            "Resource": "arn:aws:ec2:us-
east-1:111122223333:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Utilizzo di tag di risorse per controllare l'accesso alla console seriale

È possibile utilizzare i tag delle risorse per controllare l'accesso alla console seriale di un'istanza.

Attribute-based il controllo degli accessi è una strategia di autorizzazione che definisce le autorizzazioni in base a tag che possono essere allegati a utenti e AWS risorse. Ad esempio, la policy seguente consente a un utente di avviare una connessione alla console seriale per un'istanza solo se il tag risorsa dell'istanza e il tag dell'entità hanno lo stesso valore `SerialConsole` per la chiave di tag.

Per ulteriori informazioni sull'uso dei tag per controllare l'accesso alle AWS risorse, consulta Controlling access to AWS resources nella IAM User Guide.

Tieni presente che le operazioni `DescribeInstances`, `DescribeInstanceTypes` e `GetSerialConsoleAccessStatus` non supportano le autorizzazioni a livello di risorsa e pertanto tutte le risorse contrassegnate da `*` (asterisco) devono essere specificate per queste operazioni.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTagBasedSerialConsoleAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SerialConsole":
 "${aws:PrincipalTag/SerialConsole}"
                }
            }
        }
    ]
}
```

Imposta una password utente del sistema operativo su un'istanza Linux

È possibile connettersi alla console seriale senza utilizzare una password. Tuttavia, per utilizzare la console seriale per la risoluzione dei problemi di un'istanza Linux, è necessario che l'istanza disponga di un utente del sistema operativo basato su password.

È possibile impostare la password per qualsiasi utente del sistema operativo, incluso l'utente root. Tieni presente che l'utente root può modificare tutti i file, mentre ogni utente del sistema operativo potrebbe avere autorizzazioni limitate.

È necessario impostare una password utente per ogni istanza per la quale si utilizzerà la console seriale. Si tratta di una procedura da eseguire una volta sola per ciascuna istanza.

> **Note**
>
> Per impostazione predefinita, le AMI fornite da non AWS sono configurate con un utente basato su password. Se l'istanza è stata avviata utilizzando un'AMI che dispone già della password utente root configurata, è possibile ignorare queste istruzioni.

Per impostare una password utente del sistema operativo su un'istanza Linux

1. Connettiti alla tua istanza. È possibile utilizzare qualsiasi metodo per il collegamento all'istanza ad eccezione del metodo di connessione della console seriale EC2.
2. Per impostare la password per un utente, utilizza il comando passwd. Nell'esempio seguente, l'utente è `root`.

```
[ec2-user ~]$ sudo passwd root
```

Di seguito è riportato un output di esempio.

```
Changing password for user root.
New password:
```

3. Al prompt di `New password`, specifica la nuova password.
4. Al prompt, immetti di nuovo la password.

Connessione alla console seriale EC2

Puoi connetterti alla console seriale dell'istanza EC2 utilizzando la console Amazon EC2 o tramite SSH. Dopo la connessione alla console seriale, sarà possibile utilizzarla per la risoluzione dei problemi di avvio, di configurazione di rete e di altro tipo. Per ulteriori informazioni sulla risoluzione dei problemi, consulta Risoluzione dei problemi relativi all'istanza Amazon EC2 utilizzando la console seriale EC2.

Considerazioni

- È supportata 1 sola connessione alla console seriale attiva per istanza.
- La connessione alla console seriale dura in genere 1 ora, a meno che non sia disconnessa. Tuttavia, durante la manutenzione del sistema, Amazon EC2 interromperà la sessione della console.

  La durata di una connessione RDP non è determinata dalla durata delle credenziali IAM. Se le credenziali IAM scadono, la connessione continua a persistere fino al raggiungimento della durata massima della connessione alla console seriale. Quando utilizzi l'esperienza della console seriale EC2, se le credenziali IAM scadono, termina la connessione chiudendo la pagina del browser.
- Sono necessari 30 secondi per interrompere una sessione dopo la disconnessione dalla console seriale per consentirne una nuova.
- Porte console seriali supportate: `ttyS0` (istanze Linux) e `COM1` (istanze Windows)
- Quando ti connetti alla console seriale, è possibile che vi sia un leggero calo del throughput dell'istanza.

Argomenti

- Connessione tramite client basato su browser
- Connessione tramite la propria chiave e un client SSH
- Endpoint e impronte digitali della console seriale EC2

Connessione tramite client basato su browser

Puoi connetterti alla console seriale dell'istanza EC2 utilizzando il client basato su browser. A tale scopo, seleziona l'istanza nella console Amazon EC2 e sceglie di connetterti alla console seriale. Il client basato su browser gestisce le autorizzazioni e garantisce una corretta connessione.

La console seriale EC2 funziona dalla maggior parte dei browser e supporta l'input di tastiera e mouse.

Prima di effettuare la connessione, assicurati di avere soddisfatto tutti i prerequisiti.

Per connettersi alla porta seriale dell'istanza utilizzando il client basato su browser (console Amazon EC2)

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Puoi selezionare l'istanza e scegliere Actions (Operazioni), Monitor and troubleshoot (Monitoraggio e risoluzione dei problemi), EC2 Serial Console (Console seriale EC2), Connect (Connetti).

   In alternativa, puoi selezionare l'istanza e scegliere Connect (Connetti), EC2 Serial Console (Console seriale EC2), Connect (Connetti).

   Verrà aperta una finestra del terminale nel browser.
4. Premi Invio. Se viene restituito un prompt di accesso, allora significa che sei connesso alla console seriale.

   Se lo schermo rimane nero, potrai utilizzare le seguenti informazioni per risolvere i problemi relativi alla connessione alla console seriale:

   - Verifica di aver configurato l'accesso alla console seriale. Per ulteriori informazioni, consulta Configurazione dell'accesso alla console seriale EC2.

- (Solo istanze Linux) Usalo SysRq per connetterti alla console seriale. SysRq non richiede la connessione tramite il client basato su browser. Per ulteriori informazioni, consulta (istanze Linux) Usalo SysRq per risolvere i problemi della tua istanza.
- (Solo istanze Linux) Riavvia getty. Se hai accesso SSH alla tua istanza, connettiti alla tua istanza usando SSH e riavvia getty usando il seguente comando.

```
[ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
```

- Riavviare l'istanza. È possibile riavviare l'istanza utilizzando SysRq (istanze Linux), la console EC2 o il. AWS CLI Per ulteriori informazioni, consulta (istanze Linux) Usalo SysRq per risolvere i problemi della tua istanza (istanze Linux) o Riavvio di un'istanza Amazon EC2.

5. (Solo istante Linux) Al prompt di `login`, specifica il nome utente dell'utente con password configurato in precedenza quindi premi Invio.
6. (Solo istanze Linux) Al prompt di `Password`, specifica la password e premi Invio.

Connessione tramite la propria chiave e un client SSH

Puoi utilizzare la tua chiave SSH e connetterti all'istanza dal client SSH preferito durante l'utilizzo dell'API della console seriale. In questo modo, potrai sfruttare la capacità della console seriale di inviare una chiave pubblica all'istanza.

Dopo aver inviato la chiave SSH all'istanza, la connessione SSH non è soggetta alle politiche IAM configurate per concedere agli utenti l'accesso alla console seriale EC2.

Prima di iniziare

Verifica che i prerequisiti siano soddisfatti.

Per connettersi alla console seriale di un'istanza utilizzando SSH

1. Invia la tua chiave pubblica SSH nell'istanza per avviare una sessione di console seriale

   Utilizza il comando send-serial-console-ssh-public-key per inviare la chiave pubblica SSH all'istanza. Verrà avviata una sessione di console seriale.

   Se per questa istanza è già stata avviata una sessione della console seriale, il comando avrà esito negativo perché è possibile aprire una sola sessione alla volta. Sono necessari 30 secondi per interrompere una sessione dopo la disconnessione dalla console seriale per consentire una nuova sessione.

```
aws ec2-instance-connect send-serial-console-ssh-public-key \
    --instance-id i-001234a4bf70dec41EXAMPLE \
    --serial-port 0 \
    --ssh-public-key file://my_key.pub \
    --region us-east-1
```

2. Connessione alla console seriale utilizzando la chiave privata

   Utilizza il comando ssh per connetterti alla console seriale prima che la chiave pubblica venga rimossa dal servizio della console seriale. Hai 60 secondi prima che la chiave venga rimossa.

   Utilizza la chiave privata corrispondente alla chiave pubblica.

   Il formato del nome utente è `instance-id.port0`, che comprende l'ID istanza e la porta 0. Nell'esempio seguente, il nome utente è `i-001234a4bf70dec41EXAMPLE.port0`.

   L'endpoint del servizio della console seriale è diverso per ogni Regione. Consulta la tabella Endpoint e impronte digitali della console seriale EC2 per l'endpoint di ogni regione. Nell'esempio seguente, il servizio della console seriale si trova nella regione *us-est-1*.

   ```
   ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-connect.us-east-1.aws
   ```

   L'esempio seguente utilizza `timeout 3600` per impostare la sessione SSH in modo che termini dopo 1 ora. I processi avviati durante la sessione possono continuare a essere eseguiti sull'istanza dopo la terminazione della sessione.

   ```
   timeout 3600 ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-connect.us-east-1.aws
   ```

3. (Facoltativo) Verifica dell'impronta digitale

   Quando ti connetti per la prima volta alla console seriale, ti sarà richiesto di confermare l'impronta digitale. Puoi confrontare l'impronta digitale della console seriale con l'impronta digitale visualizzata per la verifica. Se le impronte non corrispondono, è possibile che un utente non autorizzato stia cercando di eseguire un attacco di tipo "man-in-the-middle". Se corrispondono, potrai tranquillamente connetterti alla console seriale.

La seguente impronta digitale è per il servizio della console seriale nella regione us-est-1. Per le impronte digitali di ciascuna regione, consulta Endpoint e impronte digitali della console seriale EC2.

```
SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
```

L'impronta digitale viene visualizzata solo la prima volta che ci si connette alla console seriale.

4. Premi Invio. Se viene restituito un prompt, allora significa che sei connesso alla console seriale.

   Se lo schermo rimane nero, potrai utilizzare le seguenti informazioni per risolvere i problemi relativi alla connessione alla console seriale:

   - Verifica di aver configurato l'accesso alla console seriale. Per ulteriori informazioni, consulta Configurazione dell'accesso alla console seriale EC2.
   - (Solo istanze Linux) Usalo SysRq per connetterti alla console seriale. SysRq non richiede la connessione tramite SSH. Per ulteriori informazioni, consulta (istanze Linux) Usalo SysRq per risolvere i problemi della tua istanza.
   - (Solo istanze Linux) Riavvia getty. Se hai accesso SSH alla tua istanza, connettiti alla tua istanza usando SSH e riavvia getty usando il seguente comando.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```

   - Riavviare l'istanza. È possibile riavviare l'istanza utilizzando SysRq (solo istanze Linux), la console EC2 o il. AWS CLI Per ulteriori informazioni, consulta (istanze Linux) Usalo SysRq per risolvere i problemi della tua istanza (solo istanze Linux) o Riavvio di un'istanza Amazon EC2.

5. (Solo istante Linux) Al prompt di `login`, specifica il nome utente dell'utente con password configurato in precedenza quindi premi Invio.
6. (Solo istanze Linux) Al prompt di `Password`, specifica la password e premi Invio.

Endpoint e impronte digitali della console seriale EC2

Di seguito sono riportati gli endpoint e le impronte digitali del servizio per la console seriale EC2. Per connettersi a livello di codice alla console seriale di un'istanza, viene utilizzato un endpoint della console seriale EC2. Gli endpoint e le impronte digitali della console seriale EC2 sono unici per ogni Regione AWS .

Nome della regione	Regione	Endpoint	Impronta digitale
Stati Uniti orientali (Ohio)	us-east-2	serial-console.ec2-instance-connect.us-east-2.aws	SHA256:EhwPkTzRtTY7TRSzz26XbB0/HvV9jRM7mCZN0xw/d/0
Stati Uniti orientali (Virginia settentrionale)	us-east-1	serial-console.ec2-instance-connect.us-east-1.aws	SHA256:dXwn5ma/xadVMeBZGEru5l2gx+y l5LDiJaLUcz0FMmw
Stati Uniti occidentali (California settentrionale)	us-west-1	serial-console.ec2-instance-connect.us-west-1.aws	SHA256:OHldlcMET8u7QLSX3jmRTRAPFHVtqbyoLZBMUCqiH3Y
Stati Uniti occidentali (Oregon)	us-west-2	serial-console.ec2-instance-connect.us-west-2.aws	SHA256:EMCIe23TqKaBI6yGHainqZcMwqNkDhhAVHa1O2JxVUc
Africa (Città del Capo)	af-south-1	ec2-serial-console.af-south-1.api.aws	SHA256:RMWWZ2fVePeJUqzjO5jL2KIgXsczoHlz21Ed00biiWI
Asia Pacific (Hong Kong)	ap-east-1	ec2-serial-console.ap-east-1.api.aws	SHA256:T0Q1lpiXxChoZHplnAkjbP7tkm2xXViC9bJFsjYnifk
Asia Pacifico (Taipei)	ap-east-2	ec2-serial-console.ap-east-2.api.aws	SHA256:z1rsF5DE8aQqsHwBr/D40tR2GnyMqnScCUa1z1eFwDQ

Nome della regione	Regione	Endpoint	Impronta digitale
Asia Pacifico (Hyderabad)	ap-south-2	ec2-serial-console.ap-south-2.api.aws	SHA256:WJgPBSwV4/shN+OPITValoewAuYj15DVW845JEhDKRs
Asia Pacifico (Giacarta)	ap-southeast-3	ec2-serial-console.ap-southeast-3.api.aws	SHA256:5ZwgrCh+lfns32XITqL/4O0zIfbx4bZgsYFqy3o8mIk
Asia Pacifico (Malesia)	ap-southeast-5	ec2-serial-console.ap-southeast-5.api.aws	SHA256:cQXTHQMRcqRdIjmAGoAMBSExeoRobYyRwT67yTjnEiA
Asia Pacifico (Nuova Zelanda)	ap-southeast-6	ec2-serial-console.ap-southeast-6.api.aws	SHA256:wNltdH0gVfM5uHJKjrw+ LLKv4 ElFuKoJgalcSKqjCS
Asia Pacifico (Melbourne)	ap-southeast-4	ec2-serial-console.ap-southeast-4.api.aws	SHA256:Avaq27hFgLvjn5gTSShZ0oV7h90p0GG46wfOeT6ZJvM
Asia Pacifico (Mumbai)	ap-south-1	serial-console.ec2-instance-connect.ap-south-1.aws	SHA256:oBLXcYmklqHHEbliARxEgH8IsO51rezTPiSM35BsU40
Asia Pacifico (Osaka-Locale)	ap-northeast-3	ec2-serial-console.ap-northeast-3.api.aws	SHA256:Am0/jiBKBnBuFnHr9aXsgEV3G8Tu/vVHFXE/3UcyjsQ

Nome della regione	Regione	Endpoint	Impronta digitale
Asia Pacific (Seoul)	ap-northeast-2	serial-console.ec2-instance-connect.ap-northeast-2.aws	SHA256:FoqWXNX +DZ++ GuNTztg9P K49WYMqBX +FRCZM2DSRqri
Asia Pacifico (Singapore)	ap-southeast-1	serial-console.ec2-instance-connect.ap-southeast-1.aws	SHA256:PL FNn7WnCQD Hx3qmwLu1Gy/ O8TUX7LQgZuaC6L 45CoY
Asia Pacifico (Sydney)	ap-southeast-2	serial-console.ec2-instance-connect.ap-southeast-2.aws	SHA256:yF vMwUK9lEU QjQTRoXXzuN+cW9/ VSe9W984Cf5Tgzo4
Asia Pacifico (Thailandia)	ap-southeast-7	ec2-serial-console.ap-southeast-7.api.aws	SHA256:KC AZiRYrR1Q 2lqsg7vTw ixWmvc2wm jVT31XRgSdEfDY
Asia Pacifico (Tokyo)	ap-northeast-1	serial-console.ec2-instance-connect.ap-northeast-1.aws	SHA256:RQ fsDCZTOfQ awewTRDV1 t9Em/HMrFQe+ crl IoT5um4K
Canada (Centrale)	ca-central-1	serial-console.ec2-instance-connect.ca-central-1.aws	SHA256:P2 O2jOZwmpM wkpO6YW73 8FIOTHdUT yEv2gczYMMO7s4

Nome della regione	Regione	Endpoint	Impronta digitale
Canada occidentale (Calgary)	ca-west-1	ec2-serial-console.ca-west-1.api.aws	SHA256:s3 rc8Il2xhbhr3iedjJN xGAFLPGOL jx7IxxXrGckk6Q
Cina (Pechino)	cn-north-1	ec2-serial-console .cn-north-1.api.am azonwebservices.co m.cn	SHA256:2g HVFy4H7uU3+Y WaFUxD28v/ ggMeqjvSlgngpgLgGT
China (Ningxia)	cn-northwest-1	ec2-serial-console .cn-northwest-1.ap i.amazonwebservice s.com.cn	SHA256:Td grNZkiQOd VfYEBUhO4 SzUA09VWI 5rYOZGTogpwmiM
Europa (Francoforte)	eu-central-1	serial-console.ec2-instance-connect.eu-central-1.aws	SHA256:aCMFS/ yIcOdOlkXvOl8A mZ1Toe+b BnrJJ3Fy0 k0De2c
Europa (Irlanda)	eu-west-1	serial-console.ec2-instance-connect.eu-west-1.aws	SHA256:h2 AaGAWO4Ha thhtm6ezs3Bj7udgUx i2qTrHjZAwCW6E
Europe (London)	eu-west-2	serial-console.ec2-instance-connect.eu-west-2.aws	SHA256:a69rd5CE/ AEG4Amm53I6 lkD1ZPvS/ BCV3tTPW2RnJg8
Europe (Milan)	eu-south-1	ec2-serial-console.eu-south-1.api.aws	SHA256:IC 0kOVJnpgF yBVrxn0A7 n99ecLbXS X95cuuS7X7QK30

Nome della regione	Regione	Endpoint	Impronta digitale
Europa (Parigi)	eu-west-3	serial-console.ec2-instance-connect.eu-west-3.aws	SHA256:q8ldnAf9pymeNe8BnFVngY3RPAr/kxswJUzfrlxeEWs
Europa (Spagna)	eu-south-2	ec2-serial-console.eu-south-2.api.aws	SHA256:GoCW2DFRlu669QNxqFxEcsR6fZUz/4F4n7T45ZcwoEc
Europa (Stoccolma)	eu-north-1	serial-console.ec2-instance-connect.eu-north-1.aws	SHA256:tkGFFUVUDvocDiGSS3Cu8Gdl6w2uI32EPNpKFKLwX84
Europa (Zurigo)	eu-central-2	ec2-serial-console.eu-central-2.api.aws	SHA256:8Ppx2mBMf6WdCw0NUlzKfwM4/IfRz4OaXFutQXWp6mk
Israele (Tel Aviv)	il-central-1	ec2-serial-console.il-central-1.api.aws	SHA256:JR6q8v6kNNPi8+QSFQ4dj5dimNmZPTgwgsM1SNvtYyU
Messico (Centrale)	mx-central-1	ec2-serial-console.mx-central-1.api.aws	SHA256:BCuVl13iQNk+CcVnt18Ef4p2ZHUrBBAOxlFetB32GS0

Nome della regione	Regione	Endpoint	Impronta digitale
Medio Oriente (Bahrein)	me-south-1	ec2-serial-console .me-south-1.api.aws	SHA256:nP jLLKHu2Qn LdUq2kVAr soK5xvPJO MRJKCBzCDqC3k8
Medio Oriente (Emirati Arabi Uniti)	me-central-1	ec2-serial-console .me-central-1.api.aws	SHA256:zpb5duKiBZ +l0dFwPeyy kB4MPBYhI/ XzXNeFSDKBvLE
Sud America (San Paolo)	sa-east-1	serial-console.ec2-instance-connect.sa-east-1.aws	SHA256:rd2+/32 + Ognjew1yV IemENaQzC Botbih62OqAPDq1dI
AWS GovCloud (US-East)	us-gov-east-1	serial-console.ec2 -instance-connect. us-gov-east-1.amaz onaws.com	SHA256:tI we19GWsoy LClrtvu38YEEh+DHIk qnDcZnmtebvF28
AWS GovCloud (US-West)	us-gov-west-1	serial-console.ec2 -instance-connect. us-gov-west-1.amaz onaws.com	SHA256:kf OFRWLaOZfB +utbd3b Rf8OlPf8n GO2YZLqXZiIw5DQ

Disconnettiti dalla console seriale EC2

Se non è più necessario essere connessi alla console seriale EC2 dell'istanza, è possibile disconnettersi da essa. Quando ci si disconnette dalla console seriale, qualsiasi sessione di shell in esecuzione sull'istanza continuerà a essere eseguita. Se vuoi terminare la sessione shell, dovrai terminarla prima di disconnetterti dalla console seriale.

Considerazioni

- La connessione alla console seriale dura in genere 1 ora, a meno che non venga interrotta. Tuttavia, durante la manutenzione del sistema, Amazon EC2 interromperà la sessione della console.
- Sono necessari 30 secondi per interrompere una sessione dopo la disconnessione dalla console seriale per consentirne una nuova.

Il modo per disconnettersi dalla console seriale dipende dal client.

Browser-based cliente

Per terminare la sessione della console seriale, è sufficiente chiudere la finestra del terminale della console seriale nel browser.

Client OpenSSH standard

Per terminare la sessione della console seriale, utilizza il comando riportato di seguito per chiudere la connessione SSH. Questo comando deve essere eseguito immediatamente dopo una nuova riga.

```
~.
```

Il comando utilizzato per chiudere una connessione SSH potrebbe essere diverso a seconda del client SSH utilizzato.

Risoluzione dei problemi relativi all'istanza Amazon EC2 utilizzando la console seriale EC2

Grazie alla console seriale EC2, puoi risolvere i problemi di avvio, configurazione di rete e di altro tipo semplicemente collegandoti alla porta seriale dell'istanza.

Consulta le istruzioni relative al sistema operativo della tua istanza e allo strumento che hai configurato su di essa.

Tools (Strumenti)

- (Istanze Linux) Usa GRUB per risolvere i problemi della tua istanza
- (istanze Linux) Usalo SysRq per risolvere i problemi della tua istanza
- (Istanze Windows) Utilizza SAC per risolvere i problemi relativi all'istanza

Prerequisiti

Prima di iniziare, assicurati di avere soddisfatto tutti i prerequisiti, inclusa la configurazione dello strumento di risoluzione dei problemi che hai scelto.

(Istanze Linux) Usa GRUB per risolvere i problemi della tua istanza

GNU GRUB (abbreviazione di GNU Grand Unified Bootloader, comunemente chiamato GRUB) è il boot loader predefinito per la maggior parte dei sistemi operativi Linux. Dal menu di GRUB, è possibile selezionare il kernel in cui avviare o modificare le voci del menu per cambiare il modo in cui il kernel verrà avviato. Ciò può essere utile durante la risoluzione dei problemi di un'istanza con esito negativo.

Il menu di GRUB viene visualizzato durante il processo di avvio. Il menu non è accessibile tramite il normale SSH, ma è possibile accedervi utilizzando la console seriale EC2.

Puoi eseguire l'avvio in modalità utente singolo o in modalità emergenza. La modalità utente singolo avvierà il kernel con un runlevel inferiore. Ad esempio, potrebbe montare il filesystem ma non attivare la rete, dandoti la possibilità di eseguire la manutenzione necessaria per correggere l'istanza. La modalità di emergenza è simile alla modalità utente singolo tranne per il fatto che il kernel viene eseguito al runlevel più basso possibile.

Per eseguire l'avvio in modalità utente singolo

1. Connettiti alla console seriale dell'istanza.
2. Riavviare l'istanza utilizzando il comando seguente.

   ```
   [ec2-user ~]$ sudo reboot
   ```

3. Durante il riavvio, quando appare il menu di GRUB, premi un tasto qualsiasi per interrompere il processo di avvio.
4. Nel menu di GRUB, utilizzare i tasti freccia per selezionare il kernel in cui eseguire l'avvio, quindi premi e sulla tastiera.
5. Utilizza i tasti freccia per posizionare il cursore sulla riga contenente il kernel. La riga inizia con `linux` o `linux16` a seconda dell'AMI utilizzata per avviare l'istanza. Per Ubuntu, due righe iniziano con `linux` ed entrambe devono essere modificate nel passaggio successivo.
6. Alla fine della riga, aggiungi la parola `single`.

   Di seguito è riportato un esempio per Amazon Linux 2.

```
linux /boot/vmlinuz-4.14.193-149.317.amzn2.aarch64 root=UUID=d33f9c9a-\
dadd-4499-938d-ebbf42c3e499 ro  console=tty0 console=ttyS0,115200n8 net.ifname\
s=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.she\
ll=0 single
```

7. Premi Ctrl+X per eseguire l'avvio in modalità utente singolo.
8. Al prompt di `login`, specifica il nome utente dell'utente con password configurato in precedenza quindi premi Invio.
9. Al prompt di `Password`, specifica la password e premi Invio.

Per eseguire l'avvio in modalità di emergenza

Segui gli stessi passaggi della modalità utente singolo, ma al passaggio 6 aggiungi la parola `emergency` anziché `single`.

(istanze Linux) Usalo SysRq per risolvere i problemi della tua istanza

La chiave System Request (SysRq), a volte chiamata «magia SysRq «, può essere usata per inviare direttamente un comando al kernel, all'esterno di una shell, e il kernel risponderà, indipendentemente da ciò che sta facendo il kernel. Ad esempio, se l'istanza ha smesso di rispondere, puoi usare la SysRq chiave per dire al kernel di bloccarsi o riavviarsi. Per maggiori informazioni, consulta Magic SysRq key su Wikipedia.

È possibile utilizzare SysRq i comandi nel client basato su browser della console seriale EC2 o in un client SSH. Il comando per inviare una richiesta di interruzione è diverso per ogni client.

Per utilizzarlo SysRq, scegli una delle seguenti procedure in base al client che stai utilizzando.

Browser-based client

Da utilizzare SysRq nella console seriale (client basato su browser)

1. Connettiti alla console seriale dell'istanza.
2. Per inviare una richiesta di interruzione, premi il tasto `CTRL+0` (zero). Se la tastiera lo supporta, puoi inviare una richiesta di interruzione anche utilizzando il tasto Pausa o Interrompi.

```
[ec2-user ~]$ CTRL+0
```

3. Per emettere un SysRq comando, premi il tasto sulla tastiera che corrisponde al comando richiesto. Ad esempio, per visualizzare un elenco di SysRq comandi, premeteh.

```
[ec2-user ~]$ h
```

L'output del comando h è simile al seguente.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

SSH client

Da utilizzare SysRq in un client SSH

1. Connettiti alla console seriale dell'istanza.
2. Per inviare una richiesta di interruzione, premi ~B (tilde, seguita da B maiuscolo).

```
[ec2-user ~]$ ~B
```

3. Per emettere un SysRq comando, premi il tasto sulla tastiera che corrisponde al comando richiesto. Ad esempio, per visualizzare un elenco di SysRq comandi, premeteh.

```
[ec2-user ~]$ h
```

L'output del comando h è simile al seguente.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

> **Note**
>
> Il comando utilizzato per l'invio di una richiesta di interruzione potrebbe essere diverso a seconda del client SSH che si sta utilizzando.

(Istanze Windows) Utilizza SAC per risolvere i problemi relativi all'istanza

La funzionalità Special Admin Console (SAC) di Windows consente di risolvere i problemi relativi a un'istanza di Windows. Collegandosi alla console seriale dell'istanza e utilizzando SAC, potrai interrompere il processo di avvio e avviare Windows in modalità provvisoria.

> **Note**
>
> Se si abilita SAC su un'istanza, i servizi EC2 che si basano sul recupero della password non funzioneranno dalla console Amazon EC2. Gli agenti di avvio di Windows su Amazon EC2 (EC2Config, EC2Launch v1 e EC2Launch v2) si affidano alla console seriale per eseguire varie attività. Queste attività non vengono eseguite correttamente quando si abilita SAC su un'istanza. Per ulteriori informazioni sugli agenti di avvio di Windows su Amazon EC2, consulta the section called "Configurazione di istanze Windows". Se abiliti SAC, puoi disabilitarlo in un secondo momento. Per ulteriori informazioni, consulta Disabilitazione di SAC e del menu di avvio.

Processi

- Utilizzo di SAC
- Utilizzo del menu di avvio
- Disabilitazione di SAC e del menu di avvio

Utilizzo di SAC

Per utilizzare SAC

1. Collegarsi alla console seriale.

   Se SAC è abilitato sull'istanza, la console seriale visualizza il prompt `SAC>`.

```
Computer is booting, SAC started and initialized.

Use the "ch -?" command for information about using channels.
Use the "?" command for general help.


SAC>?
EVENT: The CMD command is now available.
SAC
```

2. Per visualizzare i comandi SAC, immettere ?, quindi premere Invio.

   Output previsto

```
SAC>?
ch                  Channel management commands.  Use ch -? for more help.
cmd                 Create a Command Prompt channel.
d                   Dump the current kernel log.
f                   Toggle detailed or abbreviated tlist info.
? or help           Display this list.
i                   List all IP network numbers and their IP addresses.
i <#> <ip> <subnet> <gateway> Set IPv4 addr., subnet and gateway.
id                  Display the computer identification information.
k <pid>             Kill the given process.
l <pid>             Lower the priority of a process to the lowest possible.
lock                Lock access to Command Prompt channels.
m <pid> <MB-allow>  Limit the memory usage of a process to <MB-allow>.
p                   Toggle paging the display.
r <pid>             Raise the priority of a process by one.
s                   Display the current time and date (24 hour clock used).
s mm/dd/yyyy hh:mm  Set the current time and date (24 hour clock used).
t                   Tlist.
restart             Restart the system immediately.
shutdown            Shutdown the system immediately.
crashdump           Crash the system. You must have crash dump enabled.
```

3. Per creare un canale del prompt dei comandi (ad esempio `cmd0001` o `cmd0002`), immettere cdm, quindi premere Invio.
4. Per visualizzare il canale del prompt dei comandi, premere ESC, quindi premere SCHEDA.

   Output previsto

```
Name:                 Cmd0001
Description:          Command
Type:                 VT-UTF8
Channel GUID:         ef9f20a0-1287-11eb-82b0-0e4ba51872e5
Application Type GUID: 63d02271-8aa4-11d5-bccf-00b0d014a2d0

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

5. Per cambiare canale, premere ESC+TAB+numero canale insieme. Ad esempio, per passare al canale `cmd0002` (se è stato creato), premere ESC+TAB+2.
6. Immettere le credenziali richieste dal canale del prompt dei comandi.

```
Please enter login credentials.
Username: Administrator
Domain  : .
Password: *******
```

Il prompt dei comandi è la stessa shell dei comandi completa che si ottiene su un desktop ma con l'eccezione che non consente la lettura di caratteri che erano già stati emessi.

```
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>diskpart

Microsoft DiskPart version 10.0.17763.1

Copyright (C) Microsoft Corporation.
On computer: EC2AMAZ-ASR4SAI

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online           46 GB    46 GB

DISKPART>
```

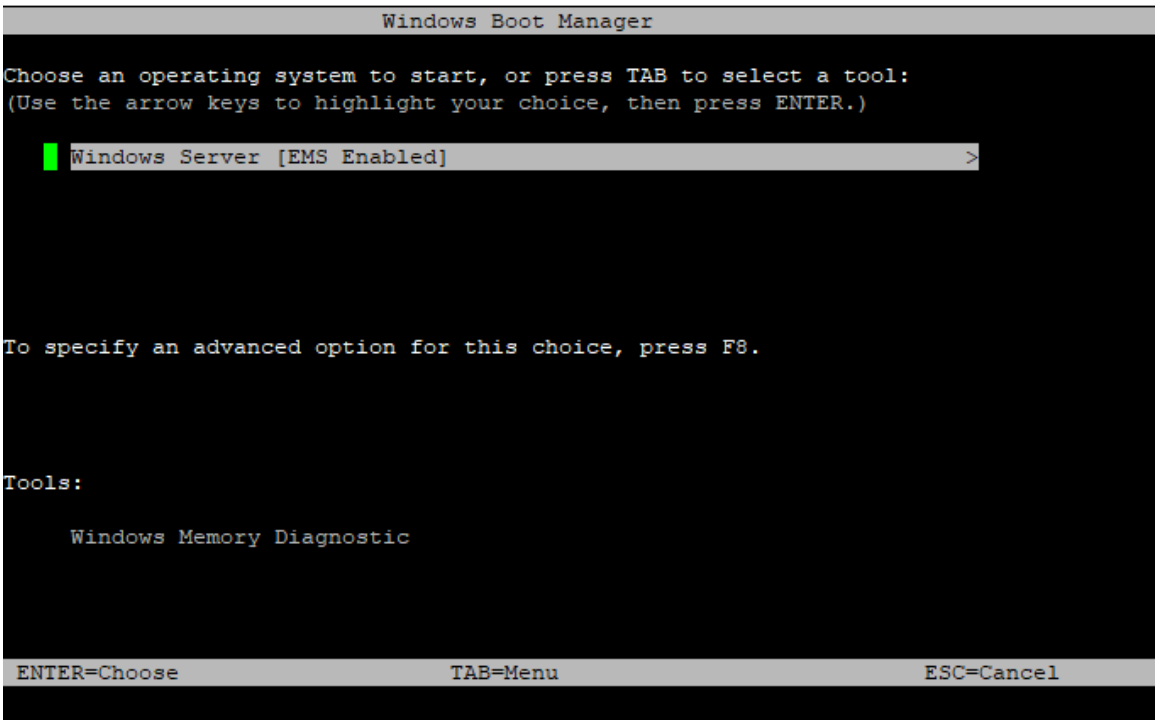
PowerShell può essere utilizzato anche dal prompt dei comandi.

Tieni presente che potrebbe essere necessario impostare la preferenza di avanzamento sulla modalità silenziosa.

```
PS C:\Windows\system32> $ProgressPreference="SilentlyContinue"
PS C:\Windows\system32> $computerInfo = Get-ComputerInfo
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Name
Intel(R) Xeon(R) Platinum 8124M CPU @ 3.00GHz
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Description
Intel64 Family 6 Model 85 Stepping 4
PS C:\Windows\system32>
```

Utilizzo del menu di avvio

Se l'istanza ha il menu di avvio abilitato ed è riavviata dopo la connessione attraverso SSH, il menu di avvio dovrebbe essere visualizzato come riportato di seguito.



Comandi del menu di avvio

INVIO

Avvia la voce selezionata del sistema operativo.

Tasto TAB

Passa al menu Strumenti.

ESC

Annulla e riavvia l'istanza.

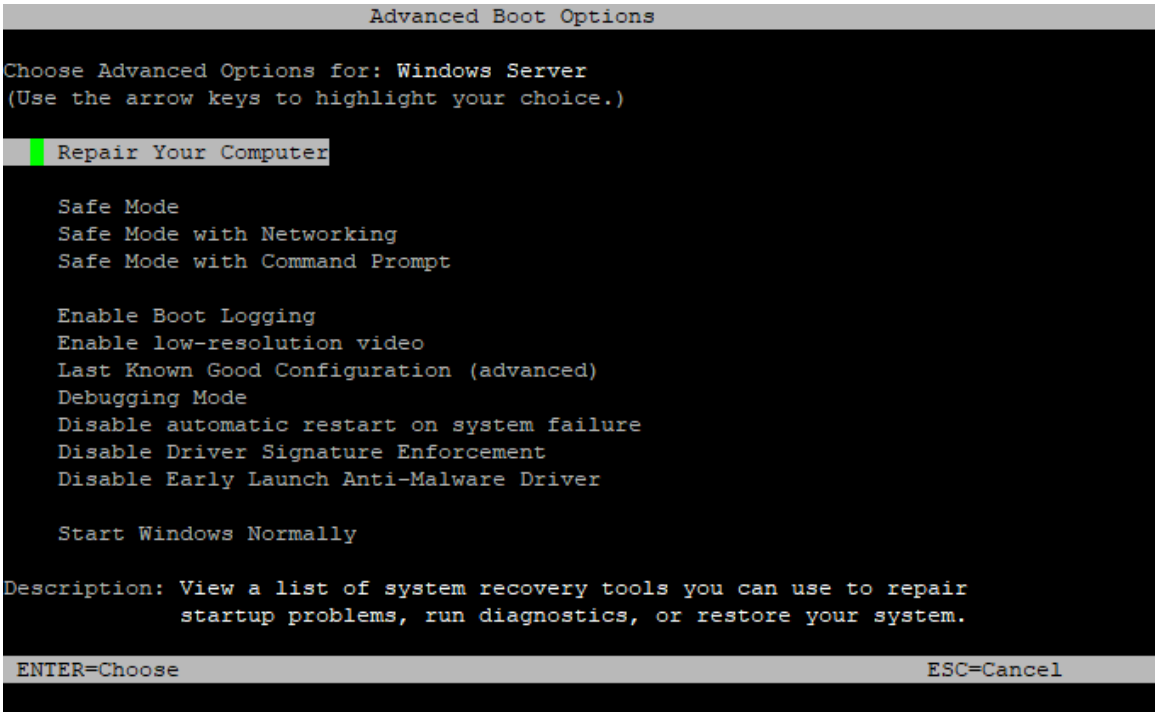
ESC seguito da 8

Equivalente a premere F8. Mostra le opzioni avanzate per l'elemento selezionato.

Tasto ESC + freccia sinistra

Torna al menu di avvio iniziale.

Il tasto ESC da solo non consente di tornare al menu principale perché Windows resta in attesa di vedere se è in corso una sequenza di escape.



Disabilitazione di SAC e del menu di avvio

Se abiliti SAC e il menu di avvio, puoi disabilitare queste funzionalità in un secondo momento.

Utilizza uno dei metodi seguenti per disabilitare SAC e il menu di avvio su un'istanza.

PowerShell

Per disabilitare SAC e il menu di avvio in un'istanza di Windows

1. Connettiti alla tua istanza ed esegui i seguenti passaggi da una riga di PowerShell comando con privilegi elevati.
2. Per prima cosa disabilita il menu di avvio modificando il valore in no.

```
bcdedit /set '{bootmgr}' displaybootmenu no
```

3. Modifica quindi il valore in `off` per disabilitare SAC.

```
bcdedit /ems '{current}' off
```

4. Applica la configurazione aggiornata riavviando l'istanza.

```
shutdown -r -t 0
```

Command prompt

Per disabilitare SAC e il menu di avvio in un'istanza di Windows

1. Connettiti all'istanza ed esegui la procedura dal prompt dei comandi.
2. Per prima cosa disabilita il menu di avvio modificando il valore in no.

```
bcdedit /set {bootmgr} displaybootmenu no
```

3. Modifica quindi il valore in `off` per disabilitare SAC.

```
bcdedit /ems {current} off
```

4. Applica la configurazione aggiornata riavviando l'istanza.

```
shutdown -r -t 0
```

Inviare un'interruzione della diagnostica per eseguire il debug di un'istanza Amazon EC2 non raggiungibile

> **Warning**
>
> Le interruzioni della diagnostica sono destinate all'uso da parte di utenti avanzati. Un utilizzo errato potrebbe influire negativamente sull'istanza. L'invio di un'interruzione della diagnostica a un'istanza potrebbe innescare l'arresto anomalo e il riavvio di della stessa, il che potrebbe causare la perdita di dati.

Puoi inviare un'interruzione della diagnostica a un'istanza non raggiungibile o che non risponde per attivare un kernel panic per un'istanza Linux o uno stop error (comunemente chiamato blue screen error) per un'istanza Windows.

Istanze Linux

I sistemi operativi Linux in genere si arrestano e vengono riavviati quando si verifica un kernel panic. Il comportamento specifico del sistema operativo dipende dalla sua configurazione. Un kernel panic può anche essere utilizzato per fare in modo che il kernel del sistema operativo dell'istanza esegua delle attività, come generare un file dump di arresto. Puoi quindi usare le informazioni del file dump di

arresto per condurre un'analisi delle cause root ed eseguire il debugging dell'istanza. I dati dump di arresto vengono generati localmente dal sistema operativo sull'istanza stessa.

Istanze Windows

In generale, i sistemi operativi Windows si arrestano e vengono riavviati quando si verifica uno stop error, ma il comportamento specifico dipende dalla sua configurazione. Uno stop error può anche portare il sistema operativo a scrivere informazioni di debugging, come il dump di una memoria kernel, su file. È quindi possibile utilizzare questa informazione per eseguire analisi della causa root per effettuare il debugging dell'istanza. I dati dump della memoria vengono generati localmente dal sistema operativo sull'istanza stessa.

Prima di inviare un'interruzione della diagnostica all'istanza, si consiglia di consultare la documentazione del sistema operativo in uso e quindi apportare le modifiche necessarie alla configurazione.

Indice

- Tipi di istanze supportati
- Prerequisiti
- Invio di un'interruzione della diagnostica

Tipi di istanze supportati

L'interruzione diagnostica è supportata su tutti i tipi di Nitro-based istanze, ad eccezione di quelle alimentate dai processori AWS Graviton. Per ulteriori informazioni, consulta le istanze basate sul sistema AWS Nitro e Graviton. AWS

Prerequisiti

Prima di utilizzare l'interruzione della diagnostica, è necessario configurare il sistema operativo dell'istanza. Questo garantisce l'esecuzione delle azioni necessarie se si verifica un kernel panic (istanze Linux) o uno stop error (istanze Windows).

Istanze Linux

Per configurare Amazon Linux 2 o Amazon Linux 2023 e generare un dump di arresto quando si verifica un kernel panic

1. Connettiti alla tua istanza.

2. Installa kexec e kdump.

```
[ec2-user ~]$ sudo yum install kexec-tools -y
```

3. Configura il kernel per prenotare una quantità di memoria adeguata per il kernel secondario. La quantità di memoria da prenotare dipende dalla memoria totale disponibile dell'istanza. Apri il file `/etc/default/grub` con l'editor di testo che preferisci, individua la riga che inizia con `GRUB_CMDLINE_LINUX_DEFAULT` e quindi aggiungi il parametro `crashkernel` nel formato seguente: `crashkernel=`*`memory_to_reserve`*. Ad esempio, per prenotare `256MB`, modifica il file `grub` come segue:

```
GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=256M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0"
GRUB_TIMEOUT=0
GRUB_DISABLE_RECOVERY="true"
```

4. Salva i cambiamenti e chiudi il file `grub`.
5. Ricompila il file di configurazione GRUB2.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. Nelle istanze basate sui processori Intel e AMD, il comando `send-diagnostic-interrupt` invia una unknown non-maskable interrupt (NMI) all'istanza. Devi configurare il kernel in modo che si arresti quando riceve una NMI sconosciuta. Apri il file `/etc/sysctl.conf` utilizzando qualsiasi editor di testo e aggiungi il seguente script.

```
kernel.unknown_nmi_panic=1
```

7. Riavvia e riconnettiti all'istanza.
8. Verifica che il kernel sia stato riavviato con il parametro `crashkernel` corretto.

```
$ grep crashkernel /proc/cmdline
```

Il seguente output di esempio indica una configurazione corretta.

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-
e38f-408e-878b-fed395b47ad6 ro crashkernel=256M console=tty0 console=ttyS0,115200n8
```

```
net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
rd.shell=0
```

9. Verifica che il servizio kdump sia in esecuzione.

```
[ec2-user ~]$ systemctl status kdump.service
```

Il seguente output di esempio mostra il risultato se il servizio kdump è in esecuzione.

```
kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset:
enabled)
   Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago
  Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
 Main PID: 2503 (code=exited, status=0/SUCCESS)
```

> **Note**
>
> Per impostazione predefinita, il file dump di arresto viene salvato su `/var/crash/`. Per cambiare la posizione, modifica il file `/etc/kdump.conf` tramite l'editor di testo che preferisci.

Per configurare SUSE Linux Enterprise, Ubuntu o Red Hat Enterprise Linux

Nelle istanze basate sui processori Intel e AMD, il comando `send-diagnostic-interrupt` invia una unknown non-maskable interrupt (NMI) all'istanza. È necessario configurare il kernel affinché si arresti quando riceve il NMI modificando il file di configurazione del sistema operativo. Per informazioni su come configurare il kernel affinché si arresti, consultare la documentazione per il sistema operativo in uso:

- SUSE Linux Enterprise
- Ubuntu
- Red Hat Enterprise Linux (RHEL)

Istanze Windows

Per configurare Windows e generare un dump della memoria quando si verifica uno stop error

1. Connettiti alla tua istanza.
2. Apri il Pannello di controllo e seleziona Sistema, Impostazioni avanzate di sistema.
3. Nella finestra di dialogo Proprietà di sistema, selezionare la scheda Avanzate.
4. Nella sezione Avvio e ripristino, selezionare Impostazioni....
5. Nella sezione Arresto sistema, configurare le impostazioni richieste e scegliere OK.

Per ulteriori informazioni sulla configurazione degli stop error di Windows consulta Panoramica delle opzioni del file dump di memoria per Windows.

Invio di un'interruzione della diagnostica

Dopo aver completato le modifiche di configurazione necessarie, puoi inviare un'interruzione diagnostica alla tua istanza utilizzando l'API AWS CLI o Amazon EC2.

AWS CLI

Per inviare un'interruzione della diagnostica all'istanza

Utilizza il comando send-diagnostic-interrupt.

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

PowerShell

Per inviare un'interruzione della diagnostica all'istanza

Utilizza il cmdlet Send-EC2DiagnosticInterrupt.

```
Send-EC2DiagnosticInterrupt -InstanceId i-1234567890abcdef0
```

Cronologia dei documenti per la Guida per l’utente di Amazon EC2

Nella seguente tabella sono descritte importanti aggiunte alla Guida per l’utente di Amazon EC2 a partire dal 2019. La guida viene inoltre aggiornata frequentemente per rispondere al feedback che ci invii.

Modifica	Descrizione	Data
Controlli delle autorizzazioni per EC2 Fast Launch	Sono state aggiunte indicazioni su come Amazon EC2 convalida le autorizzazioni quando abiliti EC2 Fast Launch con un modello di avvio, inclusa una considerazione di sicurezza per l'utilizzo della versione del modello o launch. `$Latest` `$Default`	14 agosto 2026
Visualizzazione della mappa per regioni e zone	La pagina Regioni e zone in AWS Global View ora include una vista mappa che mostra tutte le regioni e le zone su una mappa del mondo interattiva. Puoi passare dalla visualizzazione a elenco alla visualizzazione Mappa e viceversa. La tua preferenza di visualizzazione persiste tra le sessioni.	12 agosto 2026
Sostituisci il volume principale corrente con un volume EBS esistente	Puoi sostituire il volume principale corrente di un'istanza Amazon EC2 con un volume Amazon EBS esistente che hai già configurato.	9 luglio 2026

Il modello di lancio aggiuntivo sostituisce la flotta EC2 «istantanea»	Le flotte EC2 di tipo `instant` ora supportano i seguenti parametri aggiuntivi di sostituzione del modello di avvio:,, e. `IamInstanceProfile` `KeyName` `MetadataOptions`	9 luglio 2026
Trova il parametro SSM per un'AMI pubblica	Puoi trovare il AWS Systems Manager parametro associato a un'AMI pubblica e utilizzarlo per fare riferimento automaticamente alla versione più recente di tale AMI.	7 luglio 2026
SEV-SNP sugli host dedicati	AMD SEV-SNP è ora supportato su host dedicati, consentendoti di eseguire i tuoi carichi di lavoro informatici riservati su server fisici completamente dedicati al tuo uso.	1 luglio 2026
AWS Vista globale	EC2 Global View è ora rinominato AWS Global View. Puoi usarlo per visualizzare le tue risorse EC2 e altre AWS risorse supportate in tutte le regioni in un'unica visualizzazione.	30 giugno 2026

Precision-time gruppo di collocamento	È possibile utilizzare un gruppo di posizionamento in tempo di precisione per collocare istanze sull'hardware con accesso diretto a sorgenti temporali ad alta precisione nell'infrastruttura. AWS	29 giugno 2026
Usa le filigrane con le AMI consentite	Ora puoi utilizzare le filigrane AMI con le AMI consentite per limitare l'avvio delle istanze solo alle AMI con filtri di filigrana specificati. Il nuovo parametro delle AMI consentite include i seguenti filtri:,, e. `ImageWatermarks` `MaximumDaysSinceSourceImageCreated` `MaximumDaysSinceWatermarkCreated` `SourceImageRegion` `WatermarkKey`	22 giugno 2026
AWS Dispositivo VMClock per Windows	AWS fornisce un pacchetto di driver nullo (senza funzioni) per Windows che consente al sistema operativo di riconoscere il dispositivo.	17 giugno 2026
Filigrane AMI	Puoi utilizzare le filigrane AMI per tracciare la provenienza e applicare le politiche di governance per le tue AMI private. Le filigrane persistono quando crei AMI da istanze, copi le AMI o condividi le AMI con altri account.	10 giugno 2026

Annulla una prenotazione di capacità	È possibile annullare una prenotazione di capacità con data futura. A seconda della data di annullamento, potrebbe essere applicato un addebito.	2 giugno 2026
Supporto ENA Express Cross-AZ	ENA Express ora supporta il traffico tra istanze Amazon EC2 in diverse zone di disponibilità all'interno della stessa regione.	11 maggio 2026
Visibilità gestita delle risorse	Puoi controllare se le risorse che AWS i servizi forniscon o per tuo conto vengono visualizzate nelle visualizz azioni della console Amazon EC2 e nelle operazioni degli elenchi di API.	22 aprile 2026
Inizia con EFA e NIXL	Puoi utilizzare Elastic Fabric Adapter (EFA) con NIXL per carichi di lavoro di inferenza disaggregati.	17 marzo 2026
Tutorial: lancio di una flotta EC2 con prenotazioni di capacità interrompibile	Un nuovo tutorial mostra come creare una flotta EC2 che utilizzi le prenotazioni di capacità interrompibile per rendere disponibile la capacità riservata inutilizzata per i carichi di lavoro interrompibili.	16 marzo 2026
Blocchi di capacità nelle zone locali	I blocchi di capacità per il machine learning sono ora disponibili nelle zone locali.	25 febbraio 2026

Applicazione del protocollo IMDSv2	È possibile imporre l'uso di IMDSv2 a livello di account per ciascuno. Regione AWS Una volta applicate, le istanze possono essere avviate solo se sono configurate per richiedere IMDSv2.	24 febbraio 2026
Virtualizzazione annidata	Puoi eseguire hyperviso r, come KVM, all'interno di Hyper-V istanze Amazon EC2 virtualizzate.	16 febbraio 2026
Reti secondarie	Le reti secondarie sono reti virtuali create appositamente per casi d'uso specializzati in reti. È possibile avviare istanze EC2 selezionate sia in un VPC che in una rete secondaria.	9 febbraio 2026
Condivisione dei blocchi di capacità	Puoi condividere i blocchi di capacità EC2 con altri membri Account AWS della tua AWS organizzazione.	2 febbraio 2026
Prenotazioni di capacità interrompibile	Le prenotazioni della capacità interrompibile ti aiutano a rendere temporaneamente disponibile la capacità inutilizz ata per altri carichi di lavoro all'interno del tuo account.	21 novembre 2025
Topologia delle istanze per le istanze P6-B300	Puoi ottenere le informazioni sulla topologia per le istanze `p6-b300.48xlarge` .	18 novembre 2025

Ascendenza AMI	È ora possibile risalire all'origine di un'AMI ottenendo un elenco di tutte le AMI antenate.	12 novembre 2025
Topologia della prenotazione della capacità	Puoi utilizzare l' DescribeCapacityReservationTopology API per descrivere dove verrà posizionata la capacità riservata l'una rispetto all'altra nella gerarchia di rete prima di avviare le istanze.	28 ottobre 2025
Ottimizza le CPU per risparmiare sulle licenze	Ora puoi configurare le CPU attive per risparmiare sui costi di licenza per le istanze Windows e SQL Server incluse nella licenza.	15 ottobre 2025
Nuovo EC2 Capacity Manager	Amazon EC2 ha aggiunto EC2 Capacity Manager che consente di monitorare, analizzare e gestire l'utilizzo della capacità tra On-Demand istanze, istanze Spot e prenotazioni di capacità da un'unica posizione.	15 ottobre 2025
AWSEC2CapacityManagerServiceRolePolicy — nuova politica gestita	Amazon EC2 ha aggiunto la policy AWSEC2CapacityManagerServiceRolePolicy gestita per consentirti di gestire le risorse di capacità e integrarti con AWS le organizzazioni per tuo conto.	15 ottobre 2025

Parametro GPUPowerUtilization	Nuova metrica GPUPowerUtilization per istanze a calcolo accelerato.	13 ottobre 2025
Supporto di IPv6 per l'endpoint EC2 Instance Connect	L'endpoint EC2 Instance Connect supporta ora la connettività IPv6. Ora puoi configurare gli endpoint EC2 Instance Connect per supportare il dual-stack o IPv6 solo per la connessione a istanze con indirizzi IPv6.	2 ottobre 2025
AMI consentite: nuovi parametri	Le AMI consentite, una funzionalità che consente di limitare il rilevamento e l'uso delle AMI all'interno dell'azienda Account AWS, ora supporta quattro nuovi parametri: codici di Marketplace AWS prodotto, nomi AMI, periodo massimo dall'obsolescenza delle AMI e età massima per le AMI.	25 settembre 2025
Statistiche dettagliate delle prestazioni per i volumi di archivio dell'istanza	Amazon EC2 fornisce statistiche sulle prestazioni in tempo reale e ad alta risoluzione per i volumi di storage di istanze NVMe collegati alle istanze. Nitro-based	16 settembre 2025
Aggiornamenti dell'Host dedicato Mac di Amazon EC2	Gli Host dedicati Mac di Amazon EC2 supportano il ripristino automatico degli Host dedicati e la manutenzione degli host basata sul riavvio.	28 agosto 2025

Copie dell’AMI per le zone locali	Ora puoi copiare le EBS-backed AMI Amazon da e verso le zone locali.	28 agosto 2025
AmazonEC2ImageReferencesAccessPolicy — nuova policy gestita	Amazon EC2 ha aggiunto la policy AmazonEC2ImageReferencesAccessPolicy gestita per fornire l'autorizzazione alla scansione di tutti i tipi di risorse supportati dall'API EC2 DescribeImageReferences.	26 agosto 2025
Report di utilizzo dell’AMI	Se condividi le tue Amazon Machine Images (AMI) con altre Account AWS persone, con organizzazioni specifiche Account AWS, unità organizzative (OU) o pubblicamente, puoi vedere come vengono utilizzate creando report sull'utilizzo delle AMI. I report forniscono visibilità su quali Account AWS sono le AMI utilizzate nelle istanze EC2 o nei modelli di avvio e quante istanze o modelli di avvio fanno riferimento a ciascuna AMI.	26 agosto 2025

Riferimenti AMI	Puoi identificare AWS le tue risorse che fanno riferimento a specifiche Amazon Machine Images (AMI), indipende ntemente dal fatto che le AMI siano pubbliche o private o da chi le possiede. Questa visibilità ti aiuta a garantire che le tue risorse utilizzino le AMI conformi più recenti.	26 agosto 2025
Modifica endpoint EC2 Instance Connect	Ora puoi modificare un endpoint EC2 Instance Connect esistente utilizzando o un SDK. AWS CLI	14 agosto 2025
Miglioramenti alla condivisi one della prenotazione della capacità	Ora puoi condividere prenotazi oni della capacità create da te nei gruppi di posizionamento cluster.	12 agosto 2025

Policy gestita aggiornata per endpoint EC2 Instance Connect	Per supportare la modifica degli endpoint EC2 Instance Connect esistenti, Amazon EC2 ha aggiornato la policy `Ec2InstanceConnect Endpoint` aggiungendo autorizzazioni per assegnare e annullare l'assegnazione di indirizzi IPv6 e modificar e i gruppi di sicurezza sulle interfacce di rete create dall'endpoint EC2 Instance Connect. Amazon EC2 ha aggiornato questa policy anche per sostituire l'operato re di condizione `Null` con l'operatore di condizione `StringLike` .	31 luglio 2025
Topologia dell'istanza: supporto regionale aggiuntivo	L' DescribeInstanceTopology API è ora disponibile in Asia Pacifico (Melbourne).	31 luglio 2025
Terminazione forzata	Ora puoi forzare la terminazi one dell'istanza.	31 luglio 2025
Topologia dell'istanza: supporto regionale aggiuntivo	L' DescribeInstanceTopology API è ora disponibile in AWS GovCloud (US-West).	24 luglio 2025
Salta l'arresto del sistema operativo durante la terminazi one dell'istanza	Puoi saltare lo spegnimen to controllato del sistema operativo (OS) quando si termina un'istanza.	23 luglio 2025

Salta l'arresto del sistema operativo durante l'interruzione dell'istanza	Puoi saltare lo spegnimento controllato del sistema operativo (OS) quando si arresta un'istanza.	23 luglio 2025
P6-B200 Blocchi di capacità in us-east-1	P6-B200 I Capacity Block sono ora disponibili negli Stati Uniti orientali (Virginia settentrionale) -. `us-east-1`	23 luglio 2025
Policy gestita aggiornata per il ruolo collegato al servizio EC2 Fast Launch	Per aiutare a prevenire le risorse orfane, Amazon EC2 ha aggiornato questa policy aggiungendo l'autorizzazione a descrivere volumi, attributi dei volumi e interfacce di rete, nonché a eliminare volumi e interfacce di rete creati da EC2 Fast Launch.	17 luglio 2025
Console seriale EC2: supporto regionale aggiuntivo	La Console seriale EC2 è ora disponibile anche in Asia Pacifico (Thailandia) e Messico (Centrale).	15 luglio 2025
EC2 Instance Connect: supporto regionale aggiuntivo	EC2 Instance Connect è ora disponibile anche in Asia Pacifico (Thailandia) e Messico (Centrale).	15 luglio 2025
Marcatura temporale dei pacchetti hardware	Puoi abilitare la marcatura temporale dei pacchetti hardware sull'istanza EC2 per aggiungere una marcatura temporale con precisione in nanosecondi a 64 bit a ogni pacchetto di rete in ingresso.	23 giugno 2025

Elimina gli snapshot durante l'annullamento della registrazione dell'AMI	Quando annulli la registrazione di un'AMI, allo stesso tempo puoi eliminare automaticamente gli snapshot associati.	28 maggio 2025
User-initiated riavviare la migrazione	Quando l'istanza riceve una notifica di un evento di riavvio pianificato di EC2, viene abilitata per impostazione predefinita, ad esempio la migrazione, quando si riavvia l'istanza prima dell'evento.	20 maggio 2025
Configurazione SIP per istanze Mac di Amazon EC2	Puoi configurare le impostazioni di System Integrity Protection (SIP) per le istanze Mac x86 e Mac con processore Apple.	20 maggio 2025
Delega di proprietà del volume root	Ora puoi automatizzare la delega di proprietà del volume root per il volume root di Amazon EBS durante l'aggiornamento del sistema operativo su istanze Mac con processore Apple.	20 maggio 2025
Topologia delle istanze per le istanze P6-B200	Puoi ottenere le informazioni sulla topologia per le istanze `p6-b200.48xlarge` .	15 maggio 2025

Policy gestite aggiornate per il ruolo collegato al servizio EC2 Fast Launch	È stata aggiornata la policy sui ruoli collegati al servizio EC2 Fast Launch con accesso alla creazione e gestione delle regole EventBridge degli eventi Amazon e altre azioni per migliorare l'esperienza di EC2 Fast Launch. Per ulteriori informazioni sulle autorizzazioni concesse dal ruolo collegato ai servizi, consulta Permissions granted by `EC2FastLaunchServiceRolePolicy`.	14 maggio 2025
Policy gestite aggiornate per la policy di accesso completo di EC2 Fast Launch	Aggiornamento della policy di accesso completo di EC2 Fast Launch con autorizzazione per creare e modificare le operazioni del modello di avvio, creare risorse di rete e di gruppi di sicurezza, autorizzare le regole di ingresso ed eliminare le risorse create da EC2 Fast Launch. La policy può inoltre descrivere e creare stack ed eliminare CloudFormation gli stack creati da EC2 Fast Launch.	14 maggio 2025
Onboarding semplificato per EC2 Fast Launch	EC2 Fast Launch aggiornato per semplificare il processo di onboarding.	14 maggio 2025

AWS Config integrazione con le AMI consentite	Utilizza la AWS Config regola ec2-instance-launched-with-allowed-ami per verificare se le istanze in esecuzione o interrotte sono state avviate con AMI che soddisfano i criteri delle AMI consentite.	11 marzo 2025
Policy gestite da AWSEC2CapacityReservationFleetRolePolicy aggiornate	Amazon EC2 ha aggiornato la policy gestita `AWSEC2CapacityReservationFleetRolePolicy` per usare l'operatore di condizione `ArnLike` anziché l'operatore di condizione `StringLike` .	3 marzo 2025
Time-based Copie AMI	È ora possibile richiedere una durata di completamento per le operazioni di copia EBS-backed AMI per garantire che le copie AMI siano completate entro un periodo di tempo specifico.	25 febbraio 2025
Policy AmazonEC2ReadOnlyAccess aggiornata	Amazon EC2 ha aggiunto l'`GetSecurityGroupsForVpc` operazione alla policy esistente AmazonEC2 ReadOnlyAccess .	27 dicembre 2024
Istanze gestite	Ora puoi visualizzare le istanze gestite di Amazon EC2 nella console EC2.	1º dicembre 2024

Policy dichiarative	Ora puoi utilizzare le policy dichiarative per applicare le impostazioni a livello di account su più regioni e account contemporaneamente . Le policy dichiarative sono supportate per configurare l'accesso alla console seriale EC2, le AMI consentite, le impostazioni predefinite IMDS e le impostazioni di blocco dell'accesso pubblico per VPC, AMI e snapshot. Per ulteriori informazioni, consulta Policy dichiarative nella Guida per l'utente di AWS Organizat ions , nonché la documenta zione specifica per ciascuna funzionalità supportata.	1º dicembre 2024
AMI consentite	Ora puoi controllare il rilevamento e l'uso delle AMI in Amazon EC2 specificando i criteri che le AMI devono soddisfare.	1º dicembre 2024
Blocchi di capacità istantanei	Ora puoi prenotare blocchi di capacità per ML, che possono iniziare già dopo 30 minuti.	21 novembre 2024
Future-dated Prenotazioni di capacità	Ora puoi richiedere prenotazi oni della capacità per una data futura.	21 novembre 2024
Estensione del blocco di capacità	Ora puoi estendere la durata dei blocchi di capacità esistenti .	21 novembre 2024

Blocchi di capacità da 6 mesi	Ora puoi prenotare blocchi di capacità per ML per un massimo di 6 mesi (182 giorni).	21 novembre 2024
Set di filtri salvati	Ora puoi creare gruppi di filtri personalizzati e riutilizzarli per visualizzare in modo efficiente le tue risorse EC2.	20 novembre 2024
Protezione delle prestazioni	Quando utilizzi la selezione del tipo di istanza basata sugli attributi per il tuo parco istanze EC2 o parco istanze spot, ora puoi abilitare la protezione delle prestazioni per garantire che i tipi di istanza seleziona ti siano simili o superino un riferimento prestazionale specificato.	20 novembre 2024
Solo prenotazioni della capacità	Ora puoi specificare che le istanze vengano eseguite solo in una prenotazione della capacità o in un gruppo di risorse di prenotazione della capacità.	20 novembre 2024
Identificare AMI di origine	Ora puoi identificare l'AMI di origine utilizzata per creare un'AMI.	13 novembre 2024
Suddivisione della capacità	Puoi suddividere la capacità da una prenotazione della capacità esistente e creare una nuova prenotazione.	30 ottobre 2024

Spostare la capacità	Ora puoi spostare la capacità da una prenotazione della capacità a un'altra.	30 ottobre 2024
Tutorial per principianti	Due nuovi tutorial per principianti: Avvia la mia primissima istanza EC2 e Avvia un'istanza EC2 di prova e connettiti a essa.	21 ottobre 2024
Supporto per Windows Server 2025	Aggiunto il supporto per Windows Server 2025.	16 ottobre 2024
EC2 Global View	EC2 Global View ora ti consente di visualizzare le prenotazioni della capacità e i blocchi di capacità nel tuo account in tutte le regioni.	16 ottobre 2024
Manutenzione degli host con migrazione live	Gli host dedicati di Amazon EC2 ora supportano la manutenzione degli host con migrazione live, che effettua automaticamente la migrazione delle istanze supportate da un host dedicato danneggiato a un host dedicato sostitutivo senza arrestarle e riavviarle.	15 ottobre 2024
Assegnazione di fatturazione per prenotazioni della capacità condivise	Ora puoi assegnare la fatturazione di qualsiasi capacità disponibile di una prenotazione di capacità condivisa a un account consumatore appartenente alla stessa AWS organizzazione.	14 ottobre 2024

Clock hardware PTP: supporto regionale aggiuntivo	Il clock hardware PTP è ora disponibile anche negli Stati Uniti orientali (Ohio) e nell'Asia Pacifico (Malesia).	23 settembre 2024
EC2 Instance Connect supporta IPv6	Ora puoi utilizzare EC2 Instance Connect per connetterti all'indirizzo IPv6 pubblico dell'istanza.	23 settembre 2024
Elenchi di prefissi di EC2 Instance Connect	Ora puoi selezionare un elenco di prefissi gestiti per gli indirizzi IPv4 o IPv6 durante la creazione di regole nei gruppi di sicurezza per consentire il traffico SSH dal servizio EC2 Instance Connect.	23 settembre 2024
Nuove funzionalità per gestire le prenotazioni On-Demand di capacità	Ora puoi suddividere la tua prenotazione della capacità, spostare la capacità tra le prenotazioni della capacità e modificare l'attributo di idoneità dell'istanza della tua prenotazione della capacità.	14 agosto 2024
Supporto per l'ibernazione per C6g, C6gn, C6gd, C7g, C7gd, M6g, M6gd, M7g, M7gd, R6g e R6gd	Iberna le istanze appena avviate in esecuzione sui tipi di istanza C6g, C6gn, C6gd, C7g, C7gd, M6g, M6gd, M7g, M7gd, R6g e R6gd.	30 luglio 2024
Supporto di ibernazione per AMI che supportano i tipi di istanza Graviton	Iberna le istanze appena avviate da un'AMI Amazon Linux o Ubuntu che supporta i tipi di istanza Graviton.	30 luglio 2024

Tipi di istanza aggiuntivi supportati per Credential Guard	Ora puoi abilitare Credential Guard per le istanze C7i C7-flex, M7i M7i-flex, R7i e T3. R7i-flex	26 giugno 2024
Strumento di ricerca del tipo di istanza EC2 – Parametri aggiuntivi	Lo strumento di ricerca del tipo di istanza EC2 ora fornisce parametri aggiuntiv i per specificare requisiti più dettagliati per il carico di lavoro.	5 giugno 2024
Nuova policy gestita per EC2 Fast Launch	Aggiunta della policy EC2FastLaunchFullAccess per eseguire azioni API relative alla funzionalità di avvio rapido EC2 da un'istanza.	14 maggio 2024
Protezione dall'annullamento della registrazione AMI	Puoi attivare la protezion e dall'annullamento della registrazione su un'AMI per impedirne l'eliminazione accidentale o dannosa.	23 aprile 2024
Clock hardware PTP – Supporto per tipi di istanze	Il clock hardware PTP è ora disponibile sui tipi di istanza M7a, M7g, M7i, R7a e R7i.	22 aprile 2024
Sono state aggiunte considera zioni sulle prestazioni di Nitro per una rete avanzata	Questa pagina si concentra su considerazioni di rete per aiutarti a ottimizzare le prestazioni delle istanze Amazon EC2 basate su Nitro.	4 aprile 2024

Nuova policy gestita per gli snapshot EBS basati su VSS	Amazon EC2 VSS dispone di una nuova policy gestita da IAM che puoi aggiunger e al ruolo del profilo dell'ista nza per garantire che le tue autorizzazioni rimangano aggiornate e seguano le best practice.	28 marzo 2024
Clock hardware PTP – Stati Uniti orientali (Virginia settentri onale)	Il clock hardware PTP è ora disponibile nella regione Stati Uniti orientali (Virginia settentri onale).	26 marzo 2024
Configurazione di IMDSv2 come impostazione predefinita dell'account	Puoi impostare tutti i nuovi avvii di istanza EC2 nel tuo account in modo da utilizzar e Instance Metadata Service versione 2 (IMDSv2) per impostazione predefinita.	25 marzo 2024
Assegna tag alle nuove AMI Linux create da uno snapshot	Quando crei un'AMI Linux da uno snapshot, puoi assegnare tag alla nuova AMI.	7 marzo 2024
Assegna tag alle nuove AMI e agli snapshot durante la copia	Quando copi un'AMI, puoi contrassegnare la nuova AMI e i nuovi snapshot con gli stessi tag, oppure contrasse gnarli con tag diversi.	7 marzo 2024

AWS Rimuovi le pagine del Management Pack	Il AWS Management Pack è stato utilizzato principal mente con Windows Server 2012 e versioni precedenti. Queste versioni precedenti della piattaforma del sistema operativo non sono più supportate. Per gestire e risolvere i problemi relativi alla tua flotta di server in esecuzione in locale AWS e in locale, consulta AWS Systems Manager Fleet Manager.	12 febbraio 2024
EC2 Instance Connect preinstallato sulle AMI macOS	EC2 Instance Connect ora è preinstallato su macOS Sonoma 14.2.1 o versioni successive, macOS Ventura 13.6.3 o versioni successive e macOS Monterey 12.7.2 o versioni successive.	26 gennaio 2024
Supporto per CentOS, macOS e RHEL di EC2 Instance Connect	Ora è possibile installare EC2 Instance Connect sulle AMI supportate di CentOS, macOS e RHEL.	6 dicembre 2023
Supporto per l'ibernazione per C7a, C7i, R7a, R7i e R7iz	Iberna le istanze appena avviate in esecuzione sui tipi di istanza C7a, C7i, R7a, R7i e R7iz.	1 dicembre 2023

Selettore del tipo di istanza EC2 di Amazon Q	Il selettore del tipo di istanza EC2 di Amazon Q considera il caso d’uso, il tipo di carico di lavoro e le preferenze del produttore della CPU, nonché il modo in cui dai priorità a prezzo e prestazioni. Utilizza quindi questi dati per fornire indicazioni e suggerimenti per i tipi di istanze Amazon EC2 più adatti ai nuovi carichi di lavoro.	28 novembre 2023
Piano gratuito EC2	Puoi monitorare l’utilizzo del piano gratuito di EC2 dal pannello di controllo di EC2.	26 novembre 2023
Console-to-Code	Console-to-Code può aiutarti a iniziare con il tuo codice di automazione. Console-to-Code registra le azioni della console e quindi utilizza l'intelli genza artificiale generativ a per suggerire il codice nell'infrastruttura preferita, come formato di codice. Puoi usare il codice come punto di partenza, personalizzandolo per renderlo pronto per la produzione per il tuo caso d’uso specifico.	26 novembre 2023

Timeout configurabili per il tracciamento delle connessioni inattive	Le connessioni dei gruppi di sicurezza che rimangono inattive possono portare all'esaurimento del tracciamento delle connessioni, impedire il tracciamento delle connessioni ed eliminare i pacchetti. Ora puoi impostare il timeout in secondi per il tracciamento delle connessioni del gruppo di sicurezza su un'interfaccia di rete elastica.	17 novembre 2023
Clock hardware PTP	Le istanze supportate ora dispongono di un clock hardware PTP (Precision Time Protocol). Il clock hardware PTP supporta NTP o una connessione PTP diretta.	16 novembre 2023
Cambio del tipo di istanza per l'istanza abilitata per l'ibernazione	Adesso puoi modificare il tipo di istanza di un'istanza abilitata per l'ibernazione quando si trova nello stato `stopped`.	16 novembre 2023
Topologia delle istanze	Puoi utilizzare l' DescribeInstanceTopology API per rilevare la posizione delle tue istanze e quindi utilizzare queste informazioni per ottimizzare i processi HPC e ML eseguendoli su istanze fisicamente più vicine tra loro.	13 novembre 2023

Supporto delle AMI per EC2 Fast Launch	Ora puoi abilitare EC2 Fast Launch su un'AMI condivisa con te. Quando si abilita EC2 Fast Launch su un'AMI condivisa, gli snapshot pre-assegnati per l'avvio rapido vengono creati nel tuo account.	6 novembre 2023
Blocchi di capacità per ML	Ora puoi prenotare istanze GPU in date future per supportare i tuoi carichi di lavoro di machine learning (ML) di breve durata.	31 ottobre 2023
Ibernazione di istanze spot	Ora puoi ibernare le tue istanze Spot utilizzando la stessa esperienza di ibernazione e le stesse famiglie di istanze attualmente disponibili per le istanze. On-Demand	24 ottobre 2023
Blocco dell'accesso pubblico per le AMI per impostazione predefinita	Il blocco dell'accesso pubblico per le AMI è ora abilitato per impostazione predefinita per tutti i nuovi account e per gli account esistenti senza AMI pubbliche.	20 ottobre 2023
Amazon EC2 Global View	Amazon EC2 Global View supporta tipi di risorse aggiuntivi e opzioni di visualizzazione personalizzabili.	18 ottobre 2023
Supporto dell'ibernazione per Ubuntu 22.04.2 LTS (Jammy Jellyfish)	Iberna le istanze appena avviate dall'AMI Ubuntu 22.04.2 LTS (Jammy Jellyfish).	16 ottobre 2023

Disabilitazione di un'AMI	È possibile disabilitare un'AMI per impedirne l'utilizzo per gli avvii delle istanze.	12 ottobre 2023
Controlli dello stato dei volumi EBS collegati	È possibile utilizzare i controlli dello stato dei volumi EBS collegati per monitorare se i volumi Amazon EBS collegati a un'istanza sono raggiungibili.	11 ottobre 2023
Supporto di ibernazione per Red Hat Enterprise Linux 9	Ibernazione delle istanze appena avviate da AMI Red Hat Enterprise Linux 9.	2 ottobre 2023
Supporto di ibernazione per Microsoft Windows Server 2022	Ibernazione delle istanze appena avviate da AMI Microsoft Windows Server 2022.	2 ottobre 2023
Supporto per l'ibernazione per AL2023	Ibernazione delle istanze appena avviate da AMI AL2023.	2 ottobre 2023
Avvio dell'interruzione delle istanze spot in una serie di istanze spot	Puoi selezionare una serie di istanze spot nella console di Amazon EC2 e avviare un'interruzione delle istanze spot della serie in modo da poter provare in che modo le applicazioni sulle tue istanze spot gestiscono le interruzioni.	21 settembre 2023
Blocco dell'accesso pubblico sulle AMI	Puoi abilitare il blocco dell'accesso pubblico alle AMI a livello di account per bloccare qualsiasi tentativo di rendere pubbliche le tue AMI.	12 settembre 2023

Supporto per l'ibernazione per M7i e M7i-flex	Metti in ibernazione le istanze appena lanciate in esecuzion e su M7i e i tipi di istanza. M7i-flex	22 agosto 2023
EC2-Classic è stato deprecato	Con EC2-Classic, le istanze EC2 venivano eseguite in un'unica rete piatta condivisa con altri clienti. Amazon VPC sostituisce. EC2-Classic Con Amazon VPC, le istanze vengono eseguite in un cloud privato virtuale (VPC) isolato a livello logico dall'account AWS .	8 agosto 2023
Host dedicati	È possibile allocare host dedicati su risorse hardware specifiche in un Outpost.	20 giugno 2023
Endpoint EC2 Instance Connect	Ora puoi connetterti a un'istanza tramite SSH o RDP senza che l'istanza abbia un indirizzo IPv4 pubblico.	13 giugno 2023
IMDS Package Analyzer	Ora puoi utilizzare IMDS Packet Analyzer per identific are le origini delle chiamate IMDSv1 sulle tue istanze EC2.	1 giugno 2023
Istanze bare metal della Console seriale EC2	La console seriale EC2 ora supporta la connettività alla porta seriale di istanze bare metal selezionate.	11 aprile 2023

Quote per i modelli di avvio	Ora è possibile visualizzare le quote per i modelli di avvio e le versioni dei modelli di avvio nella console Service Quotas e utilizzando la CLI Service Quotas.	3 aprile 2023
Notifiche sull'utilizzo delle prenotazioni di capacità	AWS Health ora invia notifiche quando l'utilizzo della capacità per le prenotazioni di capacità nel tuo account scende al di sotto del 20 percento.	3 aprile 2023
Gruppi Prenotazione della capacità	Ora puoi aggiungere le prenotazioni di capacità condivise con te ai gruppi di prenotazioni di capacità di cui sei proprietario.	30 marzo 2023
Modifica opzioni dei metadati dell'istanza	Ora puoi utilizzare la console Amazon EC2 per modificare le opzioni dei metadati dell'ista nza.	20 marzo 2023
In-place aggiornamenti del sistema operativo macOS	Ora puoi eseguire aggiornam enti locali del sistema operativo Apple macOS sulle istanze Mac M1.	14 marzo 2023
UEFI preferred	Ora puoi creare un'unica AMI che supporta sia la modalità di avvio Unified Extensible Firmware Interface (UEFI) che BIOS legacy.	3 marzo 2023

Modifica di un'AMI per IMDSv2	Modifica l'AMI esistente in modo che le istanze avviate dall'AMI richiedano IMDSv2 per impostazione predefinita.	28 febbraio 2023
Virtualization-based Sicurezza di Windows - Credential Guard	Puoi abilitare Credentia l Guard, una funzionalità Virtualization-based di sicurezza (VBS), sulle istanze Amazon EC2 supportate.	31 gennaio 2023
Nuova policy gestita per endpoint EC2 Instance Connect	È stata aggiunta la `Ec2InstanceConnect Endpoint` policy, associata al ruolo AWSServiceRoleForE C2InstanceConnect collegato al servizio, per consentire ad Amazon EC2 di eseguire azioni per tuo conto quando crei un endpoint EC2 Instance Connect.	24 gennaio 2023
Alias AMI nei modelli di avvio	Puoi specificare un AWS Systems Manager parametro al posto dell'ID AMI nei modelli di avvio per evitare di dover aggiornare i modelli ogni volta che l'ID AMI cambia.	19 gennaio 2023
Supporto di ibernazione per C6i, I3en e M6i	Iberna le istanze appena avviate in esecuzione sui tipi di istanza C6i, I3en e M6i.	19 dicembre 2022

Prevenzione delle distorsioni di scrittura	Migliora le prestazioni dei carichi di lavoro dei tuoi database I/O-intensive relazionali e riduci la latenza senza influire negativamente sulla resilienza dei dati con la prevenzione delle scritture strappate, una funzionalità di archiviazione a blocchi.	29 novembre 2022
ENA Express	Aumenta il throughput e minimizza la latenza di coda del traffico di rete tra le istanze EC2 con ENA Express.	28 novembre 2022
Copia di tag dell'AMI	Quando copi un'AMI, puoi copiare contemporaneamente i tag dell'AMI definiti dall'utente.	18 novembre 2022
Dimensioni dell'AMI per l'archiviazione e il ripristino	La dimensione di un'AMI (prima della compressione) che può essere archiviata e ripristinata da e verso un bucket Amazon S3 ora può arrivare a 5.000 GB.	16 novembre 2022
Strategia di allocazione di priceCapacityOptimized per le Istanze spot	Un parco istanze Spot che utilizza la strategia di allocazione `priceCapacityOptimized` analizza sia il prezzo sia la capacità per selezionare i pool di istanze spot che hanno meno probabilità di essere interrotti e hanno il prezzo più basso possibile.	10 novembre 2022

Strategia di allocazione di price-capacity-optimized per le Istanze spot	Un parco istanze EC2 che utilizza la strategia di allocazione `price-capacity-optimized` analizza sia il prezzo sia la capacità per selezionare i pool di istanze spot che hanno meno probabilità di essere interrotti e hanno il prezzo più basso possibile.	10 novembre 2022
Annullamento la condivisione di un'AMI con il tuo account	Se un'AMI è stata condivisa con te Account AWS e non desideri più che sia condivisa con il tuo account, puoi rimuovere il tuo account dalle autorizzazioni di avvio dell'AMI.	4 novembre 2022
Trasferimento degli indirizzi IP elastici	Ora puoi trasferire gli indirizzi IP elastici da uno Account AWS all'altro.	31 ottobre 2022
Sostituzione di un volume root	Puoi sostituire il volume Amazon EBS root per un'istanza in esecuzione utilizzando un'AMI.	27 ottobre 2022
Connessione automatica dell'istanza al database	Usa la funzione di connessione automatica per connettere rapidamente una o più istanze EC2 a un database RDS per consentire il traffico tra queste.	10 ottobre 2022
Quote delle AMI	Ora le quote si applicano alla creazione e alla condivisione di AMI.	10 ottobre 2022

Configurazione di un'AMI per IMDSv2	Configura un'AMI in modo che le istanze avviate dall'AMI richiedano IMDSv2 per impostazione predefinita.	3 ottobre 2022
Avvio dell'interruzione di un'istanza spot	Puoi selezionare un'istanza spot nella console di Amazon EC2 e avviare un'interruzione in modo da poter provare in che modo le applicazioni sulle tue istanze spot gestiscono le interruzioni.	26 settembre 2022
Fornitore di AMI verificato	Nella console Amazon EC2, le AMI pubbliche di proprietà di Amazon o di un partner Amazon verificato sono contrassegnate dalla dicitura Verified provider (fornitore verificato).	22 luglio 2022
Gruppi di collocamento attivi AWS Outposts	Aggiunta una strategia di diffusione degli host per i gruppi di collocamento su un outpost.	30 giugno 2022
Host dedicati su AWS Outposts	È possibile allocare host dedicati su AWS Outposts.	31 maggio 2022
Protezione da arresto delle istanze	Se desideri che un'istanza non venga arrestata per errore, puoi abilitare la funzionalità di protezione da arresto per tale istanza.	24 maggio 2022

UEFI Secure Boot	UEFI Secure Boot si basa sul processo di avvio sicuro di lunga data di Amazon EC2 e fornisce un'ulteriore difesa approfondita per aiutare i clienti a proteggere il software dalle minacce che persistono tra i riavvii.	10 maggio 2022
NitroTPM	Nitro Trusted Platform Module (NitroTPM) è un dispositivo virtuale fornito dal sistema AWS Nitro e conforme alle specifiche TPM 2.0.	10 maggio 2022
Eventi di modifica dello stato dell'AMI	Amazon EC2 ora genera un evento quando un'AMI cambia stato. Puoi usare Amazon per rilevare e reagire EventBridge a questi eventi.	09 maggio 2022
Descrizione delle chiavi pubbliche	È possibile eseguire query sulla chiave pubblica e sulla data di creazione di una coppia di chiavi Amazon EC2.	28 aprile 2022
Creazione di coppie di chiavi	È possibile specificare il formato della chiave (PEM o PPK) quando si crea una nuova coppia di chiavi.	28 aprile 2022

Montaggio di file system Amazon FSx all'avvio	Puoi montare un file system Amazon FSx for NetApp ONTAP o Amazon FSx for OpenZFS nuovo o esistente all'avvio utilizzando la nuova procedura guidata per l'istanza di avvio.	12 aprile 2022
Nuova procedura guidata di avvio dell'istanza	Un'esperienza di avvio nuova e migliorata nella console Amazon EC2, che offre un modo più rapido e semplice per avviare un'istanza EC2.	5 aprile 2022
Obsolescenza automatica delle AMI pubbliche	Di default, la data di obsolescenza di tutte le AMI pubbliche è impostata a due anni dalla data di creazione dell'AMI.	31 marzo 2022
Categoria autoscaling/target di metadati dell'istanza: -lifecycle-state	Quando si utilizzano i gruppi di Auto Scaling, è possibile accedere allo stato del ciclo di vita di destinazione di un'istanza dai metadati dell'istanza.	24 marzo 2022
Ultima data e ora di avvio dell'AMI	`lastLaunchedTime` indica la data e l'ora dell'ultimo utilizzo dell'AMI per avviare un'istanza.	28 febbraio 2022
Chiavi ED25519	Le chiavi ED25519 non sono supportate per le istanze di Windows, EC2 Instance Connect e Console seriale EC2.	20 gennaio 2022

Piattaforme RHEL aggiuntive per prenotazioni di capacità	Piattaforme Red Hat Enterprise Linux aggiuntive per le prenotazioni On-Demand di capacità.	11 gennaio 2022
Configurare le AMI di Windows per avvio più rapido	Configurare le AMI di Windows per avviare istanze fino al 65% più velocemente, utilizzando snapshot pre-provisioning.	10 gennaio 2022
Tag dell'istanza nei metadati dell'istanza	È possibile accedere ai tag di un'istanza dai metadati dell'istanza.	6 gennaio 2022
Le Prenotazioni della capacità in gruppi di collocazione cluster	Le Prenotazioni di capacità possono essere create in gruppi di collocamento cluster.	6 gennaio 2022
Avvio della serie di istanze spot prima della fine	La serie di istanze spot può terminare le istanze spot che ricevono una notifica di ribilanciamento dopo l'avvio di nuove istanze spot sostitutive.	4 novembre 2021
Avvio di EC2 Fleet prima della fine	EC2 Fleet può terminare le istanze spot che ricevono una notifica di ribilanciamento dopo l'avvio di nuove istanze spot sostitutive.	4 novembre 2021
Confronto tra timestamp	Puoi determinare l'ora reale di un evento confrontando il timestamp della tua istanza Amazon EC2 Linux con. ClockBound	2 novembre 2021

AMI condivise con organizzazioni e unità organizzative	Ora puoi condividere le AMI con le seguenti AWS risorse: organizzazioni e unità organizzative (OU).	29 ottobre 2021
Punteggio di posizionamento spot	Ottieni consigli per una AWS regione o una zona di disponibilità in base ai requisiti di capacità di Spot.	27 ottobre 2021
Attribute-based selezione del tipo di istanza per Spot Fleet	Specificare gli attributi che un'istanza deve avere e Amazon EC2 identificherà tutti i tipi di istanza con tali attributi.	27 ottobre 2021
Attribute-based selezione del tipo di istanza per EC2 Fleet	Specificare gli attributi che un'istanza deve avere e Amazon EC2 identificherà tutti i tipi di istanza con tali attributi.	27 ottobre 2021
On-Demand Flotta per la prenotazione della capacità	Per avviare un gruppo, o parco istanze, di prenotazione della capacità, puoi usare un parco istanze di prenotazione della capacità.	5 ottobre 2021
Supporto all'ibernazione per Ubuntu 20.04 LTS - Focal	Ibernazione delle istanze appena avviate da Ubuntu 20.04 LTS - Focal AMI.	4 ottobre 2021
Flotta EC2 e prenotazioni mirate On-Demand della capacità	EC2 Fleet è in grado di inserire On-Demand istanze in `targeted` prenotazioni di capacità.	22 settembre 2021
Istanze T3 su host dedicati	Supporto per istanze T3 su host dedicati Amazon EC2.	14 settembre 2021

Supporto di ibernazione per RHEL, Fedora e CentOS	Iberna le istanze appena avviate da AMI RHEL, Fedora e CentOS.	9 settembre 2021
Amazon EC2 Global View	Amazon EC2 Global View consente di visualizzare VPC, sottoreti, istanze, gruppi di sicurezza e volumi su più regioni in un'unica console. AWS	1 settembre 2021
Supporto di ibernazione per C5d, M5d e R5d	Iberna le istanze appena avviate in esecuzione sui tipi di istanza C5d, M5d e R5d.	19 agosto 2021
Coppie di chiavi Amazon EC2	Amazon EC2 ora supporta le chiavi ED25519 su istanze Linux e Mac.	17 agosto 2021
Prefissi per le interfacce di rete	È possibile assegnare un intervallo CIDR IPv4 o IPv6 privato, automaticamente o manualmente, alle interfacce di rete.	22 luglio 2021
Finestre di eventi	Puoi definire finestre di eventi personalizzate con ricorrenza settimanale per eventi pianificati che riavviano, arrestano o terminano le istanze Amazon EC2.	15 luglio 2021
ID risorse e supporto di assegnazione di tag per le regole dei gruppi di sicurezza	Puoi fare riferimento alle regole del gruppo di sicurezza in base all'ID risorsa. Puoi aggiungere i tag anche alle regole di un gruppo di sicurezza.	7 luglio 2021

Dichiarazione di un'AMI come obsoleta	È ora possibile specificare quando un'AMI viene dichiarata obsoleta.	11 giugno 2021
Fatturazione al secondo per Windows	Amazon EC2 addebita l' Server-based utilizzo di Windows e SQL in secondi, con un costo minimo di un minuto.	10 giugno 2021
Prenotazioni di capacità su AWS Outposts	È ora possibile utilizzare Prenotazioni di capacità su AWS Outposts.	24 maggio 2021
Condivisione di una Prenotazione della capacità	Ora è possibile condividere Prenotazioni di capacità create in Local Zones e Wavelength.	24 maggio 2021
Sostituzione del volume root	È ora possibile utilizzare le attività di sostituzione del volume root per sostituire il volume EBS root per le istanze in esecuzione.	22 Aprile 2021
Archiviazione e ripristino di un'AMI utilizzando S3	Archivia le EBS-backed AMI in S3 e ripristinale da S3 per consentire la copia delle AMI su più partizioni.	06 aprile 2021
Console seriale EC2	Risolvere i problemi di avvio e connettività di rete stabilendo una connessione alla porta seriale di un'istanza.	30 marzo 2021
Modalità di avvio	Amazon EC2 ora supporta l'avvio UEFI su istanze AMD ed EC2 selezionate. Intel-based	22 marzo 2021

Creazione di un record DNS inverso	È ora possibile impostare la ricerca DNS inversa per gli indirizzi IP elastici.	3 febbraio 2021
Applicazione di tag ad AMI e snapshot al momento della creazione di un'AMI	Quando si crea un'AMI, è possibile contrassegnare l'AMI e gli snapshot con gli stessi tag, oppure contrassegnarli con tag diversi.	4 dicembre 2020
Usa Amazon per monitorare gli eventi di Spot EventBridge Fleet	Crea EventBridge regole che attivino azioni programmatiche in risposta alle modifiche e agli errori di stato di Spot Fleet.	20 novembre 2020
Usa Amazon EventBridge per monitorare gli eventi della flotta EC2	Crea EventBridge regole che attivino azioni programmatiche in risposta alle modifiche e agli errori dello stato della flotta EC2.	20 novembre 2020
Eliminazione di parchi istanze instant	Elimina un EC2 Fleet di tipo `instant` e termina tutte le istanze del parco istanze in una singola chiamata API.	18 novembre 2020
Supporto di ibernazione per T3 e T3a	Iberna le istanze appena avviate in esecuzione sui tipi di istanza T3 e T3a.	17 Novembre 2020
Creazione rapida di Amazon EFS	È possibile creare e montare un file system Amazon EFS su un'istanza al momento dell'avvio utilizzando la Creazione rapida di Amazon EFS.	9 novembre 2020

Categoria di metadati dell'istanza: events/recommendations/rebalance	Ora approssimativa, in UTC, in cui viene emessa la notifica della raccomandazione di ribilanciamento dell'istanza EC2 per l'istanza.	4 novembre 2020
Raccomandazione di ribilanciamento dell'istanza EC2	Un segnale che ti avvisa quando un'istanza spot è a rischio elevato di interruzione.	4 novembre 2020
Prenotazioni della capacità nelle zone Wavelength	Ora è possibile creare e utilizzare Prenotazioni di capacità in Wavelength.	4 novembre 2020
Ribilanciamento della capacità	Configurare EC2 Fleet o la serie di istanze spot affinché avvii un'istanza spot sostitutiva quando Amazon EC2 emette un suggerimento di ribilanciamento.	04 novembre 2020
Supporto di ibernazione per I3, M5ad e R5ad	Iberna le istanze appena avviate in esecuzione sui tipi di istanze I3, M5ad e R5ad.	21 Ottobre 2020
Limiti di vCPU dell'istanza spot	I limiti dell'istanza spot vengono ora gestiti in termini di numero di vCPU che vengono utilizzate o verranno utilizzate dalle istanze spot in esecuzione in attesa dell'evasione delle richieste aperte.	1 ottobre 2020
Prenotazioni della capacità in zone locali	Prenotazioni di capacità può ora essere creato e utilizzato in Local Zones.	30 settembre 2020

Supporto di ibernazione per M5a e R5a	Iberna le istanze appena avviate in esecuzione sui tipi di istanza M5a e R5a.	28 agosto 2020
I metadati dell'istanza forniscono informazioni sulla posizione dell'istanza e sul posizionamento	Nuovi campi di metadati dell'istanza nella categoria `placement` : regione, nome gruppo di posizionamento, numero di partizione, ID host e ID zona di disponibilità.	24 agosto 2020
Gruppi Prenotazione della capacità	È possibile utilizzare i gruppi di AWS risorse per creare raccolte logiche di prenotazioni di capacità e quindi l'istanza di destinazione viene lanciata in tali gruppi.	29 luglio 2020
EC2Launch v2	Puoi utilizzare EC2Launch v2 per eseguire attività durante il startup dell'istanza, se un'istanza viene arrestata e avviata successivamente, se un'istanza viene riavviata e se è on demand. EC2Launch v2 supporta tutte le versioni di Windows Server e sostituisce EC2Launch e EC2config.	30 giugno 2020
Utilizzo dei propri indirizzi IPv6	Puoi trasferire parte o tutto il tuo intervallo di indirizzi IPv6 dalla tua rete locale al tuo account. AWS	21 maggio 2020

Avvio delle istanze utilizzando un parametro Systems Manager	Puoi specificare un AWS Systems Manager parametro anziché un'AMI quando avvii un'istanza.	05 maggio 2020
Personalizzazione delle notifiche di eventi pianificati	Puoi personalizzare le notifiche di eventi pianificati per includere tag nella notifica e-mail.	04 maggio 2020
Windows Server su Host dedicati	È possibile utilizzare le AMI di Windows Server fornite da Amazon per eseguire le versioni più recenti di Windows Server Host dedicati.	7 Aprile 2020
Arrestare e avviare un'istanza spot	Arresta le istanze spot supportate da Amazon EBS e avviale quando desideri, invece di fare affidamento sul comportamento di interruzione.	13 gennaio 2020
Aggiunta di tag alle risorse	È possibile contrassegnare i gateway Internet solo egress, i gateway locali, le tabelle di routing del gateway locale, le interfacce virtuali del gateway locale, i gruppi di interfacce virtuali del gateway locale, le associazioni VPC della tabella di routing del gateway locale e le associazioni di gruppi di interfacce virtuali della tabella di routing del gateway locale.	10 gennaio 2020

Connettersi all'istanza utilizzando Session Manager	Puoi avviare una sessione di Session Manager con un'istanza dalla console Amazon EC2.	18 dicembre 2019
Host dedicati e gruppi di risorse host	Gli Host dedicati ora possono essere utilizzati con gruppi di risorse host.	2 dicembre 2019
Condivisione Host dedicato	Ora puoi condividere i tuoi host dedicati tra più AWS account.	2 dicembre 2019
Specifica crediti di default a livello di account	Puoi impostare le specifiche di credito predefinite per famiglia di istanze Burstable Performance a livello di account per AWS regione.	25 novembre 2019
Individuazione del tipo di istanza	È possibile trovare un tipo di istanza che soddisfa le proprie esigenze.	22 novembre 2019
Host dedicati	Ora puoi configurare un Host dedicato per supportare più tipi di istanza in una famiglia di istanze.	21 novembre 2019
Servizio di metadati dell'istanza versione 2	Puoi utilizzare Servizio di metadati dell'istanza Versione 2, che è un metodo orientato alla sessione per richiedere metadati dell'istanza.	19 novembre 2019
Elastic Fabric Adapter	Elastic Fabric Adapters può ora essere usato con Intel MPI 2019 Update 6.	15 novembre 2019

Supporto per l'ibernazione per le istanze Windows On-Demand	È possibile On-Demand ibernare le istanze di Windows.	14 ottobre 2019
Acquisiti in coda di istanze riservate	Puoi accodare l'acquisto di un Istanza riservata fino a un massimo di tre anni in anticipo.	4 ottobre 2019
Interruzione della diagnostica	Puoi inviare un'interruzione della diagnostica a un'istanza Linux non raggiungibile o che non risponde per attivare un kernel panic.	14 agosto 2019
Strategia di allocazione ottimizzata della capacità	Utilizzando EC2 Fleet o una serie di istanze spot, puoi avviare le istanze spot da pool spot con capacità ottimale per il numero di istanze che vengono avviate.	12 agosto 2019
On-Demand Condivisione di una Prenotazione della capacità	Ora puoi condividere le tue prenotazioni di capacità tra più account. AWS	29 luglio 2019
Elastic Fabric Adapter	EFA ora supporta Open MPI 3.1.4 e Intel MPI 2019 Update 4.	26 luglio 2019
EC2 Instance Connect	Con EC2 Instance Connect, puoi connetterti in modo semplice e sicuro alle istanze tramite Secure Shell (SSH).	27 giugno 2019

Ripristino host	Riavvia automaticamente le istanze su un nuovo host in caso di errore hardware imprevisto su un Host dedicato.	5 giugno 2019
Snapshot coerenti a livello di applicazione VSS	Crea istantanee coerenti con le applicazioni di tutti i volumi Amazon EBS collegati alle tue istanze Windows utilizzando Run Command. AWS Systems Manager	13 maggio 2019
Assistente alla conversione della piattaforma da Windows a Linux per i database Microsoft SQL Server	Spostare carichi di lavoro di Microsoft SQL Server esistenti da un sistema operativo Windows a un sistema operativo Linux. Il link aggiornato indirizza a Microsoft SQL Server sulla Guida per l'utente di Amazon EC2.	8 maggio 2019
Aggiornamento automatico Windows	Esegui aggiornamenti automatici delle istanze EC2 Windows utilizzando. AWS Systems Manager	6 maggio 2019
Elastic Fabric Adapter	È possibile collegare un Elastic Fabric Adapter alle istanze per accelerare le applicazioni di tipo High Performance Computing (HPC).	29 aprile 2019

Per informazioni sui tipi di istanza rilasciati per Amazon EC2, consulta la Cronologia dei documenti nella Guida ai tipi di istanza Amazon EC2.

Cronologia per il 2018 e anni precedenti

Nella seguente tabella sono descritte le aggiunte significative apportate alla guida per l'utente di Amazon EC2 nel 2018 e negli anni precedenti.

Funzionalità	Versione API	Descrizione	Data di rilascio
Gruppi di collocamento di partizione	15-11-2016	I gruppi di collocamento di partizione distribuiscono le istanze sulle partizioni logiche, garantendo così che le istanze in una partizione non condividano l'hardware sottostante con istanze in altre partizioni. Per ulteriori informazioni, consulta Gruppi di collocamento di partizione.	20 dicembre 2018
Ibernazione delle istanze Linux EC2	15-11-2016	Puoi ibernare un'istanza Linux se è abilitata per l'ibernazione e corrisponde ai prerequisiti di ibernazione. Per ulteriori informazioni, consulta Metti in ibernazione la tua istanza Amazon EC2.	28 novembre 2018
Acceleratori di Amazon Elastic Inference	15-11-2016	Puoi collegare un acceleratore Amazon EI alle tue istanze per aggiungere GPU-powered accelerazione e ridurre i costi di esecuzione dell'inferenza di deep learning.	28 novembre 2018
La console Spot raccomanda un parco istanze	15-11-2016	La console Spot raccomanda un parco istanze basato sulla best practice Spot (diversificazione delle istanze) per soddisfare le specifiche minime hardware (vCPU, memoria e archiviazione) per le esigenze dell'applicazione. Per ulteriori informazioni, consulta Creazione di un parco istanze Spot.	20 novembre 2018
Nuovo tipo di richiesta EC2 Fleet: instant	15-11-2016	EC2 Fleet ora supporta un nuovo tipo di richiesta, `instant`, che è possibile utilizzare per assegnare la capacità in modo sincrono	14 novembre 2018

Funzionalità	Versione API	Descrizione	Data di rilascio
		tra tutti i tipi di istanza e i modelli di acquisto. La richiesta `instant` restituisce le istanze avviate nella risposta API e non esegue ulteriori operazioni, permettendoti di controllare se e quando le istanze vengono avviate. Per ulteriori informazioni, consulta Tipi di richieste del parco istanze EC2 o parco istanze Spot.	
Informazioni sui risparmi Spot	15-11-2016	Puoi visualizzare i risparmi ottenuti utilizzando le istanze spot per un singolo parco istanze spot o per tutte le istanze spot. Per ulteriori informazioni, consulta Risparmio sull'acquisto di Istanze spot.	5 novembre 2018
Supporto della console per l'ottimizzazione delle opzioni CPU	15-11-2016	Quando avvii un'istanza, è possibile ottimizzare le opzioni della CPU per soddisfare esigenze aziendali o carichi di lavoro specifici utilizzando la console Amazon EC2. Per ulteriori informazioni, consulta Opzioni della CPU per le istanze Amazon EC2.	31 ottobre 2018
Supporto della console per la creazione di un modello di avvio da un'istanza	15-11-2016	È possibile creare un modello di avvio utilizzando un'istanza come base per un nuovo modello di avvio utilizzando la console Amazon EC2. Per ulteriori informazioni, consulta Creare un modello di avvio Amazon EC2.	30 ottobre 2018

Funzionalità	Versione API	Descrizione	Data di rilascio
On-Demand Prenotazioni di capacità	15-11-2016	Puoi prenotare la capacità per le istanze Amazon EC2 per qualsiasi durata in una determinata zona di disponibilità. Questo consente di creare e gestire le prenotazioni di capacità indipendentemente rispetto agli sconti di fatturazione offerti dalle istanze riservate (RI). Per ulteriori informazioni, consulta Riserva la capacità di calcolo con EC2 On-Demand Capacity Reservations.	25 ottobre 2018
Utilizzare i propri indirizzi IP (BYOIP)	15-11-2016	Puoi trasferire parte o tutto il tuo intervallo di indirizzi IPv4 pubblici dalla tua rete locale al tuo account. AWS Una volta inserito AWS, l'intervallo di indirizzi viene visualizzato nel tuo account come pool di indirizzi. È possibile creare un indirizzo IP elastico dal pool di indirizzi e utilizzarlo con le risorse AWS . Per ulteriori informazioni, consulta Trasferire i propri indirizzi IP (BYOIP) in Amazon EC2.	23 ottobre 2018
Inserisci un tag Host dedicato al momento della creazione e supporto per la console	15-11-2016	È possibile applicare tag ai Host dedicati al momento della creazione, ed è possibile gestire i tag Host dedicato utilizzando la console Amazon EC2. Per ulteriori informazioni, consulta Alloca un host dedicato di Amazon EC2 per l'uso nel tuo account.	08 ottobre 2018
Supporto della console per il dimensionamento pianificato per serie di istanze spot	15-11-2016	Aumenta o riduce la capacità corrente del parco istanze in base alla data e all'ora. Per ulteriori informazioni, consulta Dimensionamento pianificato: scala il parco istanze spot in base a una pianificazione.	20 settembre 2018

Funzionalità	Versione API	Descrizione	Data di rilascio
Strategia di allocazione per parchi istanze EC2	15-11-2016	Puoi specificare se la On-Demand capacità è soddisfatta per prezzo (prima il prezzo più basso) o per priorità (prima la priorità più alta). Puoi specificare il numero di pool Spot in cui allocare la capacità spot di destinazione. Per ulteriori informazioni, consulta Utilizza le strategie di allocazione per determinare in che modo EC2 Fleet o Spot Fleet soddisfano Spot e la capacità On-Demand.	26 luglio 2018
Strategia di allocazione per Parchi istanze spot	15-11-2016	Puoi specificare se la On-Demand capacità viene soddisfatta per prezzo (prima il prezzo più basso) o per priorità (prima la priorità più alta). Puoi specificare il numero di pool Spot in cui allocare la capacità spot di destinazione. Per ulteriori informazioni, consulta Utilizza le strategie di allocazione per determinare in che modo EC2 Fleet o Spot Fleet soddisfano Spot e la capacità On-Demand.	26 luglio 2018
Automazione del ciclo di vita degli snapshot	15-11-2016	È possibile utilizzare Amazon Data Lifecycle Manager per automatizzare la creazione e l'eliminazione di snapshot per i volumi EBS. Per ulteriori informazioni, consulta Amazon Data Lifecycle Manager.	12 luglio 2018
Opzioni CPU del modello di avvio	15-11-2016	Quando si crea un modello di avvio tramite gli strumenti a riga di comando, è possibile ottimizzare le opzioni della CPU per soddisfare esigenze aziendali o carichi di lavoro specifici . Per ulteriori informazioni, consulta Creare un modello di avvio Amazon EC2.	11 luglio 2018

Funzionalità	Versione API	Descrizione	Data di rilascio
Tagging di Host dedicati	15-11-2016	È possibile contrassegnare con dei tag gli Host dedicati.	3 luglio 2018
Output della console più recente	15-11-2016	È possibile recuperare l'ultimo output della console per alcuni tipi di istanza quando si utilizza il comando https://docs.aws.amazon.com/cli/latest/reference/ec2/get-console-output.html AWS CLI get-console-output.	9 maggio 2018
Ottimizzazione delle opzioni della CPU	15-11-2016	Quando avvii un'istanza, è possibile ottimizzare le opzioni della CPU per soddisfare esigenze aziendali o carichi di lavoro specifici. Per ulteriori informazioni, consulta Opzioni della CPU per le istanze Amazon EC2.	8 maggio 2018
EC2 Fleet	15-11-2016	Puoi utilizzare EC2 Fleet per avviare un gruppo di istanze su diversi tipi di istanze EC2 e zone di disponibilità e su modelli di acquisto di istanze, istanze riservate e On-Demand istanze Spot. Per ulteriori informazioni, consulta EC2 Fleet e parco istanze spot.	2 maggio 2018
On-Demand Istanze in flotte Spot	15-11-2016	Puoi includere una richiesta di On-Demand capacità nella tua richiesta Spot Fleet per assicurarti di avere sempre la capacità di istanze. Per ulteriori informazioni, consulta EC2 Fleet e parco istanze spot.	2 maggio 2018
Tag di snapshot EBS alla creazione	15-11-2016	È possibile contrassegnare con tag gli snapshot durante la creazione.	2 aprile 2018

Funzionalità	Versione API	Descrizione	Data di rilascio
Modifica dei gruppi di collocamento	15-11-2016	È possibile spostare un'istanza all'interno o all'esterno di un gruppo di collocamento o modificarne il gruppo di collocamento. Per ulteriori informazioni, consulta Modifica del collocamento per un'istanza EC2.	1 marzo 2018
ID più lunghi per le risorse	15-11-2016	È possibile abilitare il formato ID più lungo per più tipi di risorse.	9 febbraio 2018
Miglioramenti in termini di prestazioni di rete	15-11-2016	Le istanze al di fuori di un gruppo di posizionamento cluster possono ora usufruire di una maggiore larghezza di banda durante l'invio o la ricezione del traffico di rete tra altre istanze o Amazon S3.	24 gennaio 2018
Tag di indirizzi IP elastici	15-11-2016	È possibile contrassegnare con tag gli indirizzi IP elastici.	21 dicembre 2017
Amazon Time Sync Service	15-11-2016	È possibile utilizzare il servizio Amazon Time Sync per mantenere l'orario preciso nell'istanza. Per ulteriori informazioni, consulta Sincronizzazione precisa dell'orologio e dell'ora sull'istanza EC2.	29 novembre 2017
T2 Unlimited	15-11-2016	Le istanze T2 in modalità illimitata possono superare la baseline per tutto il periodo necessario. Per ulteriori informazioni, consulta Istanze a prestazioni espandibili.	29 novembre 2017

Funzionalità	Versione API	Descrizione	Data di rilascio
Modelli di lancio	15-11-2016	Un modello di avvio può contenere tutti o alcuni parametri per avviare un'istanza, così da non doverli specificare ogni volta che avvii un'istanza. Per ulteriori informazioni, consulta Archivia i parametri di avvio dell'istanza nei modelli di avvio di Amazon EC2.	29 novembre 2017
Collocazione sparsa	15-11-2016	I gruppi di collocamento sparsa sono consigliati per le applicazioni con un numero ridotto di istanze critiche che è necessario tenere separate. Per ulteriori informazioni, consulta Gruppi di collocazione sparsi.	29 novembre 2017
Ibernazione di istanza spot	15-11-2016	Il servizio Spot può ibernare le istanze spot in caso di interruzione.	28 novembre 2017
Monitoraggio degli obiettivi del parco istanze spot	15-11-2016	È possibile configurare policy di dimensionamento con monitoraggio degli obiettivi per il parco istanze spot. Per ulteriori informazioni, consulta Dimensionamento con monitoraggio degli obiettivi: scala il parco istanze spot definendo come target un valore per una metrica specifica.	17 novembre 2017
La serie di istanze spot si integra con Elastic Load Balancing	15-11-2016	È possibile collegare uno o più load balancer a una serie di istanze Spot.	10 novembre 2017

Funzionalità	Versione API	Descrizione	Data di rilascio
Unione e divisione di Istanze riservate modificabili	15-11-2016	È possibile scambiare (unire) due o più Istanze riservate modificabili per ottenere una nuova Istanza riservata modificabile. Inoltre è possibile utilizzare il processo di modifica per suddividere una Istanza riservata modificabile in prenotazioni più piccole. Per ulteriori informazioni, consulta Scambiare le Istanze riservate modificabili.	6 novembre 2017
Modifica della tenancy di un VPC	15-11-2016	È possibile modificare l'attributo della tenancy delle istanze di un VPC da `dedicated` a `default`. Per ulteriori informazioni, consulta Modifica della tenancy di un'istanza di un PVC.	16 ottobre 2017
Fatturazione per secondo	15-11-2016	Amazon EC2 addebita l' Linux-based utilizzo al secondo, con un costo minimo di un minuto.	2 ottobre 2017
Arresto in caso di interruzione	15-11-2016	È possibile specificare se Amazon EC2 deve arrestare o terminare le Istanze spot quando vengono interrotte. Per ulteriori informazioni, consulta Comportamento delle interruzioni dell'istanza spot.	18 settembre 2017
Tag di gateway NAT	15-11-2016	È possibile contrassegnare con dei tag il gateway NAT. Per ulteriori informazioni, consulta Assegnazione di tag alle risorse.	7 settembre 2017
Descrizione della regola di gruppo di sicurezza	15-11-2016	È possibile aggiungere descrizioni alle regole di un gruppo di sicurezza.	31 agosto 2017
Elastic Graphics	15-11-2016	Collegare gli acceleratori Grafica elastica alle istanze per accelerare le prestazioni grafiche delle applicazioni.	29 agosto 2017

Funzionalità	Versione API	Descrizione	Data di rilascio
Ripristino degli indirizzi IP elastici	15-11-2016	Se rilasci un indirizzo IP elastico per l'uso in un VPC, è possibile recuperarlo.	11 agosto 2017
Tag serie di istanze spot	15-11-2016	È possibile configurare il Parco istanze spot in modo che contrassegni automaticamente con tag le istanze che avvia.	24 luglio 2017
Assegnazione di tag alle risorse al momento della creazione	15-11-2016	È possibile contrassegnare con tag le istanze e i volumi durante la creazione. Per ulteriori informazioni, consulta Assegnazione di tag alle risorse. Inoltre, è possibile utilizzare le autorizzazioni a livello di risorsa basate su tag per controllare i tag applicati. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag Amazon EC2 per le risorse durante la creazione.	28 marzo 2017
Esecuzione di modifiche sui volumi EBS collegati	15-11-2016	Con la maggior parte dei volumi EBS collegata alla maggior parte delle istanze EC2, è possibile modificare le dimensioni, il tipo e IOPS del volume senza scollegare il volume o arrestare l'istanza.	13 febbraio 2017
Collegamento di un ruolo IAM	15-11-2016	Inoltre, è possibile collegare, distaccare o sostituire un ruolo IAM per un'istanza esistente . Per ulteriori informazioni, consulta Ruoli IAM per Amazon EC2.	9 febbraio 2017
Istanze spot dedicate	15-11-2016	È possibile eseguire Istanze spot su hardware con tenant singolo in un virtual private cloud (VPC). Per ulteriori informazioni, consulta Avvio su hardware con tenant singolo.	19 gennaio 2017

Funzionalità	Versione API	Descrizione	Data di rilascio
Supporto IPv6	15-11-2016	È possibile associare un CIDR IPv6 al VPC e alle sottoreti e assegnare gli indirizzi IPv6 alle istanze nel VPC. Per ulteriori informazioni, consulta Indirizzamento IP per le istanze Amazon EC2.	1 dicembre 2016
Scalabilità automatica per il Parco istanze spot		Ora è possibile configurare policy di dimensionamento per il Parco istanze spot. Per ulteriori informazioni, consulta Informazioni sulla scalabilità automatica per il parco istanze spot.	1 settembre 2016
Elastic Network Adapter (ENA)	01/04/2016	Ora, è possibile utilizzare ENA per reti avanzate. Per ulteriori informazioni, consulta Rete migliorata per le istanze Amazon EC2.	28 giugno 2016
Supporto avanzato per la visualizzazione e la modifica di ID più lunghi	01/04/2016	Ora è possibile visualizzare e modificare le impostazioni degli ID più lunghi per altri utenti IAM, ruoli IAM o per l'utente root.	23 giugno 2016
Copia istantanee crittografate di Amazon EBS tra account AWS	01/04/2016	Ora puoi copiare istantanee EBS crittografate tra account. AWS	21 giugno 2016
Acquisizione di uno screenshot di una console di istanze	01/10/2015	Ora, è possibile ottenere ulteriori informazioni durante il debug di istanze irraggiungibili. Per ulteriori informazioni, consulta Acquisizione di uno screenshot di un'istanza irraggiungibile.	24 maggio 2016
Due nuovi tipi di volume EBS	01/10/2015	Ora, è possibile creare volumi Throughput Optimized HDD (st1) e Cold HDD (sc1).	19 aprile 2016

Funzionalità	Versione API	Descrizione	Data di rilascio
Sono state aggiunte nuove NetworkPacketsIn NetworkPacketsOut metriche per Amazon EC2		Sono state aggiunte nuove NetworkPacketsIn NetworkPacketsOut metriche per Amazon EC2. Per ulteriori informazioni, consulta Parametri dell'istanza.	23 marzo 2016
CloudWatch metriche per Spot Fleet		Ora puoi ottenere le CloudWatch metriche per la tua flotta Spot. Per ulteriori informazioni, consulta Monitora la tua flotta EC2 o la tua flotta Spot utilizzando CloudWatch.	21 marzo 2016
Istanze pianificate	01/10/2015	Le istanze riservate pianificate (istanze pianificate) ti permettono di acquistare prenotazioni di capacità giornaliere, settimanali o mensili con una data di inizio e una durata specifici.	13 gennaio 2016
ID più lunghi per le risorse	01/10/2015	Amazon EC2 sta gradualmente introducendo ID di lunghezza maggiore per alcuni tipi di risorse Amazon EC2 e Amazon EBS. Durante il periodo di accettazione, è possibile abilitare il formato ID più lungo per i tipi di risorsa supportati.	13 gennaio 2016
ClassicLink Supporto DNS	01/10/2015	Puoi abilitare il supporto ClassicLink DNS per il tuo VPC in modo che i nomi host DNS indirizzati tra le istanze collegate e EC2-Classic le istanze nel VPC si risolvano in indirizzi IP privati e non in indirizzi IP pubblici.	11 gennaio 2016
Host dedicati	01/10/2015	Un host dedicato di Amazon EC2 è un server fisico con capacità di istanze dedicata al tuo uso. Per ulteriori informazioni, consulta Host dedicati di Amazon EC2.	23 novembre 2015

Funzionalità	Versione API	Descrizione	Data di rilascio
Durata dell'istanza spot	01/10/2015	Ora, è possibile specificare una durata per le Istanze spot. I blocchi di istanze Spot non sono supportati (gennaio 2023).	6 ottobre 2015
Richiesta di modificare di un Parco istanze spot	01/10/2015	Ora è possibile modificare la capacità obiettivo della richiesta del parco istanze spot. Per ulteriori informazioni, consulta Modificare una richiesta di parco istanze spot.	29 settembre 2015
Strategia di allocazione diversificata del Parco istanze spot	15/04/2015	Ora è possibile allocare le istanze spot in più pool Spot utilizzando una sola richiesta di Parco istanze spot. Per ulteriori informazioni, consulta Utilizza le strategie di allocazione per determinare in che modo EC2 Fleet o Spot Fleet soddisfano Spot e la capacità On-Demand.	15 settembre 2015
Ponderazione delle istanze del Parco istanze spot	15/04/2015	Ora, è possibile definire le unità di capacità con cui ogni tipo di istanza contribuisce alle prestazioni dell'applicazione e regolare di conseguenza il prezzo di offerta per le Istanze spot di ciascun pool di Spot. Per ulteriori informazioni, consulta Utilizza la ponderazione delle istanze per gestire i costi e le prestazioni del parco istanze EC2 o del parco istanze spot.	31 agosto 2015
Nuova operazione di allarme di riavvio e nuovo ruolo IAM per l'uso con operazioni di allarme		Sono stati aggiunti l'operazione di allarme di riavvio e un nuovo ruolo IAM per l'uso con operazioni di allarme. Per ulteriori informazioni, consulta Creazione di allarmi che arrestano, terminano, riavviano o recuperano un'istanza.	23 luglio 2015

Funzionalità	Versione API	Descrizione	Data di rilascio
Spot Fleets	15/04/2015	È possibile gestire una raccolta o un parco di istanze anziché gestire richieste di Parco istanze spot separate. Per ulteriori informazioni, consulta EC2 Fleet e parco istanze spot.	18 maggio 2015
Esegui la migrazione degli indirizzi IP elastici su EC2-Classic	15/04/2015	Puoi migrare un indirizzo IP elastico che hai assegnato per l'uso in EC2-Classic un VPC.	15 maggio 2015
Importazione di VMs con più dischi come AMI	01/03/2015	Ora, il processo VM Import supporta l'importazione di VM con più dischi come AMI. Per ulteriori informazioni, consulta Importazione di una macchina virtuale come immagine utilizzando una macchina virtuale nella Guida per l'utente della VM. Import/Export Import/Export	23 aprile 2015
Systems Manager		Systems Manager consente di configurare e gestire le istanze EC2.	17 febbraio 2015
Systems Manager per Microsoft SCVMM 1.5		Ora, puoi utilizzare Systems Manager per Microsoft SCVMM per avviare un'istanza e importare una VM da SCVMM in Amazon EC2.	21 gennaio 2015

Funzionalità	Versione API	Descrizione	Data di rilascio
Ripristino automatico di istanze EC2		Puoi creare un CloudWatch allarme Amazon che monitora un'istanza Amazon EC2 e ripristina automaticamente l'istanza se viene danneggiata a causa di un guasto hardware sottostante o di un problema che richiede l'intervento di riparazione. AWS Un'istanz a ripristinata è identica all'istanza originale, incluso l'ID dell'istanza, gli indirizzi IP e tutti i metadati dell'istanza. Per ulteriori informazioni, consulta Ripristino automatico dell'istanza.	12 gennaio 2015
ClassicLink	01/10/2014	ClassicLink ti consente di collegare la tua EC2-Classic istanza a un VPC nel tuo account. È possibile associare i gruppi di sicurezza VPC all'istanza EC2-Classic e consentire la comunicazione tra l'istanza EC2-Classic e le istanze del VPC tramite indirizzi IP privati.	7 gennaio 2015
Avvisi di interruzione delle istanze spot		Il modo migliore per prevenire l'interruzione dell'istanza spot è quello di progettare l'applica zione in modo che sia tollerante ai guasti. Inoltre, è possibile usufruire degli avvisi di interruzione delle istanze spot, che avvisano l'utente due minuti prima che Amazon EC2 termini il Parco istanze spot. Per ulteriori informazioni, consulta Avvisi di interruzione dell'istanza spot.	5 gennaio 2015
Systems Manager per Microsoft SCVMM		Systems Manager for Microsoft SCVMM fornisce un'interfaccia semplice e facile da usare per la gestione AWS delle risorse, come le istanze EC2, di Microsoft SCVMM.	29 ottobre 2014

Funzionalità	Versione API	Descrizione	Data di rilascio
Supporto della paginazione di `DescribeVolumes`	01/03/2014	Ora, la chiamata API `DescribeVolumes` supporta la paginazione dei risultati con i parametri `MaxResults` e `NextToken`. Per ulteriori informazioni, consulta Amazon EC2 API Reference. DescribeVolumes	23 ottobre 2014
È stato aggiunto il supporto per Amazon Logs CloudWatch		Puoi utilizzare Amazon CloudWatch Logs per monitorare, archiviare e accedere al sistema, all'applicazione e ai file di registro personalizzati dalle tue istanze o da altre fonti. Puoi quindi recuperare i dati di log associati da CloudWatch Logs utilizzando la CloudWatch console Amazon, i comandi CloudWatch Logs nella AWS CLI o il CloudWatch Logs SDK.	10 luglio 2014
Nuova pagina EC2 Service Limits (Restrizioni dei servizi EC2)		Utilizzare la pagina EC2 Service Limits (Restrizioni dei servizi EC2) nella console Amazon EC2 per visualizzare i limiti attuali per le risorse fornite da Amazon EC2 e Amazon VPC, in base alla regione.	19 giugno 2014
Volumi Amazon EBS General Purpose SSD	01/05/2014	I volumi General Purpose SSD offrono archiviazione conveniente ideale per un'ampia gamma di carichi di lavoro. Questi volumi offrono latenze di millisecondi a una cifra, la capacità di arrivare a 3.000 IOPS per lunghi periodi di tempo e una performance base di 3. IOPS/GiB La dimensione di un volume SSD per scopo generico può essere compresa tra 1 GiB e 1 TiB.	16 giugno 2014
AWS Management Pack		AWS Il Management Pack ora supporta System Center Operations Manager 2012 R2.	22 maggio 2014

Funzionalità	Versione API	Descrizione	Data di rilascio
Amazon EBS encryption	01/05/2014	Crittografia Amazon EBS offre una soluzione di crittografia semplice per gli snapshot e i volumi di dati EBS senza la necessità di creare e mantenere un'infrastruttura di gestione delle chiavi sicura. La crittografia EBS consente la sicurezza dei dati inattivi tramite la crittografia dei dati utilizzando Chiavi gestite da AWS. La crittografia viene implementata a livello del server che ospita le istanze EC2, perciò viene applicata anche ai dati in trasferimento tra le istanze EC2 e l'archiviazione EBS.	21 maggio 2014
Report di utilizzo di Amazon EC2		I report di utilizzo di Amazon EC2 sono un insieme di report che mostrano dati su costi e uso relativi all'utilizzo di EC2.	28 gennaio 2014
Importazione della macchina virtuale Linux	15/10/2013	Ora, il processo VM Import supporta l'importazione di istanze Linux. Per ulteriori informazioni, consulta la VM Import/Export User Guide.	16 dicembre 2013
Resource-level autorizzazioni per RunInstances	15/10/2013	Ora puoi creare policy AWS Identity and Access Management per controllare le autorizzazioni a livello di risorsa per l'azione API di Amazon EC2. RunInstances Per ulteriori informazioni e policy di esempio, consulta Identity and Access Management per Amazon EC2.	20 novembre 2013
Avvio di un'istanza da Marketplace AWS		È ora possibile avviare un'istanza Marketplace AWS utilizzando la procedura guidata di avvio di Amazon EC2. Per ulteriori informazioni, consulta Avvia un'istanza Amazon EC2 da un'AMI Marketplace AWS.	11 novembre 2013

Funzionalità	Versione API	Descrizione	Data di rilascio
Nuova procedura guidata di avvio		È disponibile una procedura guidata di avvio nuova e riprogettata di EC2. Per ulteriori informazioni, consulta Avviare un'istanza EC2 tramite la procedura guidata di avvio dell'istanza nella console.	10 ottobre 2013
Modifica dei tipi di istanza delle istanze riservate	01/10/2013	È ora possibile modificare il tipo di istanza di istanze riservate Linux all'interno della stessa famiglia (ad esempio, M1, M2, M3, C1). Per ulteriori informazioni, consulta Modificare le Istanze riservate.	09 ottobre 2013
Modifica delle istanze riservate Amazon EC2	15/08/2013	Ora, è possibile modificare le istanze riservate in una regione. Per ulteriori informazioni, consulta Modificare le Istanze riservate.	11 settembre 2013
Assegnazione di un indirizzo IP pubblico	15/07/2013	Ora, è possibile assegnare un indirizzo IP pubblico quando si avvia un'istanza in un VPC. Per ulteriori informazioni, consulta Assegnare un indirizzo IPv4 pubblico all'avvio.	20 agosto 2013
Concessione delle autorizzazioni a livello di risorsa	15/06/2013	Amazon EC2 supporta nuovi nomi della risorsa Amazon (ARN) e chiavi di condizione. Per ulteriori informazioni, consulta Identity-based politiche per Amazon EC2.	8 luglio 2013
Copie di snapshot incrementali	01/02/2013	Ora, è possibile eseguire copie di snapshot incrementali.	11 giugno 2013
AWS Pacchetto di gestione		Il AWS Management Pack collega le istanze Amazon EC2 e i sistemi operativi Windows o Linux in esecuzione al loro interno. Il AWS Management Pack è un'estensione di Microsoft System Center Operations Manager.	8 maggio 2013

Funzionalità	Versione API	Descrizione	Data di rilascio
Nuova pagina Tags (Tag)		È disponibile una nuova pagina Tags (Tag) nella console Amazon EC2. Per ulteriori informazioni, consulta Tagging delle risorse Amazon EC2..	04 aprile 2013
Copia di un'AMI da una regione a un'altra	01/02/2013	È possibile copiare un'AMI da una regione all'altra, in modo da avviare istanze coerenti in più di una AWS regione in modo rapido e semplice. Per ulteriori informazioni, consulta Copiare un'AMI Amazon EC2.	11 marzo 2013
Avvio di istanze in un VPC predefinito	01/02/2013	Il tuo AWS account è in grado di avviare istanze in uno EC2-Classic o in un VPC, o solo in un VPC, regione per regione. Se riesci ad avviare le istanze solo in un VPC, viene creato automaticamente un VPC predefinito. Quando avvii un'istanza, questa viene avviata nel tuo VPC predefinito, a meno che tu non crei un VPC non predefinito e lo specifichi all'avvio dell'istanza.	11 marzo 2013
Copia snapshot EBS	01/12/2012	È possibile utilizzare copie snapshot per creare backup di dati, creare nuovi volumi Amazon EBS o creare Amazon Machine Image (AMI).	17 dicembre 2012
Controlli dello stato e parametri EBS aggiornati per volumi SSD con capacità di IOPS allocata	01/10/2012	I parametri di EBS sono stati aggiornati in modo da includere due nuovi parametri per i volumi SSD con capacità di IOPS allocata. Inoltre, sono stati aggiunti nuovi controlli dello stato per i volumi SSD con capacità di IOPS allocata.	20 novembre 2012

Funzionalità	Versione API	Descrizione	Data di rilascio
Stato della richiesta di istanza spot	01/10/2012	Lo stato della richiesta di istanza spot facilita la determinazione dello stato delle richieste Spot.	14 ottobre 2012
Marketplace di istanze riservate Amazon EC2	15/08/2012	Il Marketplace delle istanze riservate mette in comunicazione i venditori che dispongono di istanze riservate Amazon EC2 non più necessarie e gli acquirenti che desiderano acquistare capacità aggiuntiva. Le istanze riservate acquistate e vendute attraverso il Marketplace delle istanze riservate funzionano come qualsiasi altra istanza riservata, tranne che possono avere meno di un periodo di validità standard completo rimanente e possono essere vendute a prezzi diversi.	11 settembre 2012
SSD con capacità di IOPS allocata per Amazon EBS	20/07/2012	I volumi SSD IOPS con provisioning offrono prestazioni elevate e prevedibili per carichi di lavoro I/O intensivi, come le applicazioni di database, che si basano su tempi di risposta costanti e rapidi.	31 luglio 2012
Ruoli IAM per istanze Amazon EC2	01/06/2012	I ruoli IAM per Amazon EC2 forniscono: • AWS chiavi di accesso per le applicazioni in esecuzione su istanze Amazon EC2. • Rotazione automatica delle chiavi di AWS accesso sull'istanza Amazon EC2. • Autorizzazioni granulari per le applicazioni in esecuzione su istanze Amazon EC2 che effettuano richieste ai tuoi servizi. AWS	11 giugno 2012

Funzionalità	Versione API	Descrizione	Data di rilascio
Caratteristiche delle istanze spot che semplificano l'avvio e gestiscono il potenziale di interruzione.		Ora, è possibile gestire le Istanze spot come segue: • Specificare la quantità che si è disposti a offrire per Istanze spot tramite le configurazioni di avvio di Auto Scaling e pianificare la quantità che sei disposto a offrire per Istanze spot. Per ulteriori informazioni, consulta Request Spot Instances nella Guida per l'utente di Amazon EC2 Auto Scaling. • Ricevi notifiche quando le istanze vengono avviate o terminate. • Usa CloudFormation i modelli per avviare le istanze Spot in uno stack di risorse. AWS	7 giugno 2012
Esportazione dell'istanza EC2 e time stamp per i controlli dello stato per Amazon EC2	01/05/2012	È stato aggiunto supporto per l'esportazione dell'istanza di Windows Server originariamente importate in EC2. È stato aggiunto supporto per time stamp sullo stato dell'istanza e sullo stato del sistema per indicare la data e l'ora in cui un controllo dello stato non è riuscito.	25 maggio 2012
Esportazione dell'istanza EC2 e time stamp in istanza e controlli dello stato del sistema per Amazon VPC	01/05/2012	È stato aggiunto il supporto per l'esportazione delle istanze EC2 verso Citrix XenHyper-V, Microsoft e VMware vSphere. È stato aggiunto supporto per time stamp in istanza e controlli dello stato del sistema.	25 maggio 2012
Marketplace AWS AMI	01/04/2012	È stato aggiunto il supporto per le Marketplace AWS AMI.	19 aprile 2012

Funzionalità	Versione API	Descrizione	Data di rilascio
Livelli di prezzi delle istanze riservate	15/12/2011	È stata aggiunta una nuova sezione in cui viene indicato come usufruire del prezzo scontato integrato nei livelli di prezzi delle istanze riservate.	5 marzo 2012
Interfacce di rete elastiche per istanze EC2 in Amazon Virtual Private Cloud	01/12/2011	È stata aggiunta una nuova sezione relativa alle interfacce di rete elastiche per le istanze EC2 in un VPC. Per ulteriori informazioni, consulta Interfacce di rete elastiche.	21 dicembre 2011
Nuovi tipi di offerta per le istanze riservate Amazon EC2	01/11/2011	È possibile scegliere tra una varietà di offerte di istanze riservate che riguardano l'utilizzo previsto dell'istanza.	01 dicembre 2011
Stato dell'istanza Amazon EC2	01/11/2011	Puoi visualizzare ulteriori dettagli sullo stato delle tue istanze, inclusi gli eventi programmati pianificati AWS che potrebbero avere un impatto sulle tue istanze. Queste attività operative includono i riavvii delle istanze necessari per applicare gli aggiornamenti software o le patch di sicurezza oppure i requisiti necessari per il ritiro delle istanze in caso di problemi hardware. Per ulteriori informazioni, consulta Monitoraggio dello stato delle istanze Amazon EC2.	16 novembre 2011
Istanze spot in Amazon VPC	15/07/2011	Sono state aggiunte informazioni sul supporto per le Amazon VPC in Istanze spot. Con questo aggiornamento, gli utenti possono avviare Istanze spot in un virtual private cloud (VPC). Avviando Istanze spot in un VPC, gli utenti delle Istanze spot possono sfruttare i vantaggi di Amazon VPC.	11 ottobre 2011

Funzionalità	Versione API	Descrizione	Data di rilascio
Processo di VM import semplificato per gli utenti degli strumenti CLI	15/07/2011	Il processo VM Import viene semplificato con la funzionalità avanzata di `ImportInstance` e `ImportVolume`, che ora eseguirà il caricamento delle immagini in Amazon EC2 dopo aver creato l'attività di importazione. Inoltre, con l'introduzione di `ResumeImport`, gli utenti possono riavviare un caricamento incompleto nel punto in cui l'attività è stata interrotta.	15 settembre 2011
Supporto per l'importazione in formato file VHD		Ora, VM Import può importare file di immagini di macchine virtuali in formato VHD. Il formato di file VHD è compatibile con le piattaforme di virtualizzazione Citrix Xen e Microsoft. Hyper-V Con questa versione, VM Import ora supporta i formati di immagine RAW, VHD e VMDK (VMware). ESX-compatible Per ulteriori informazioni, consulta la VM User Guide. Import/Export	24 agosto 2011
Aggiorna al connettore di importazione VM di Amazon EC2 per VMware vCenter		Sono state aggiunte informazioni sulla versione 1.1 del connettore di importazione VM di Amazon EC2 per l'appliance virtuale VMware vCenter (Connector). Questo aggiornamento include il supporto proxy per l'accesso a Internet, una migliore gestione degli errori, una maggiore accuratezza della barra di avanzamento delle attività e diverse correzioni di bug.	27 giugno 2011

Funzionalità	Versione API	Descrizione	Data di rilascio
Modifiche dei prezzi della zona di disponibilità delle Istanze spot	15/05/2011	Sono state aggiunte informazioni sulla funzione dei prezzi della zona di disponibilità delle Istanze spot. In questa versione, sono state aggiunte nuove opzioni di prezzo per le zone di disponibilità come parte delle informazioni restituite quando si richiedono le richieste di istanze Spot e la cronologia dei prezzi Spot. Queste aggiunte semplificano la determinazione del prezzo richiesto per avviare un'istanza spot in una particolare zona di disponibilità.	26 maggio 2011
AWS Identity and Access Management		Sono state aggiunte informazioni su AWS Identity and Access Management (IAM), che consentono agli utenti di specificare quali azioni Amazon EC2 un utente può utilizzare con le risorse Amazon EC2 in generale. Per ulteriori informazioni, consulta Identity and Access Management per Amazon EC2.	26 aprile 2011
Istanze dedicate		Avviate all'interno dell'Amazon Virtual Private Cloud (Amazon VPC), le istanze dedicate sono istanze fisicamente isolate a livello di hardware host. Le istanze dedicate ti consentono di sfruttare Amazon VPC e il AWS cloud, con vantaggi che includono il provisioning elastico su richiesta e pagano solo per ciò che usi, isolando le istanze di calcolo di Amazon EC2 a livello hardware. Per ulteriori informazioni, consulta Istanze dedicate Amazon EC2.	27 marzo 2011

Funzionalità	Versione API	Descrizione	Data di rilascio
AWS Aggiornamenti delle istanze riservate alla console di gestione		Gli aggiornamenti alla Console di AWS gestione facilitano agli utenti la visualizzazione delle proprie istanze riservate e l'acquisto di istanze riservate aggiuntive, incluse le istanze riservate dedicate.	27 marzo 2011
Informazioni sui metadati	01-01-2011	Sono state aggiunte informazioni sui metadati per riflettere le modifiche nella versione 01/01/2011. Per ulteriori informazioni, consulta Utilizzo dei metadati dell'istanza per gestire l'istanza EC2 e Categorie di metadati dell'istanza.	11 marzo 2011
Amazon EC2 VM Import Connector per VMware vCenter		Sono state aggiunte informazioni sul connettore di importazione VM di Amazon EC2 per l'appliance virtuale VMware vCenter (Connector). Il Connector è un plug-in per VMware vCenter che si integra con il client VMware vSphere e fornisce un'interfaccia utente grafica che è possibile utilizzare per importare le macchine virtuali VMware in Amazon EC2.	3 marzo 2011
Forzatura del distacco del volume		Ora puoi utilizzare Console di gestione AWS per forzare il distacco di un volume Amazon EBS da un'istanza.	23 febbraio 2011
Protezione per la cessazione dell'istanza		È ora possibile utilizzare la console di AWS gestione per impedire la chiusura di un'istanza. Per ulteriori informazioni, consulta Modifica della protezione da terminazione dell'istanza.	23 febbraio 2011

Funzionalità	Versione API	Descrizione	Data di rilascio
VM Import	15/11/2011	Sono state aggiunte informazioni su VM Import, cosa che consente l'importazione di una macchina virtuale o un volume in Amazon EC2. Per ulteriori informazioni, consulta la VM Import/Export User Guide.	15 dicembre 2010
Monitoraggio base per istanze	31/08/2010	Sono state aggiunte informazioni sul monitoraggio base per le istanze EC2.	12 dicembre 2010
Filtri e tag	31/08/2010	Sono state aggiunte informazioni sull'elenco, il filtraggio e il tagging delle risorse. Per ulteriori informazioni, consulta Trova le risorse Amazon EC2 e Tagging delle risorse Amazon EC2..	19 settembre 2010
Avvio di istanze idempotenti	31/08/2010	Sono state aggiunte informazioni sull'assicurazione dell'idempotenza durante l'esecuzione delle istanze.	19 settembre 2010
AWS Identity and Access Management per Amazon EC2		Amazon EC2 ora si integra con AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta Identity and Access Management per Amazon EC2.	2 settembre 2010
Designazione di indirizzi IP di Amazon VPC	15/06/2010	Ora, gli utenti Amazon VPC possono specificare l'indirizzo IP pubblico per assegnare un'istanza avviata in un VPC.	12 luglio 2010
CloudWatch Monitoraggio Amazon per i volumi Amazon EBS		Il CloudWatch monitoraggio di Amazon è ora disponibile automaticamente per i volumi Amazon EBS.	14 giugno 2010

Funzionalità	Versione API	Descrizione	Data di rilascio
Istanze riservate con Windows		Ora, Amazon EC2 supporta le istanze riservate con Windows.	22 febbraio 2010

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.